

# NetQoS NetVoyant 7.0 Administrator Guide

[www.netqos.com](http://www.netqos.com)

NetVoyant Administrator Guide

Copyright © 2010 NetQoS, Inc. All rights reserved.

DV70AG-0

This document and the software it describes are furnished under license and must be used in accordance with that license. Except as permitted by license, no part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or information storage or retrieval system, without the written permission of NetQoS.

**The contents of this document are for informational purposes only and subject to change without notice. No liability is assumed for technical or editorial omissions contained herein.**

NetQoS, the NetQoS Logo, SuperAgent, ReporterAnalyzer, NetVoyant, and Allocate are trademarks or registered trademarks of NetQoS, Inc. Other product and company names mentioned herein may be the trademarks or registered trademarks of their respective organizations.

Notice to U.S. government end users: this document and the software it describes are “commercial items” as defined by 48 C.F.R § 2.101 and consist of “commercial computer software” and “commercial computer software documentation” as used in 48 C.F.R 12.212 or 48 C.F.R § 227.7202 as applicable. Consistent with 48 C.F.R § 12.212 or 48 C.F.R § 227.7202-1 through 48 C.F.R § 227.7202-4, the commercial software and commercial computer software documentation are being licensed to U.S. government end users only as commercial items and with only those rights as are granted to all other end users pursuant to the terms and conditions set forth in the NetQoS standard commercial license agreement for this software. For DOD agencies, the government’s rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202. Any unpublished rights are reserved under the copyright laws of the United States of America.

---

# Contents

---

<b>PREFACE</b>	<b>About This Document</b>	<b>11</b>
	Related Documentation.....	12
	Conventions.....	12
	Providing Documentation Feedback.....	13
<b>CHAPTER 1</b>	<b>NetVoyant System Setup</b>	<b>15</b>
	NetVoyant Architectural Overview and Licensing.....	16
	Operational Requirements.....	17
	NetVoyant Licensing.....	18
	Disabling License Warnings.....	20
	Managing Poll Instances.....	20
	Contacting Technical Support.....	21
	About the Master Server and Pollers.....	21
	Adding Remote Pollers to a NetVoyant Distributed System.....	21
	Configuring a Poller.....	22
	Adding a Poller as Trusted Site.....	22
	About NetVoyant Administration.....	23
	Using the NetVoyant Console.....	24
	Configuring NetVoyant Console Properties.....	26
	Opening Reports from the NetVoyant Console.....	27
	Scheduling Command Line Tasks from the NetVoyant Console.....	28
	Installing a Remote NetVoyant Console.....	29
	Maintaining the NetVoyant Database.....	30
<b>CHAPTER 2</b>	<b>Configuring Your NetVoyant System</b>	<b>31</b>
	NetVoyant Configuration Tasks.....	32
	Using the Configuration Wizard.....	33

Performing Initial Configuration Tasks .....	34
Adding SNMP Profiles to the Console .....	34
Configuring the Discovery Scopes .....	40
Adding Discovery Seeds .....	43
Enabling or Disabling Polling for a Device Class .....	45
Initiating Discovery .....	46
Monitoring the Discovery Process .....	47
Viewing the Discovery Log .....	48
Configuring Discovery .....	49
The NetVoyant Discovery Process .....	49
Configuration Settings that Affect Discovery and Polling .....	51
Configuring Discovery Options .....	52
Configuring Interface Types .....	57
Configuring Device Classes and Models .....	59
NetVoyant Device Classifications .....	60
Adding or Editing a Device Model .....	63
Enabling or Disabling Polling for a Device Model .....	64
Troubleshooting NetVoyant Configuration .....	65

## CHAPTER 3

<b>Configuring Data Collection and Retention</b> .....	<b>67</b>
NetVoyant Data Collection and Storage .....	68
Data Organization by Poll Instance .....	68
Viewing and Configuring Data by Poll Instance .....	69
Managing Dataset Properties .....	71
Editing Dataset Details .....	71
Managing Discovery for a Dataset .....	74
Naming Poll Instances and Interfaces .....	78
Creating and Configuring Custom Datasets .....	80
Using the Dataset Wizard to Create a New Dataset .....	80
Selecting a MIB in the Dataset Wizard .....	81
Adding Expressions in the Dataset Wizard .....	82
Adding Polling Groups in the Dataset Wizard .....	84
Enabling and Disabling Polling .....	85
Disabling Polling for Devices .....	85
Configuring Polling Settings .....	85

Enabling and Disabling Polling for Datasets .....	86
Using Auto-Enable Polling .....	88
Monitoring Polling .....	92
Configuring Data Collection Frequency .....	94
Configuring the Frequency for Polling and Rollups .....	94
Creating or Editing a Polling Group .....	94
Changing the Default Polling Group for a Dataset .....	96
Creating or Editing an Interval .....	97
Configuring Data Rollup and Retention .....	99
Configuring Time Filter Definitions .....	101
Restricting Database Storage .....	103
Configuring What Data to Gather .....	104
Using Expressions to Gather Data .....	104
Using Baselines .....	108
Using Dataset Properties .....	111
Using Data Validation Rules .....	112
<b>CHAPTER 4</b>	
<b>Managing Your Devices and Networks</b> .....	<b>115</b>
Manually Adding Networks and Devices .....	116
Adding a Network .....	116
Adding a Device .....	116
Working with NetVoyant Groups .....	118
Default NetVoyant Groups .....	118
Groups in the NetVoyant Console .....	118
Groups in the Reporting Interface .....	120
Group Membership .....	121
Adding Devices, Poll Instances, or Interfaces to Groups .....	125
Managing Devices In NetVoyant .....	130
Managing Device Polling and Maintenance .....	130
Configuring Details for a Device .....	135
Configuring Devices in the NetVoyant Console .....	147
Managing Device Discovery .....	150
Using the Find Utility to Locate Devices .....	154
Starting a Telnet Session with a Device .....	155
Performing a Ping or Traceroute .....	155

Configuring Protocol Data.....	157
Adding an RMON2 Probe .....	157
Viewing Details for an RMON Protocol Distribution.....	157
Editing an Application Group or Protocol Group .....	159
Adding or Removing a Protocol from a Protocol Group .....	160
Working with Poll Instances and Interfaces.....	161
Polling Status and Expiration .....	161
Viewing and Editing Poll Instance and Interface Details .....	162
Viewing and Acknowledging Alarms.....	167
Deleting All Data for a Poll Instance or Interface .....	169
Managing Device Interfaces .....	170

## **CHAPTER 5      Working with Management Information Bases      177**

Using MIBs for Data Collection.....	178
MIB Structure.....	178
MIB Object Identifiers .....	179
Viewing MIBs in the NetVoyant Console.....	179
Using the MIB Browser .....	182
Opening the MIB Browser .....	182
Configuring What the MIB Browser Displays .....	183
Performing an SNMP Query in the MIB Browser.....	184
Viewing a Real-Time Graph .....	184
Adding MIBs to the NetVoyant Product.....	185
Determining MIB Dependencies .....	185
Compiling New MIBs into the NetVoyant Product.....	187

## **CHAPTER 6      Managing NetVoyant Events and Alarms      189**

Using Events and Alarms.....	190
Event and Alarm Tasks .....	190
Using Alarm Profiles .....	191
Working with Alarm Rules .....	199
Using Dataset Expressions in Thresholds.....	206
Creating Dynamic Thresholds and Expressions.....	208
Working with Event and Alarm Logs .....	209
Viewing the Log Panels .....	209
Viewing Details for an Event or Alarm.....	211

	Viewing the Source of an Event or Alarm.....	215
	Saving Log Files to a CSV File .....	216
	Editing the Alarm Log Colors.....	217
	Acknowledging an Alarm.....	218
	Clearing an Event or Alarm from the Log Panel.....	219
	Viewing Cleared Events or Alarms.....	220
	Deleting Events or Alarms from the Database .....	220
	Displaying Fewer Logs in the Log Panels.....	221
	Filtering the Events and Alarms in the Log Panels.....	221
	Configuring Event Severities .....	224
<b>CHAPTER 7</b>	<b>Managing Notifications</b>	<b>225</b>
	Using NetVoyant Notifications .....	226
	Notification Types.....	226
	Database Notifications.....	227
	Creating a Notification.....	227
	Enabling or Disabling a Notification .....	229
	Notification Configuration Parameters.....	230
	Examples for Using Notifications.....	237
	Selecting the Events that Trigger a Notification.....	240
	Writing an Event Filter Expression.....	241
	Triggering Notifications by Device Availability.....	242
	Triggering Notifications by Operational Status.....	243
	Triggering Notifications for a Threshold Event .....	243
	Triggering Notifications by Device Name or Address .....	244
	Triggering Notifications for Incoming SNMP Traps .....	246
	Triggering Notifications by Event Timestamp .....	246
	Triggering Notifications by Event Severity .....	247
	Triggering Escalated Notifications by Event Severity.....	247
	Triggering Notifications for Sustained Events .....	248
	Calculating Sustained and Spike Events .....	248
	Using Polling Notification Limits .....	249
	Using the Event Duration Property .....	252

<b>CHAPTER 8</b>	<b>Configuring IP SLA Operations</b>	<b>255</b>
	NetVoyant Support for Cisco IP SLA.....	256
	Configuring IP SLA Operations.....	258
	Selecting Source Routers for IP SLA Operations.....	259
	Setting Target Addresses for IP SLA Operations.....	260
	IP SLA Test Configuration Settings.....	261
	ICMP Echo Test Configuration Settings.....	261
	Path Echo Test Configuration Settings .....	261
	UDP Echo Test Configuration Settings.....	262
	TCP Connect Test Configuration Settings .....	263
	HTTP Echo Test Configuration Settings .....	263
	DNS Test Configuration Settings.....	264
	UDP Jitter Test Configuration Settings .....	264
	VoIP Jitter (Enhanced UDP) Test Configuration Settings .....	265
	DHCP Test Configuration Settings .....	267
	FTP Test Configuration Settings .....	268
	Viewing and Editing IP SLA Operations.....	269
	Disabling Polling for an IP SLA Operation .....	271
	Using the IP SLA Import Utility .....	272
	IP SLA Import XML File Format .....	273
<b>CHAPTER 9</b>	<b>Managing NetVoyant Services</b>	<b>279</b>
	About the NetVoyant Services .....	280
	Managing NetVoyant Services.....	281
	Starting and Stopping Services .....	281
	Starting and Stopping Individual Services on the Services Tab .....	281
	Starting or Stopping All Services .....	282
	Configuring a Service's Start Mode or Logging Level.....	283
	Configuring Event Log Retention .....	284
<b>CHAPTER 10</b>	<b>Reporting Administration</b>	<b>287</b>
	Changing Your User Account Password.....	288
	Configuring Email Servers and Schedules .....	289
	Adding an SMTP Server .....	289
	Viewing, Editing, or Deleting an Email Schedule.....	290



	Editing the Report Menus.....	292
	Configuring Global Settings.....	294
	Working with Roles and User Accounts .....	295
	NetVoyant Default Roles .....	295
	Adding and Editing Roles .....	296
	Adding or Editing a NetVoyant User .....	299
	Changing User Permission Groups.....	301
	Proxying a User Account.....	302
	Adding Pages to a User's My Pages Menu .....	303
	Proxying a Role .....	304
<b>APPENDIX A</b>	<b>NetVoyant Properties and Operators</b>	<b>307</b>
	Working with NetVoyant Properties .....	308
	Using Properties in Dataset Expressions.....	308
	Using Properties in Notifications .....	309
	Using Event Properties .....	314
	Adding, Viewing, or Setting Values for Properties.....	316
	Using NetVoyant Operators in Expressions .....	319
<b>APPENDIX B</b>	<b>Managing NetVoyant SNMP Traps</b>	<b>323</b>
	Working with NetVoyant SNMP Traps.....	324
	Configuring How the NetVoyant Product Receives SNMP Traps .....	324
	Configuring an External Source to Receive NetVoyant Traps.....	324
	Creating a Notification for Incoming SNMP Traps .....	325
	Configuring a Trap Notification .....	325
	Adding or Editing an SNMP Trap Event.....	325
	Including Dynamic Content in SNMP Trap Events.....	328
	Using Variable Bindings.....	330
	Determining Variable Bindings from a MIB Trap Definition .....	330
	Syntax for Referencing Variable Bindings .....	331
	Determining Appropriate Values for Variable Bindings.....	331
	<b>Index</b>	<b>333</b>



---

# About This Document

---

NetQoS NetVoyant is a powerful performance analysis and reporting software package that automates the collection, analysis, and reporting of critical device data. Using Simple Network Management Protocol (SNMP), the NetVoyant product automatically polls and correlates data from devices installed on your network. Data from routers, switches, servers, RMON2 probes, frame relay circuits, logical segments, and wide area links are collected and organized to give you real information about your network. You can easily identify trends and issues before they become problems.

This document provides information and procedures to help you perform administrative tasks in the NetVoyant product effectively.

Chapter	Description
Chapter 1, “NetVoyant System Setup” on page 15	Introduces you to NetVoyant administration in the NetVoyant Console.
Chapter 2, “Configuring Your NetVoyant System” on page 31	Describes how to use the Configuration Wizard to perform the initial configuration of the NetVoyant product.
Chapter 3, “Configuring Data Collection and Retention” on page 67	Describes how to manage datasets and configure how the NetVoyant product collects and retains SNMP data from your devices.
Chapter 4, “Managing Your Devices and Networks” on page 115	Describes how to manage groups, devices, poll instances, and interfaces in the NetVoyant Console.
Chapter 5, “Working with Management Information Bases” on page 177	Describes how to use Management Information Bases (MIBs) in the NetVoyant Console to control what types of SNMP data NetVoyant can collect from your devices.
Chapter 6, “Managing NetVoyant Events and Alarms” on page 189	Describes how to manage NetVoyant events and alarms and how to view information in event logs.
Chapter 7, “Managing Notifications” on page 225	Describes how to configure and manage notifications that the NetVoyant product sends in response to events on your network.
Chapter 8, “Configuring IP SLA Operations” on page 255	Describes how to configure Cisco IOS IP SLA operations for your Cisco devices using the IP SLA Wizard.
Chapter 9, “Managing NetVoyant Services” on page 279	Describes how to start and stop NetVoyant services and configure database logging.
Chapter 10, “Reporting Administration” on page 287	Describes administration tasks in the NetVoyant reporting interface, such as adding NetVoyant user accounts and configuring an SMTP server.

Chapter	Description
<a href="#">Appendix A, “NetVoyant Properties and Operators” on page 307</a>	Describes NetVoyant properties and operators, which you can use when writing expressions and thresholds.
<a href="#">Appendix B, “Managing NetVoyant SNMP Traps” on page 323</a>	Describes how to configure the NetVoyant product to send and receive SNMP traps.

## RELATED DOCUMENTATION

In addition to this book, you can find useful information in the following publications:

Document	Description
<i>NetVoyant User Guide</i>	This guide provides information and procedures to help you effectively use the NetVoyant reporting interface.
NetVoyant v7.0 Release Notes	Summarizes product enhancements, fixes, and open issues.
NetVoyant v7.0 online Help	Provides context-sensitive help for tasks that you perform through the NetVoyant Console and web reporting tool.

You can access the product documentation in the following ways:

- In the NetVoyant web reporting tool, navigate to the **About** page in the product and click the **User Guide** link.
- Navigate to the **Documentation** directory on the server, which contains the PDF files for both the User Guide and Administrator Guide, as well as supplemental documentation.

The product documentation is available in PDF format on the server where the NetVoyant product is installed. Find the PDF files in the following location:

D:\NetVoyant\Portal\WebSite\Docs

- On the desktop of the server, find shortcuts that link to the User Guide and Administrator Guide PDF files.

The current versions of the PDF files for the product documentation, including the *Release Notes*, are always available on the NetQoS Self-Service Portal.

## CONVENTIONS

The following conventions are used in this book:

- In instructional text, **boldface** type highlights information that you enter or GUI elements that you select.
- All syntax and literal examples are presented in monospace typeface.
- In syntax, path names, or system messages, text enclosed in angle brackets (<>) represents a variable as shown in the following example:  
net time/setsntp: <ntpserver>

## PROVIDING DOCUMENTATION FEEDBACK

We want to help you use our products effectively so that you can work quickly and efficiently. By telling us about your experience with this document, you can help us achieve that goal. Send an email message with your feedback to our technical publications team at the following address:

[docfeedback@netqos.com](mailto:docfeedback@netqos.com)



# NetVoyant System Setup

---

The NetVoyant product is a powerful performance analysis and reporting software package that automates the collection, analysis, and reporting of critical device data. Using Simple Network Management Protocol (SNMP), it automatically polls and correlates data from devices installed on your network. Data from routers, switches, servers, RMON2 probes, frame relay circuits, logical segments, and wide area links are collected and organized to give you real information about your network. You can easily identify trends and issues before they become problems.

This chapter provides information about the initial installation and configuration of the NetVoyant product and provides helpful tips and tricks for working in the NetVoyant Console.

This chapter covers the following topics:

- “NetVoyant Architectural Overview and Licensing” on page 16
- “About the Master Server and Pollers” on page 21
- “Operational Requirements” on page 17
- “About NetVoyant Administration” on page 23

## NETVOYANT ARCHITECTURAL OVERVIEW AND LICENSING

The NetVoyant product can operate on a single server (standalone system) or on multiple servers (distributed system). To determine which of these systems is best for your organization, you must consider the overall structure of your network, the devices you want to discover, and the licensing requirements.

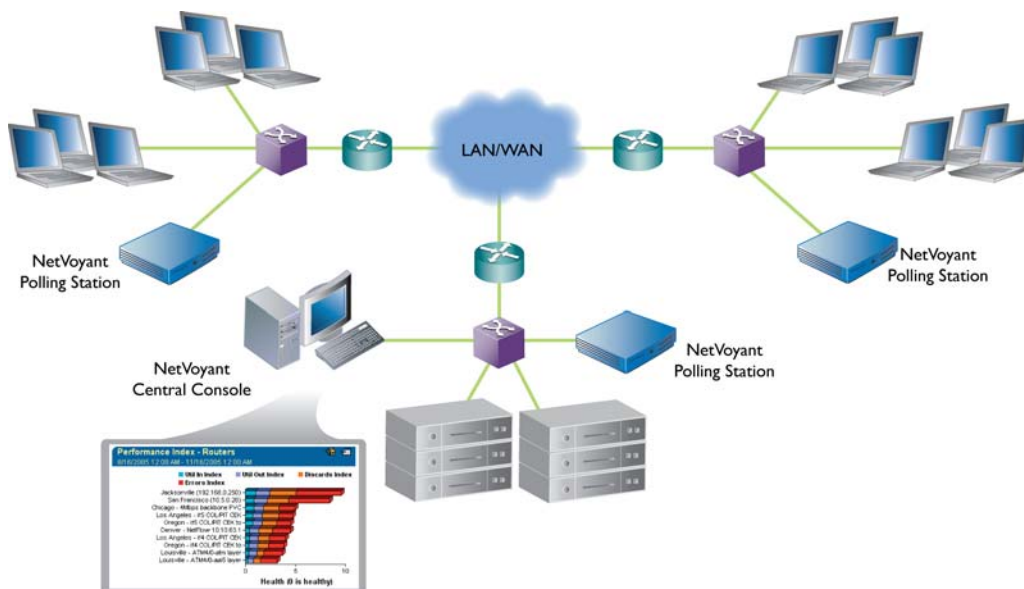
### NetVoyant Standalone System

In a standalone configuration, you set up one NetVoyant server called the Master. All administration, reporting, and polling takes place on the Master server. For a standalone NetVoyant system, there is one license for the entire system.

### NetVoyant Distributed System

In a distributed system, also known as NetVoyant Enterprise, you set up a central server for administration and reporting called the Master. You then set up remote servers, called *pollers*, from which the NetVoyant system discovers and polls the devices on your network. In distributed systems, there is a license for the Master and separate licenses for each poller. The Master has a poll instance license limit of zero poll instances and each poller has a limit according to the number of poll instances that it is licensed to poll.

Using remote pollers in a distributed system makes it possible to monitor several remote data centers and their associated LANs while preserving bandwidth. These remote servers poll and aggregate data on a local level, and the data is retrieved by the central station and a network operations view of the entire network can be seen. Conversely, when an alarm is received from a remote location, network operations staff has the capability to drill down from data maintained on the central server to poll-rate data at the remote site.





## Operational Requirements

NetVoyant servers require 24-hour access to network devices. The computer should not be powered down during off hours. For optimum performance, the network devices should be accessible through LAN rather than WAN connections whenever possible.

Networking services must be configured and enabled for the software to operate correctly. This includes TCP/IP and all configuration parameters. Access to a naming service, such as DNS, is essential for the presentation of devices through the NetVoyant user interface components.

Many routers and other network connectivity devices require that the address of the “Manager” nodes that will be polling the device be entered into the device’s access list. The access list typically contains a list of trusted hosts that the device responds to via SNMP. Configuration of the access list is typically performed via a proprietary interface to the device. Contact your device manufacturer for questions about adding the NetVoyant host to the access list.

**SNMP Profiles.** SNMP profiles are used by SNMP Agents to verify the identity of requesting managers. The NetVoyant product needs to know the read profiles supported by your network devices for these devices to respond to discovery and polling. If you plan to configure IP SLA tests, both the read and write profiles are required. The NetVoyant Console supports authentication to devices using SNMPv1, SNMPv2, and SNMPv3.

**Network Addresses and Masks.** You will need to know about your network addresses and address masks. It is important to “scope” the discovery process to those address spaces that you want to manage. A network address (address space) is a network number such as 205.195.82.0. A network mask for such an address might be 255.255.255.0. This example defines a Class C address space. Normally, this example would be denoted as 205.195.82.0/24, with the /24 signifying the number of bits dedicated to the network address.

**Seed Devices for WAN Discovery.** You might need to know the names or addresses of gateway or backbone routers or other connectivity devices to provide the NetVoyant product with a “seed” device. Seed devices are necessary when discovering networks that are separated from the NetVoyant host via a public network or when a gateway router is not discoverable because of problems with access lists or profiles. In these cases, NetVoyant will target discovery of network nodes through these seed devices.

## NetVoyant Licensing

Your NetVoyant license allows you to enable a set number of poll instances. The number of poll instances that you have enabled in the NetVoyant product affects the amount of data that you can collect from your devices.

In order to increase the number of poll instances that your NetVoyant system can poll, you must upgrade your license; however, you can attempt other methods for managing your current license limit of poll instances before requesting an upgrade. For more information about poll instances, see [“Data Organization by Poll Instance”](#) on page 68.

Some NetVoyant products are licensed using a pre-configured USB HASP (Hardware Against Software Piracy) according to the number of enabled poll instances in your environment. If you are running the NetVoyant product under a HASP license, you must plug in the HASP before you boot the NetVoyant machine for the first time.

**Important:** If you do not have the correct HASP or need an updated or upgraded license, contact NetQoS Technical Support.

### Licensing Differences Between Standalone and Distributed Systems

For a standalone NetVoyant system, there is one license with a maximum number of poll instances for the entire system; however, in larger distributed NetVoyant systems, there is a license for the Master server and separate licenses for each poller. By default, the Master has a license limit of 0 poll instances and each poller has a limit according to the number of poll instances that it is licensed to poll.

### Viewing Your License Information

If you are considering whether you need additional NetVoyant licensing, you can open the **License Information** dialog box to view the license information for your system. This dialog box displays the number of discovered poll instances that are enabled and also the number of instances for which you are licensed on each server in your system. Using this dialog box, you can track your licensing status and requirements.

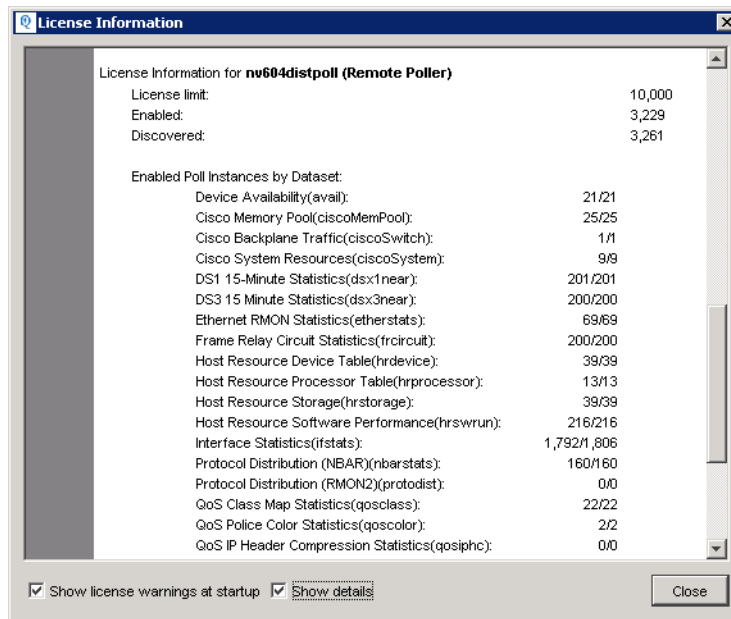
#### To view information about your NetVoyant license:

1. From the **File** menu in the NetVoyant Console, select **License Info**.

The **License Information** dialog box opens.

2. Select the **Show details** check box at the bottom of the dialog box to view detailed information about how poll instances are enabled and discovered by dataset.

For example, license information for Interface Statistics (`ifstats`) reported as “1,792/1,806” indicates that there are 1806 discovered poll instances for this dataset, but only 1792 are enabled.



If you view your license information for a distributed system, the dialog box displays a 0 poll instance license for the Master Console and details about poll instance limits and usage for each of the remote pollers.

You can enable and disable poll instances from the NetVoyant Console to comply with your license agreement. For more information, see [“Managing Poll Instances” on page 20](#).

**Note:** It is possible to see a higher number of discovered poll instances than enabled poll instances even if you have not disabled any. In this situation, there is one or more discovered poll instances that has no associated dataset and acts as a parent to one or more enabled poll instances. The NetVoyant product does not collect data for these parent poll instances and does not count them towards your license total; therefore, they are discovered but not enabled.

## Licensing by Poll Instance

Your NetVoyant license allows you to enable a set number of poll instances in the NetVoyant product. The number of poll instances that you have enabled affects the amount of data that you can collect from your devices.

In order to increase the number of poll instances that your system can handle you might need to upgrade your NetVoyant system as well as purchase a larger license. However, you should attempt to employ other methods for managing your current license limit of poll instances before requesting an upgrade.

For more information about managing your poll instances and reduce collection of non-essential data, see [“Managing Poll Instances” on page 20](#).

If you need an upgraded license, please contact NetQoS Technical Support.

## Disabling License Warnings

At startup, the NetVoyant Console displays warnings when you are close to exceeding your license limit of poll instances, or have exceeded it. You can disable this option if you no longer want to see these messages.

### To disable license warnings:

1. From the **File** menu in the NetVoyant Console, select **License Info**.  
The **License Information** dialog box opens.
2. Disable the **Show license warnings at startup** check box at the bottom of the dialog box.
3. Click **Close**.

## Managing Poll Instances

Most datasets and device classes are enabled for polling by default. If there are enabled poll instances that you do not need and you want to make poll instance licenses available for those that you do need, you can disable polling for the following items in the NetVoyant Console to reduce the number of currently enabled poll instances in your NetVoyant system:

Disable polling for...	More information
<b>Datasets</b> for which you are not interested in displaying reports.	"Enabling and Disabling Polling for Datasets" on page 86
<b>Groups</b> for which you are not interested in displaying reports.	"Configuring Polling for a Group" on page 123
<b>An entire network</b> for which you are not interested in displaying reports.	"Configuring Polling for a Group" on page 123
<b>Device classes or device models</b> for which you are not interested in displaying reports.	"Configuring a Polling Group for a Network" on page 124
<b>Individual devices</b> for which you are not interested in displaying reports.	"Changing the Polling Status for a Device" on page 148
<b>Interface types</b> for which you are not interested in displaying reports.	"Performing Mass Operations by Interface Type" on page 173
<b>Individual interfaces or poll instances</b> for which you are not interested in displaying reports.	"Configuring Polling for Poll Instances and Interfaces" on page 166
<b>IP SLA operations</b> for which you are not interested in displaying reports.	"Disabling Polling for an IP SLA Operation" on page 271
<b>Non-operational interfaces.</b>	"Disabling Polling for Non-Operational Interfaces" on page 91
<b>Interfaces that do not have any traffic.</b>	"Disabling Polling for Interfaces without Traffic" on page 92

## Contacting Technical Support

If you have questions about the NetVoyant product or would like to upgrade your license, go to the technical support page at:

<http://www.netqos.com/support/>

This page provides the latest contact information for the Technical Support team.

If you do not have access to the Internet, use one of the following telephone numbers:

- United States or Canada: (877) 835-9575; Option 3.
- Outside the United States or Canada: (512) 407-9443; Option 3.

## ABOUT THE MASTER SERVER AND POLLERS

The Master is the central NetVoyant server. In a standalone system, all administration, reporting, and polling is done on or by the Master. In a distributed system, there is a central server for administration and reporting called the Master and you then set up remote servers called pollers, which discover and poll your network.

### Adding Remote Pollers to a NetVoyant Distributed System

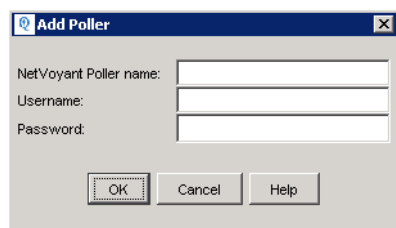
After you configure the Master server in a distributed system, you must add and configure the remote servers, called *pollers*, that discover and poll the devices on your network. You can add up to 15 pollers per Master.

**Important:** Many NetVoyant configuration tasks must take place on the Master server. Configuration changes are synced from the Master to each connected poller. If configuration changes occur on the Master when a poller is operationally down, the change will be synced to the poller when communication with the Master is restored.

#### To add a poller to the Master:

1. Install the NetVoyant product on the poller server.
2. Open the NetVoyant Console application on the Master.
3. From the **File** menu, select **New > NetVoyant Poller**.

The **Add Poller** dialog box opens.



4. Enter the following parameters:

Parameter	Description
<b>NetVoyant server name</b>	The poller's IP address or fully qualified DNS name.
<b>Username</b>	The username used to log in to the NetVoyant Console on the poller. You can use the <b>nvadmin</b> user name, which is set as an administrator user account by default.
<b>Password</b>	The password used to log in for the user account on the poller. If you are using the <b>nvadmin</b> user account, the password is set to <b>nv</b> by default.

5. Click **OK**.

You can repeat this process for each poller that you want to add to the Master.

## Configuring a Poller

After you add a poller to the NetVoyant Master server, you can assign devices to the poller from the NetVoyant Console on the Master using the Configuration Wizard. You can change the assigned poller for the existing items in the discovery scopes and discovery seeds lists, or add new items and assign them to the new poller.

**Important:** Many NetVoyant configuration tasks must take place on the Master server. Configuration changes are synced from the Master to each connected poller. If configuration changes occur on the Master when a poller is operationally down, the change will be synced to the poller when communication with the Master is restored.

### To configure the pollers on the Master:

1. From the **Tools** menu, select **Configuration Wizard**.
2. Step through the wizard and complete the steps to specify the poller assigned to each item in the discovery scopes and discovery seeds.

For more assistance with this step, see [“Using the Configuration Wizard” on page 33](#).

## Adding a Poller as Trusted Site

After you have configured the Master server and the pollers, you must add these servers as trusted sites in Internet Explorer on the Master. This enables the NetVoyant reporting interface on the Master server to display data from these servers.

### To add a poller as a trusted site in Internet Explorer:

1. On the Master, open the Internet Explorer browser.
2. In Internet Explorer, select **Tools > Internet Options**.  
The **Internet Options** dialog box opens.
3. Click the **Security** tab.
4. Click the **Trusted sites** icon.

5. Click **Sites**.
6. Clear the **Require server verification** check box.
7. Enter the IP address of the poller.
8. Click **Add**.
9. Repeat steps 7 and 8 for each poller.
10. Click **OK**.

## ABOUT NETVOYANT ADMINISTRATION

Most NetVoyant administrative tasks are performed in the NetVoyant Console. Only user accounts with the Administrator role can make configuration changes in the NetVoyant Console. An administrator typically performs the following tasks:

Task	Description	Page
Configure NetVoyant	When you first start the NetVoyant Console, you must configure how the NetVoyant product discovers and polls your devices and networks. Use the Configuration Wizard to streamline this process.	31
Manage devices and networks	The NetVoyant product automatically adds the devices and networks that it discovers to the groups shown on the <b>Group</b> tab of the NetVoyant Console; however, you can manually add devices and networks and implement custom groups to assist with management and reporting.	115
Manage MIBs	The NetVoyant product uses SNMP Management Information Bases (MIBs) to define the types of data it can collect from your devices and how it collects that data. You can view these MIBs to assist in creating event notifications or other administrative tasks or you can compile new MIBs to add functionality to the NetVoyant product.	177
Manage events and alarms	The NetVoyant product uses events and alarms to alert you to issues with NetVoyant Services as well as missed SNMP polls, exceeded utilization, or other configurable thresholds on critical devices. As an administrator, you can set thresholds, create notifications that are triggered in response to events, and view event and alarm logs.	189
Configure IP SLA operations	In the NetVoyant Console, you can use the IP SLA Wizard to configure Cisco IP SLA operations for devices that support them. These operations provide data for IP SLA reports in the NetVoyant reporting tool and the NetQoS Performance Center.	255
Manage NetVoyant services	As an administrator, you can manage the processes generated by the NetVoyant product to assist with troubleshooting. You can also configure the alarm logging level for NetVoyant Services.	279

Task	Description	Page
Administer reporting and user accounts	In the NetVoyant web reporting tool, you can configure access to the collected and stored data displayed in NetVoyant reports. You can also control access to specific reports and create custom views for NetVoyant data.	287

## Using the NetVoyant Console

The NetVoyant Console is the central administrative interface for the NetVoyant product. Within the NetVoyant Console, you configure how NetVoyant discovers, polls, and groups your SNMP-enabled devices and networks. In the NetVoyant Console, you can also configure what type of data NetVoyant gathers and how that data is stored in datasets.

### To open and log into the NetVoyant Console:

1. From the **Start** menu, select **All Programs > NetVoyant > NetVoyant Console**.
2. Enter the username (user account) and password.

When you first set up your NetVoyant system, you can log in to the NetVoyant Console with the default login:

username: nvadmin

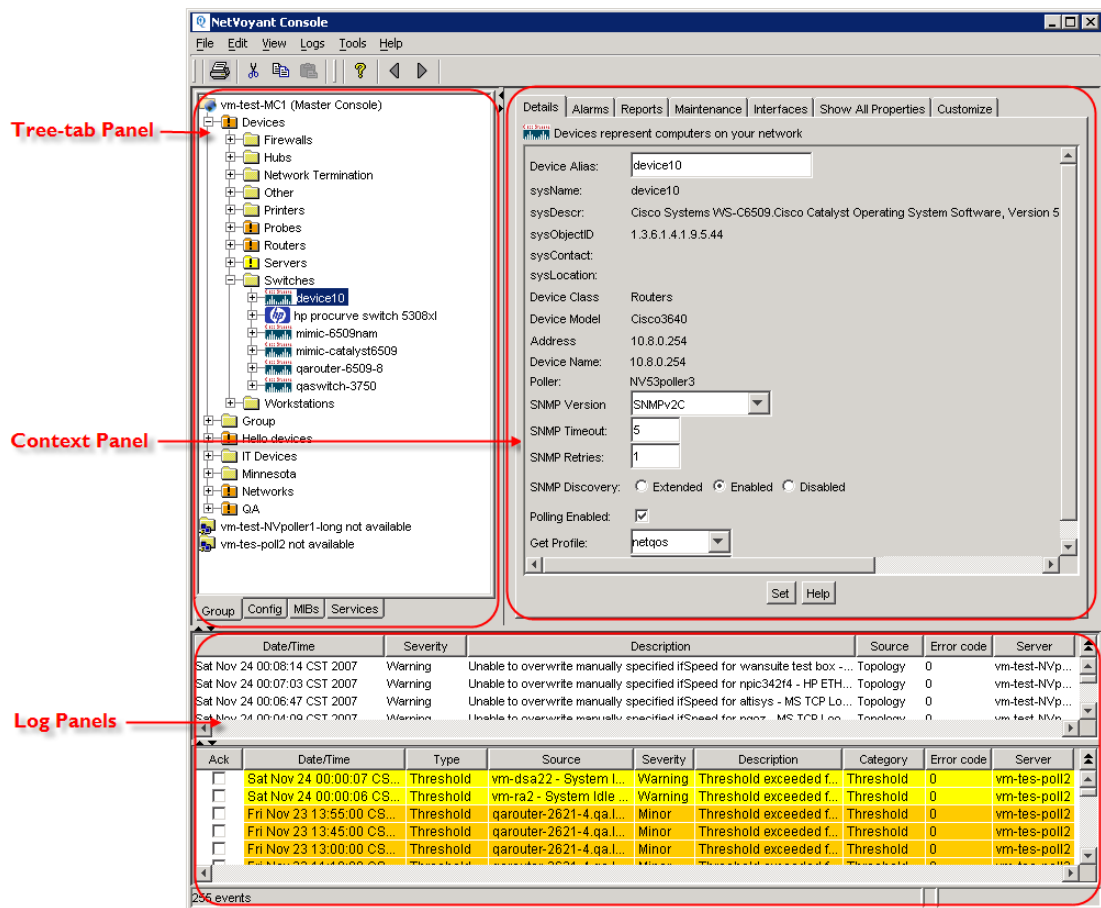
password: nv



### The NetVoyant Console Interface

On the left side of the NetVoyant Console is a tabbed panel called the tree-tab panel. On the right side is a panel called the context panel. Selecting tabs and items in the tree-structures on the tree-tab panel changes the information that appears in the context panel. For example, when you select a device on the **Group** tab in the tree-tab panel, the context panel displays information about the selected device.





## The Tree-Tab Panel

The tree-tab panel on the left-hand side of the NetVoyant Console is divided into four tabs:

Tab	Description	Page
<b>Group</b>	Use this tab to view and configure your networks and devices, which are organized according to default and customized groups.	118
<b>Config</b>	Use this tab to perform configuration tasks such as determining how the NetVoyant product discovers and polls your devices and networks. You can also set thresholds and notifications for your devices.	32
<b>MIBs</b>	Use this tab to view the Management Information Bases (MIBs) compiled into the NetVoyant product. These MIBs determine the type of data that can be collected.	177
<b>Services</b>	Use this tab to stop, start, and change the logging level for NetVoyant Services, which are the processes that make up the NetVoyant product.	279

## The Log Panels

You can choose to display the Event and Alarm Log panels at the bottom of the NetVoyant Console. These panels display current event and alarm logs as triggered by service logging, missed polls, and database notifications of threshold events. For more information, see [“Working with Event and Alarm Logs” on page 209](#).

You can also view the Discovery Log window, which displays logs related to the discovery process. For more information, see [“Configuring Discovery” on page 49](#).

## The Context Panel

You can customize the tabs that are shown in the context panel for an object in the NetVoyant Console. By displaying hidden tabs, you can view more information about the selected object. By hiding tabs, you can restrict the tabs displayed in the context panel to only those that you need to access.

### To display, hide, or reorder tabs in the context panel:

1. Select the object in the tree-tab panel to view the object’s details in the context panel.

For example, to set the properties for a router, expand the poller, expand **Devices > Routers**, and select the router.

2. Click the **Customize** tab in the context panel.

3. You can perform the following actions:

- To display a hidden tab, select the **Show/Hide** check box for the **Tab Panel Title**.
- To hide a tab, clear the **Show/Hide** check box for the **Tab Panel Title**.
- To change the order of the displayed tabs, select a tab panel title and click **Raise** or **Lower**.

**Note:** You cannot hide the **Customize** tab.

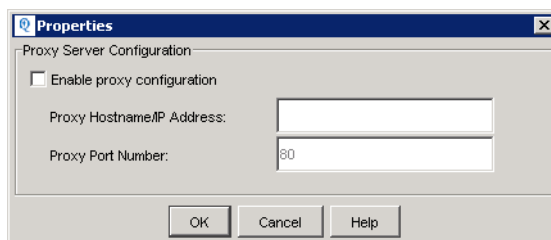
## Configuring NetVoyant Console Properties

You can configure proxy server properties for the NetVoyant Console, such as the proxy server for the NetVoyant Console to access HTML pages. This is an optional configuration setting.

### To configure the NetVoyant Console options:

1. From the **File** menu in the NetVoyant Console, select **Properties**.

The **Properties** dialog box opens.



2. Edit the following parameters:

Parameter	Description
<b>Enable proxy configuration</b>	Select this check box to enable NetVoyant to access HTML files through a proxy server.
<b>Proxy Hostname/IP Address</b>	The hostname or IP address of the proxy server.
<b>Proxy Port Number</b>	The port number of the proxy server.

3. Click **OK**.

## Opening Reports from the NetVoyant Console

You can access NetVoyant reports for a selected group, device, poll instance, or interface directly from the NetVoyant Console. You can also open the NetVoyant reporting tool from the NetVoyant Console to view all NetVoyant reports, or open the NetQoS Performance Center from the NetVoyant Console to view cross-product reports.

### To open the NetVoyant reporting tool from the NetVoyant Console:

- From the **Tools** menu, select **NetVoyant Reporting**.

**Note:** For more information about viewing reports in the NetVoyant reporting tool, see the *NetVoyant User Guide*.

If your NetVoyant system is registered as a data source with the NetQoS Performance Center, you can view NetVoyant data as well as data from the other NetQoS data source products in the NetQoS Performance Center web interface.

### To open the NetQoS Performance Center from the NetVoyant Console:

- From the **Tools** menu, select **NetQoS Performance Center**.

### Viewing the Reports Available for an Object in the NetVoyant Console

In the NetVoyant Console you can view a list of the NetVoyant reports that are currently available for a selected device. Use this information to determine which reports will be affected if you disable polling for a device or make other changes to the device's configuration in the NetVoyant Console.

### To view the reports available for a selected object:

1. On the **Groups** tab, expand the tree structure to locate the object.
2. Select the object.

The object's details appear in the context panel.

3. Click the **Reports** tab.

This tab displays a list of NetVoyant reports available for the selected object.

**Note:** If the Reports tab does not appear in the context panel, click the **Customize** tab and select the **Reports** tab for display.

4. If you want to launch the reporting tool and view the report using the selected object as the context, select a report in the list and click **Display**.

The NetVoyant reporting tool displays the selected report in a browser window.

**Note:** For groups, you can open additional reports from the NetVoyant Console according to type. To view these reports, click the tabs that correspond to the report menus in the NetVoyant reporting tool. Select a report to see the report page for the selected group.

## Scheduling Command Line Tasks from the NetVoyant Console

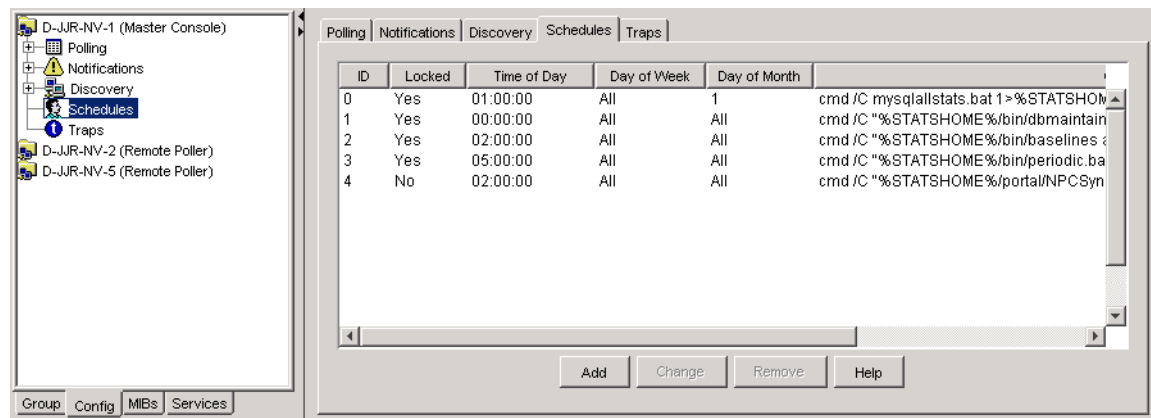
The NetVoyant product includes a scheduling feature so that various tasks can be performed on a repeated basis, at specific times of the day and on a particular day of the week or month. It can also support daily tasks.

**Note:** Tasks that are required for NetVoyant system functioning are locked by default and cannot be modified.

### To add or change a scheduled task:

1. On the **Config** tab, select the **Schedules** object.

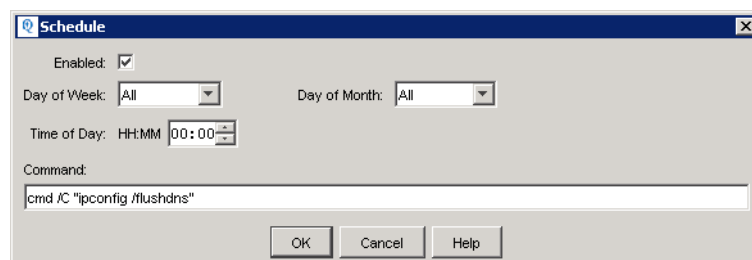
The scheduled tasks appear in the context panel.



2. Do one of the following:

- To add a new task, click **Add**.
- To change a task definition, select the task in the list and click **Change**.

The **Schedule** dialog box opens.



- Set the parameters to define the scheduled task:

Parameter	Description
<b>Enabled</b>	Select this check box to enable the task so that it is executed according to its schedule.
<b>Day of Week</b>	Use this setting to specify a day for a weekly task. Leave the default ( <b>All</b> ) if all days of the week are valid.  When both <b>Day of the Week</b> and <b>Day of the Month</b> are set to <b>All</b> , it specifies a daily task.
<b>Day of Month</b>	Use this setting to specify a date of the month for a monthly task. Leave the default ( <b>All</b> ) if all dates in the month are valid.
<b>Time of Day</b>	Use this setting to specify a time of day to execute the command line task. This setting uses a HH:MM format. Click the HH in the field and use the arrow buttons to adjust the specified hour up or down. Do the same for the minutes (MM).
<b>Command</b>	In this field, enter the command that will be executed.

- Click **OK**.

## Installing a Remote NetVoyant Console

A remote NetVoyant Console can be installed on a standard desktop or laptop. This utility enables you to remotely configure the NetVoyant system without using a terminal session to gain access to the NetVoyant Console on the main server. There are no additional licenses required to use the remote NetVoyant Console application.

The installer for the NetVoyant Console is located with your NetVoyant server as:

```
d:/NetVoyant/netvoyant-console-x.x.x-win32-i586..exe
```

where **d:** is the drive on which NetVoyant is installed and **x.x.x** is the version number of the NetVoyant Console Installer.

### To install the remote NetVoyant Console:

- Copy the installer (the full executable) to the target workstation or laptop.
- On the workstation or laptop, double-click the installer to start the installation process.  
You should see cab files being expanded and then an Install Shield window.
- Step through the process using the **Next>** button.
- At the DNS hostname or IP address prompt, enter the fully qualified DNS name or the IP address of the NetVoyant Master or standalone server.

When the main NetVoyant server is upgraded, you should also update Console-only desktops or laptops with the installation kit copied to the main server during the upgrade.

## Maintaining the NetVoyant Database

You should perform a backup of the NetVoyant database on a monthly basis. All of the NetVoyant data is stored under the D:\NetVoyant\db\nms2 directory.

**Important:** It is strongly recommended that you stop the web server and the NetVoyant services when backing up or restoring the database to ensure data consistency. For more information about stopping NetVoyant services, see [“Starting or Stopping All Services” on page 282](#).

### NetQoS Database Tools Suite

The NetQoS Technical Support team distributes and maintains the NetQoS Database Tools Suite on the NetQoS Self Service Portal. The NetQoS Database Tools Suite contains a bundle of small, efficient, and feature-rich tools that interact with the MySQL databases on most NetQoS products. These tools have been developed to ease the administration overhead of database backups, optimization, and repairs, as well as provide a way to restore an existing backup. It also includes a user administration tool for creating MySQL user accounts with SELECT-only rights for accessing/exporting data.

To download and install the NetQoS Database Tools Suite, log into the NetQoS Self Service Portal, navigate to the **Support > Support Tools** page, and click the NetQoS Database Tools Suite link.

# Configuring Your NetVoyant System

---

The NetVoyant product includes a number of flexible configuration options that you can use to determine how it discovers and polls your devices and networks. You can also configure how the NetVoyant database stores related data and the display of data in NetVoyant reports. When you first start the NetVoyant Console, use the Configuration Wizard to streamline the initial configuration process.

**Note:** You can return to the Configuration Wizard or access the **Config** tab in the NetVoyant Console to update configuration options at any time.

This chapter covers the following topics:

- “NetVoyant Configuration Tasks” on page 32
- “Using the Configuration Wizard” on page 33
- “Performing Initial Configuration Tasks” on page 34
- “Configuring Discovery” on page 49
- “Configuring Device Classes and Models” on page 59
- “Troubleshooting NetVoyant Configuration” on page 65

## NETVOYANT CONFIGURATION TASKS

Before the NetVoyant system identifies the devices on your network, collects data for those devices, and provides reports on the data, you must complete some initial configuration tasks. Additional configuration is required only to ensure that the data you need is collected and displayed in reports according to your organizational needs.

Configuring the NetVoyant product includes the following types of tasks:

Required?	Configuration task	More information
Yes	<b>Configure discovery.</b> Define what NetVoyant discovers by configuring NetVoyant discovery.  <b>Note:</b> The initial tasks that you perform in the Configuration Wizard quickly configure the NetVoyant discovery process. For more information, see <a href="#">“Using the Configuration Wizard” on page 33</a>	<a href="#">“Configuring Discovery” on page 49</a>
No	<b>Configure data collection and retention.</b> Configure overall data collection and retention by configuring datasets.  If you do not complete this task type, the NetVoyant system collects data based on default settings and the information from the discovered devices.	<a href="#">“Viewing and Configuring Data by Poll Instance” on page 69</a>
No	<b>Configure and manage polling.</b> Configure the polling frequency for a device by managing polling.  If you do not complete this task type, the NetVoyant system collects data based on default datasets and the information from the discovered devices.	<a href="#">“Configuring Data Collection Frequency” on page 94</a>
No	<b>Configure user roles.</b> Control how users are able to use the NetVoyant reporting tool and interact with your networks and devices by adding and configuring NetVoyant user roles (performed in the NetVoyant reporting tool or the NetQoS Performance Center).  If you do not complete this task type, the NetVoyant system provides access to administration and report data using the default roles and settings.	<a href="#">“Adding and Editing Roles” on page 296</a>
No	<b>Configure user accounts.</b> Manage access to the NetVoyant Console and collected data by creating and configuring NetVoyant user accounts (performed in the NetVoyant reporting tool or the NetQoS Performance Center).  If you do not complete this task type, the NetVoyant system provides access to administration and report data using the default user accounts and settings.	<a href="#">“Adding or Editing a NetVoyant User” on page 299</a>



## USING THE CONFIGURATION WIZARD

The first time you open the NetVoyant Console in a standalone system, the Configuration Wizard opens. Use this wizard to set up the initial configuration for the NetVoyant product and discover the devices on your network. It continues to open by default until you have configured discovery scopes and SNMP profiles.

**Note:** The Configuration Wizard does not display the first time that you open the NetVoyant Console on a distributed system. However, it is the most straightforward method for performing the initial configuration on a distributed system from the Master console. For more information about differences between standalone and distributed systems, see [“NetVoyant Architectural Overview and Licensing” on page 16.](#)

### To use the Configuration Wizard to configure the NetVoyant product:

1. From the **Tools** menu in the NetVoyant Console, select **Configuration Wizard**.
  - Click **Next** to step through the wizard.
  - Click **Back** to step backwards to a previous step.



2. Add the SNMP profiles.  
For more information, see [“Adding SNMP Profiles to the Console” on page 34.](#)
3. Add discovery scopes.  
For more information, see [“Configuring the Discovery Scopes” on page 40.](#)
4. (Optional) Add discovery seeds.  
For more information, see [“Adding Discovery Seeds” on page 43.](#)
5. Select polled device classes.  
For more information, see [“Enabling or Disabling Polling for a Device Class” on page 45.](#)
6. Start discovery.  
For more information, see [“Initiating Discovery” on page 46.](#)
7. On the last screen of the wizard, click **Finish**.

## PERFORMING INITIAL CONFIGURATION TASKS

You can use the Configuration Wizard to perform the tasks described in this section. These tasks enable you to complete a preliminary configuration of your NetVoyant system and initiate the discovery of your network.

### Adding SNMP Profiles to the Console

The NetVoyant Console uses SNMP profiles in order to establish access to the devices on your network. In defining a profile, you create an identity used for authentication when performing SNMP queries and sets. The NetVoyant Console supports authentication to devices using SNMPv1, SNMPv2, and SNMPv3.

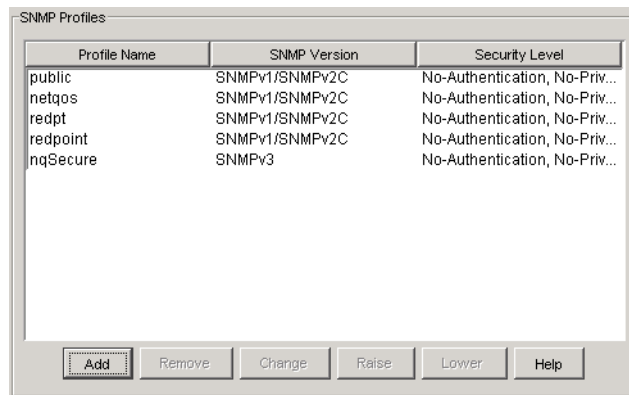
**Note:** If you are running a distributed NetVoyant system, you must add or modify SNMP profiles on the Master server. If a poller is not operational when the configuration change occurs on the Master, the change will be synchronized when communication with the poller is restored.

### Configuring the SNMP Profile List

You can configure these profiles directly in the Configuration Wizard or you can access and edit SNMP Profiles from the **Config** tab in the NetVoyant Console. The NetVoyant product requires at least one valid SNMP profile for each device in order to retrieve polling data.

#### To add an SNMP profile in the Configuration Wizard:

1. From the **Tools** menu in the NetVoyant Console, select **Configuration Wizard**.
2. Click **Next** once to display the **SNMP Profiles** list.



3. Click **Add**.
4. In the **SNMP Profiles** dialog box, enter the parameters for the new SNMP profile and click **OK**.  
For information about setting parameters for SNMP Profiles, see [“Defining SNMP Profiles” on page 35](#).
5. To change the position of a profile in the list, select it and click **Raise** or **Lower**.

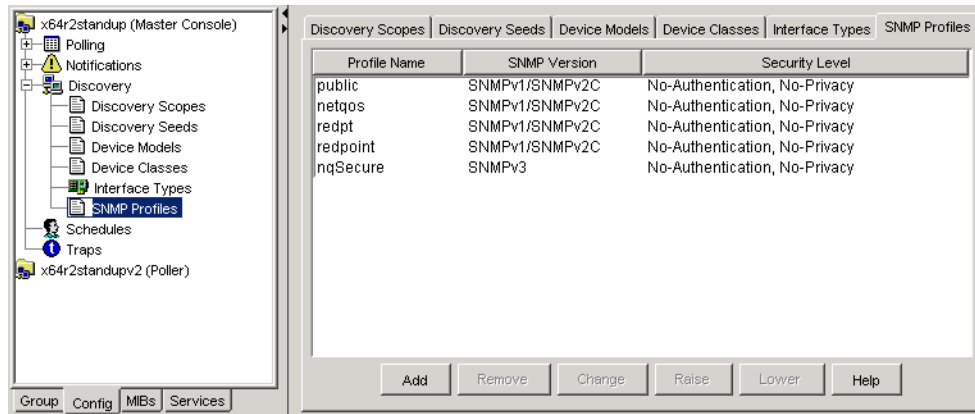
**Note:** When discovering a device, the NetVoyant product checks each profile in list order to identify a valid profile for that device. Re-ordering the SNMP profiles to make the most-used profiles highest in the list can significantly reduce the amount of time required for discovery.

6. Click **Next** to continue through the rest of the Configuration Wizard.
7. On the last page of the wizard, click **Finish**.

### To add an SNMP profile from the Config tab:

1. In the NetVoyant Console (Master or standalone), click the **Config** tab.
2. Expand the Master server.
3. Expand **Discovery** and select **SNMP Profiles**.

The currently configured profiles appear in the context panel.



4. Click **Add**.

The **SNMP Profiles** dialog box opens.

5. In the dialog box, enter the parameters for the new user profile and click **OK**.  
For information about setting parameters for SNMP Profiles, see the following section.
6. To change the position of the profile in the list, select it and click **Raise** or **Lower**.

**Note:** When discovering a device, the NetVoyant product checks each profile in list order to identify a valid profile for that device. Re-ordering the SNMP profiles to make the most-used profiles highest in the list can significantly reduce the amount of time required for discovery.

## Defining SNMP Profiles

Establishing access to the devices on your network from the NetVoyant Console depends upon creating profiles that it can use for authentication. NetVoyant supports authentication to devices using SNMPv1, SNMPv2C, and SNMPv3. You can define multiple SNMP profiles in the NetVoyant Console so that you can accommodate multiple types of protocols and access credentials used across your network.

### SNMPv1 and SNMPv2

For SNMPv1 or SNMPv2C, authentication consists of providing the correct community string for a particular access level (get and set). If a device is assigned an SNMP profile with the correct community strings, access is granted.

If you plan to configure IP SLA operations for a device directly from the NetVoyant Console via SNMPv1 or SNMPv2C, you must create a profile to define both the read and write community strings (the get and set community strings) for the device. For more information, see [“Setting SNMP Profiles for a Device” on page 149](#).

### **SNMPv3**

Establishing contact using SNMPv3 is more complex. SNMPv3 employs a User-based Security Model (USM). Before access is granted at a particular level, a security user (in this case, the NetVoyant Console) and a set of authentication and privacy keys must be verified by the device’s SNMP engine. This set of authentication and privacy keys (called a *credential*) is linked to an SNMP profile that the NetVoyant Console uses when contacting a device.

For more information about specifying SNMPv3 authentication and privacy, see [“Using SNMPv3 Security Credentials” on page 37](#).

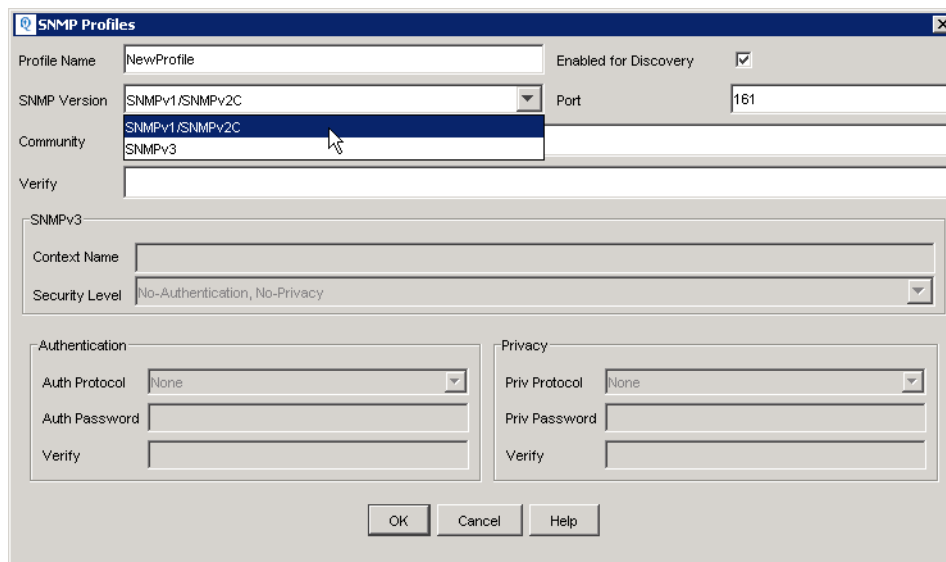
#### **To create or edit an SNMP Profile:**

1. Open the **SNMP Profiles** dialog box.
  - From the **Config** tab, expand **Discovery**, select **SNMP Profiles**, and click **Add** or **Change** in the context panel.
  - From the Configuration Wizard, click **Next** once to display the **SNMP Profiles** list and click **Add** or **Change**.
2. In the **Profile Name** field, enter a unique name for the profile.

**Note:** Profile names must be unique and are not case-sensitive (for example, “Public” and “public” are considered the same and not unique). The NetVoyant Console does a validity check when you save the settings.
3. Select or clear the **Enabled for Discovery** check box.
  - If the profile is enabled (the default setting), NetVoyant tests the profile during discovery and assigns it based on a successful match.
  - If the profile is **not** enabled for discovery, NetVoyant does not test the profile during discovery when it attempts to determine a device’s SNMP version/profile. When the profile has previously been assigned to a device and you disable the profile, NetVoyant attempts to assign another profile during the next discovery cycle.
4. Choose the **SNMP Version** for the profile.

Profiles can be configured for SNMPv1, SNMPv2c, or SNMPv3. When either SNMPv1 or SNMPv2c is selected, you specify the community string that is used to gain access. When SNMPv3 is selected, you use the bottom portion of the dialog box to configure access levels using authentication and privacy protocols.

**Note:** You cannot change the SNMP version for a profile after it has been created.



The image shows a screenshot of the 'SNMP Profiles' configuration window. The window has a title bar with a question mark icon and a close button. Inside, there are several fields and sections:

- Profile Name:** A text field containing 'NewProfile'.
- Enabled for Discovery:** A checkbox that is checked.
- SNMP Version:** A dropdown menu showing 'SNMPv1/SNMPv2C'.
- Port:** A text field containing '161'.
- Community:** A dropdown menu showing 'SNMPv1/SNMPv2C'.
- Verify:** A text field.
- SNMPv3 Section:**
  - Context Name:** A text field.
  - Security Level:** A dropdown menu showing 'No-Authentication, No-Privacy'.
- Authentication Section:**
  - Auth Protocol:** A dropdown menu showing 'None'.
  - Auth Password:** A text field.
  - Verify:** A text field.
- Privacy Section:**
  - Priv Protocol:** A dropdown menu showing 'None'.
  - Priv Password:** A text field.
  - Verify:** A text field.

At the bottom of the window are three buttons: 'OK', 'Cancel', and 'Help'.

5. Enter the port number in the **Port** field.

The default port for SNMP is port 161; however, if you are using another port for SNMP polling, specify that port number for the profile.

6. Enter the community/security information.

If either SNMPv1 or SNMPv2c is selected as the SNMP version, enter the community string in the **Community** field and again in the **Verify** field.

**Note:** Each SNMPv1/v2 profile must use a unique community string. If you attempt to create a profile with a community string used by an existing profile, the NetVoyant Console will not accept the profile.

If SNMPv3 is selected as the SNMP version, see the following section for more information about configuring SNMPv3 security protocols.

7. Click **OK**.

## Using SNMPv3 Security Credentials

SNMP Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices using a combination of authenticating and encrypting frames over the network.

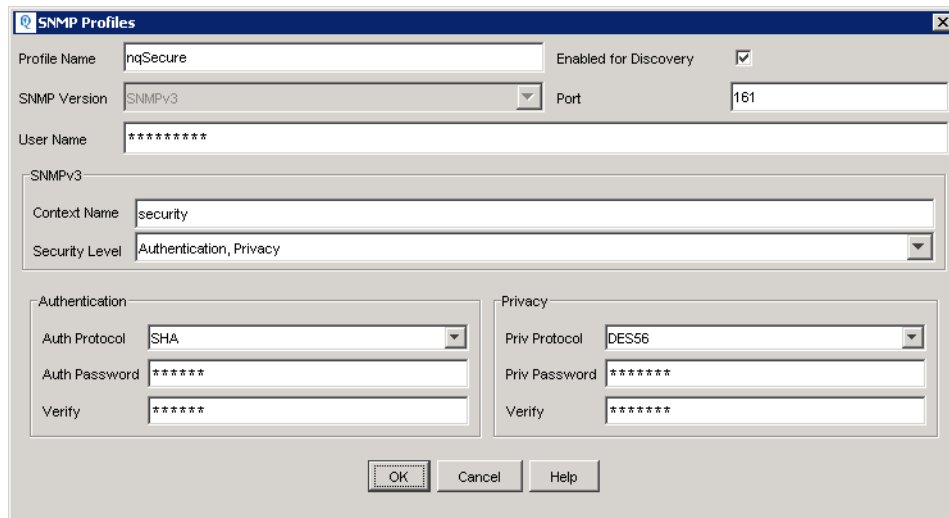
SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

- **Authentication** - utilizes time-stamping and password hashing to reduce the chance of unauthorized access of an SNMP-enabled device from a Network Management Station (NMS).
- **Privacy** - provides encryption for SNMP messages sent across a network, ensuring message integrity and preventing intercepted SNMP packets from being deciphered by unauthorized users. This can be used only with authentication.

## To a define an SNMP Profile using SNMPv3:

1. Open the **SNMP Profiles** dialog box.
  - From the **Config** tab, expand **Discovery**, select **SNMP Profiles**, and click **Add** or **Change** in the context panel.
  - From the Configuration Wizard, click **Next** once to display the **SNMP Profiles** list and click **Add** or **Change**.
2. In the **Profile Name** field, enter a unique name for the profile.

**Note:** Profile names must be unique and are not case-sensitive (for example, “Public” and “public” are considered the same and not unique). The NetVoyant Console performs a validity check when you save the profile settings.

The image shows the 'SNMP Profiles' dialog box. It has a title bar with a question mark icon and the text 'SNMP Profiles'. The dialog contains several fields: 'Profile Name' with the value 'ngSecure', 'Enabled for Discovery' checked, 'SNMP Version' set to 'SNMPv3', and 'Port' set to '161'. Below these is a 'User Name' field with asterisks. A section titled 'SNMPv3' contains 'Context Name' set to 'security' and 'Security Level' set to 'Authentication, Privacy'. This section is divided into 'Authentication' and 'Privacy' sub-sections. 'Authentication' has 'Auth Protocol' set to 'SHA', 'Auth Password' with asterisks, and 'Verify' with asterisks. 'Privacy' has 'Priv Protocol' set to 'DES56', 'Priv Password' with asterisks, and 'Verify' with asterisks. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

3. Select or clear the **Enabled for Discovery** check box.
  - If the profile is enabled (the default setting), NetVoyant tests the profile during discovery and assigns it based on a successful match.
  - If the profile is **not** enabled for discovery, NetVoyant does not test the profile during discovery when it attempts to determine a device’s SNMP version/profile. When the profile has previously been assigned to a device and you disable the profile, NetVoyant attempts to assign another profile during the next discovery cycle.
4. Choose SNMPv3 as the **SNMP Version** for the profile.
5. Enter the port number in the **Port** field.

The default port for SNMP is port 161; however, if you are using another port for SNMP polling, specify that port number for the profile.

6. Enter the remaining parameters in the dialog box to define the security and authentication.

Parameter	Description
<b>User Name</b>	This is the User Name used for device access.  <b>Note:</b> Each SNMPv3 profile must use a unique user name. If you attempt to create a profile using the same user name as an existing profile, the NetVoyant Console will not accept the profile.
<b>Context Name</b>	(Optional) For devices that support both switch and router interfaces, use this setting to specify a keyword that applies to the particular context where this profile will be applied.  <b>Note:</b> You must create separate profiles for each context when a device supports both router and switch contexts.
<b>Security Level</b>	This specifies the security level to be used. The two security areas are grouped together into a security level, allowing for three possible Security Levels: <ul style="list-style-type: none"> <li>• <b>No Authentication, No Privacy</b></li> <li>• <b>Authentication, No Privacy</b></li> <li>• <b>Authentication, Privacy</b></li> </ul>
<b>Authentication</b>	If the selected security level applies authentication, select the authentication type ( <b>MD5</b> or <b>SHA</b> ) from the drop-down list and enter the password (between 1 and 64 characters in length) used to determine Authentication and verify it.  If you make a change to an existing password and the credential is currently used with a profile that is applied to one or more devices, a confirmation dialog box opens.
<b>Privacy</b>	If the selected security level applies privacy, select <b>DES56</b> , <b>AES128</b> , or <b>3DES</b> from this drop-down list and enter a password (between 1 and 64 characters in length) used to determine Privacy and verify it.  If you make a change to an existing password and the credential is currently used with a profile that is applied to one or more devices, a confirmation dialog box opens.

7. Click **OK**.

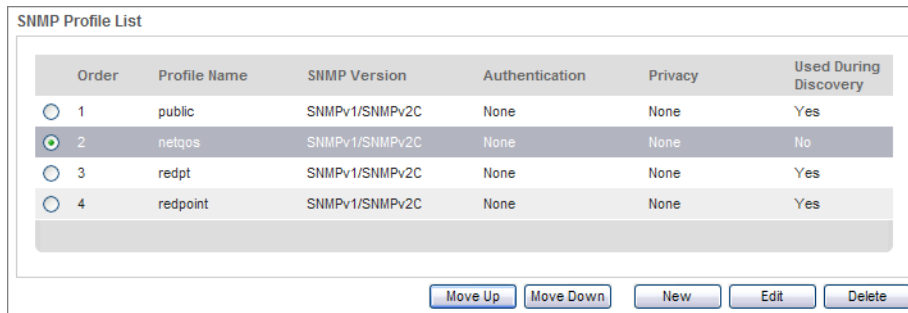
## SNMP Profiles in the NetQoS Performance Center

When your installation of the NetVoyant product is bound to the NetQoS Performance Center, the SNMP profiles defined in the NetVoyant Console are automatically added to NetQoS Performance Center. These profiles are also distributed to any other NetQoS products that are bound to that NetQoS Performance Center during the next synchronization cycle.

The NetQoS Performance Center minimizes duplication of SNMP profiles by comparing the User (SNMP v3) or Community String (SNMP v1 and v2) values to existing profiles when a new data source is added. If a profile already exists with the same User or Community String, the profile with the most recent change (based on the timestamp) is used as the master profile.

During synchronization, if the NetQoS Performance Center encounters a new profile name that matches an existing profile, but the User or Community String values do not match, it saves the newer profile by appending a number to the duplicate name so that it is unique. For example, the first profile

named “Boston” retains this name, and “Boston(1)” is used as a unique name for the second profile. When the NetQos Performance Center changes the profile name during this synchronization process, the name change is also implemented in the data source product during the next synchronization.



The image shows a window titled "SNMP Profile List". It contains a table with the following data:

Order	Profile Name	SNMP Version	Authentication	Privacy	Used During Discovery
1	public	SNMPv1/SNMPv2C	None	None	Yes
2	netqos	SNMPv1/SNMPv2C	None	None	No
3	redpt	SNMPv1/SNMPv2C	None	None	Yes
4	redpoint	SNMPv1/SNMPv2C	None	None	Yes

Below the table are five buttons: "Move Up", "Move Down", "New", "Edit", and "Delete".

If you or another administrator add or modify an SNMP profile in the NetQoS Performance Center, these changes are synchronized with all of the registered data source products, including the NetVoyant product.

## Configuring the Discovery Scopes

When you specify discovery scopes, the NetVoyant product discovers only networks and devices included in your discovery scope list. It can detect all networks and devices connected to your system, but you should designate the items to include and exclude from the discovery process. It is highly recommended that you add discovery scopes to limit the number of devices discovered, especially when connected to large networks, such as the Internet.

**Note:** If you are running a distributed NetVoyant system, it is recommended that you configure discovery scopes on the Master server and specify the appropriate poller for each scope. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

You can add, edit, and remove items in the Discovery Scopes list using the **Configuration Wizard**, or from the **Config** tab in the NetVoyant Console. You can also import a list of items using a standard text file.

### Adding Networks and Devices to the Discovery Scopes

By default, the Discovery Scopes list is empty when the NetVoyant product is first installed. If the discovery process is enabled and executed without any scoping parameters, the NetVoyant product will attempt to discover all networks that are connected to the NetVoyant system. This can produce undesired results.

To ensure that the NetVoyant product discovers only those networks and devices that you want, add items to the Discovery Scopes list to be explicitly included or excluded during discovery.

**Note:** It is possible to explicitly exclude networks and devices. This may be necessary when you specify a large network (such as a class B), but you want to exclude some of the smaller scopes (such as class C networks). The inclusion and exclusion of certain networks and devices is controlled by the **Include** check box in the Discovery Scopes list.



## To add a discovery scope:

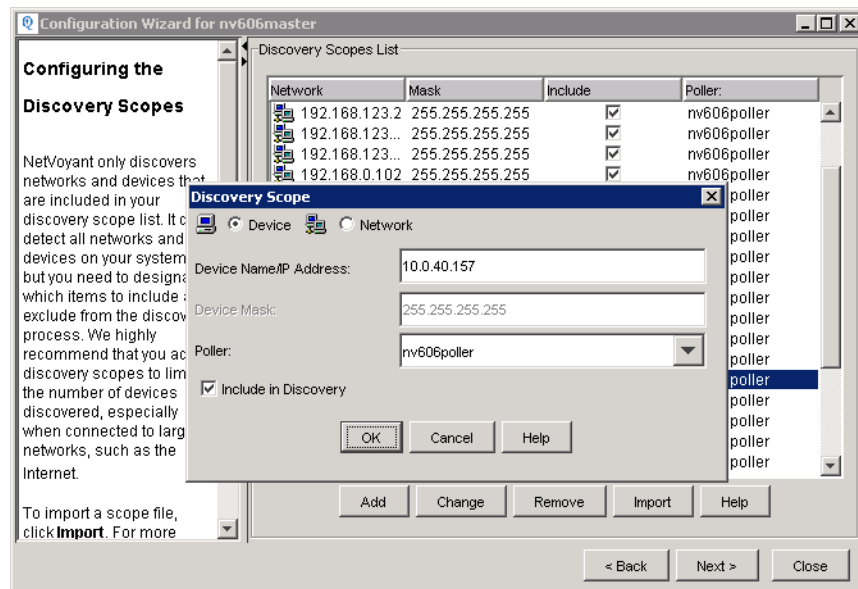
1. Access the discovery scopes list in the NetVoyant Console in one of two ways:
  - From the **Tools** menu in the NetVoyant Console, select **Configuration Wizard** and click **Next** until the Discovery Scopes screen appears.
  - Click the **Config** tab and select **Discovery > Discovery Scopes**.

2. Click **Add**.

**Note:** If you need to import a scope file instead of entering the scope information, click **Import**. For more information, see “[Importing Discovery Scopes](#)” on page 42.

3. Specify the discovery scope:

- To add a network, select **Network** and enter the **Network IP Address** and **Network Mask**.
- To add an individual device, select **Device**, enter the **Device Name** or **IP Address**.



4. Designate the scope as included or excluded:
  - To include the network or device in discovery, select the **Include in Discovery** check box.
  - To exclude the network or device from discovery, clear the **Include in Discovery** check box.

5. For a distributed system, use the **Poller** drop-down list to designate a poller.

This setting determines which poller “owns” the scoped item because pollers are typically partitioned by network scopes. For a standalone system, this is automatically set to the local poller (Master) and cannot be changed.

6. Click **OK**.

7. If you add or edit discovery scopes in the list using the Configuration Wizard, click **Next** to continue to the last page of the wizard and then click **Finish**.

## Importing Discovery Scopes

You can import a text file that contains your discovery scopes to simplify this process. The file must contain a list of devices and networks that you want to include in your discovery scope. Each device or network IP address must be on a separate line in the file.

The following is an example of a valid list of discovery scope entries:

```
192.168.123.1
192.168.123.2,255.255.255.255
192.168.123.3/32
192.168.123.0/24
192.168.124.0,255.255.255.0
```

**Note:** If you are using a distributed NetVoyant system, you must specify a single poller for the imported discovery scope list. If your list contains items for different pollers, you can create separate text files and import each with an assignment to the correct poller. Or, you can import the scopes designating a single poller and then use the **Change** button to re-assign items to the correct poller.

### To import a list of discovery scopes:

1. In the NetVoyant Console, click the **Config** tab.
2. Expand **Discovery**.

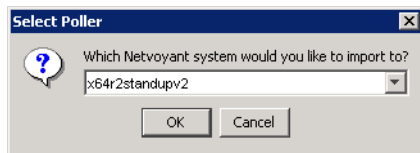
This provides access to discovery configuration.

3. Select **Discovery Scopes**.

The currently configured discovery scopes appear in the context panel.

4. Click **Import**.

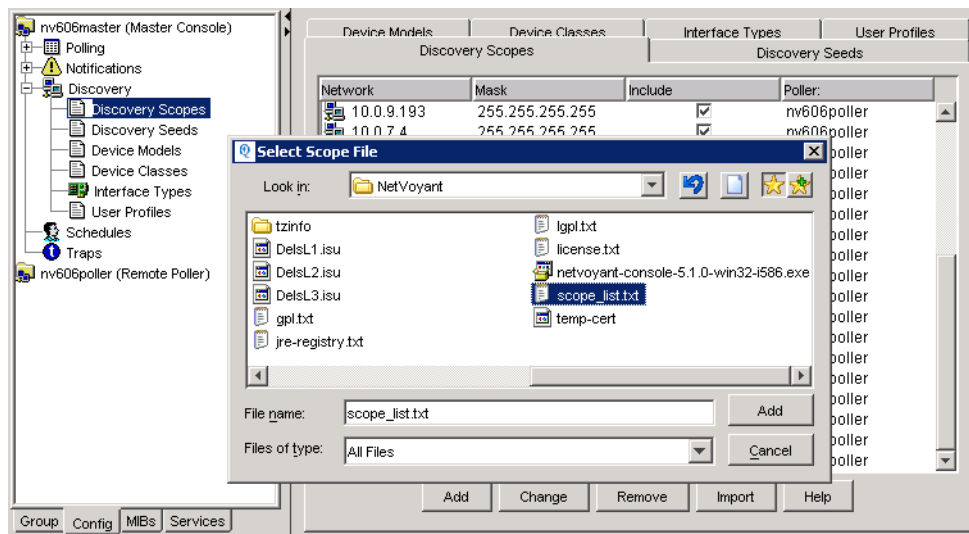
If you are running a distributed NetVoyant system and are importing the scope on the Master, the **Select Poller** dialog box opens.



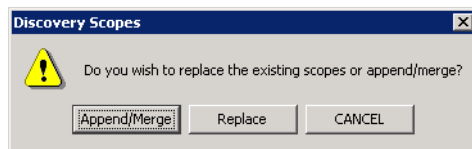
5. (*Distributed only*) Use the drop-down menu to select a poller and click **OK**.

The **Select Scope File** dialog box opens.

6. Browse for and select the text file that contains the discovery scopes.



7. Click **Add**.



8. Confirm the import by choosing to append or replace the existing discovery scopes list.
  - Click **Append/Merge** to add the discovery scopes in the imported file to the current discovery scopes. The NetVoyant product scans the imported file for valid scopes, ignores duplicate entries, and displays the number of valid scopes that it finds.
  - Click **Replace** to remove the current discovery scopes and add the discovery scopes in the imported file. The NetVoyant product scans the imported file for valid scopes and displays the number of valid scopes that it finds.
9. Click **OK**.

## Adding Discovery Seeds

The NetVoyant product uses discovery seeds to provide starting points for the discovery process. Seeds are specific devices or networks that it probes during the discovery process to find other devices and networks to discover.

Adding discovery seeds is not required; however, in some situations it can be useful to provide these “hints.” For example, when you want the NetVoyant product to discover networks that are separated from the poller by a public network or when it cannot discover a gateway router because of problems with its access list or SNMP profiles.

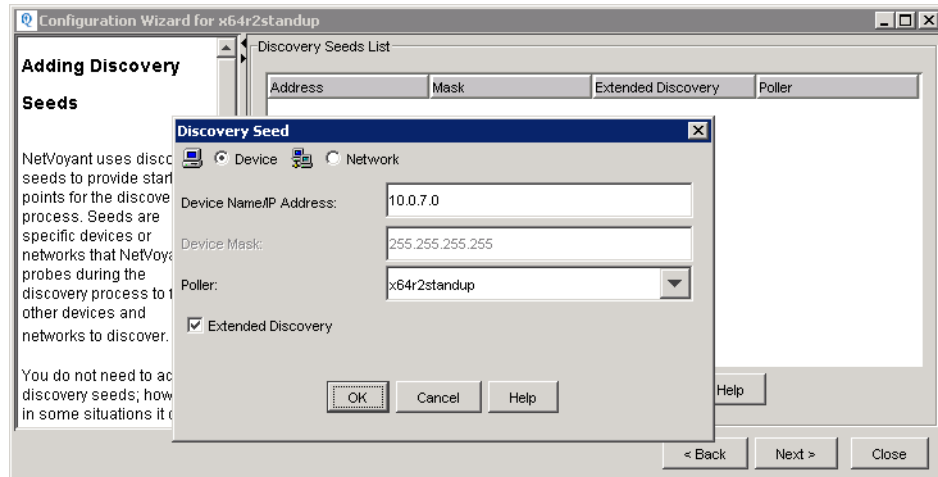
If you add a device as a discovery seed, the discovery process will first PING, then scan the device and start discovery at that point. If you add a network as a discovery seed, a broadcast Ping will be sent to that subnet and all devices that respond will be discovered.

**Note:** If you are running a distributed NetVoyant system, it is recommended that you configure discovery seeds on the Master and specify the appropriate poller for each seed. If a poller is not

operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

### To add a discovery seed:

1. Access the discovery seeds list in the NetVoyant Console in one of two ways:
  - From the **Tools** menu in the NetVoyant Console, select **Configuration Wizard** and click **Next** until the Discovery Seeds List screen appears.
  - Click the **Config** tab and select **Discovery > Discovery Seeds**.
2. Click **Add**.



3. In the **Discovery Seed** dialog box, specify a seed.
  - To add a network as a discovery seed, select **Network** and enter the network IP address and network mask.
  - To add an individual device as a discovery seed, select **Device** and enter the device name or IP address.
4. For a distributed system, use the **Poller** drop-down list to designate a poller.  
 This setting determines which poller “owns” the seed item. For a standalone system, this is automatically set to the local poller (Master) and cannot be changed.
5. Select or clear the **Extended Discovery** check box to include or omit the seed in extended discovery.  
 When this option is selected, the NetVoyant product rediscovers the device’s characteristics during its rediscovery process. It also uses information in the ARP cache and IP routing table for this device to discover other devices. For more information about extended discovery, see [“The NetVoyant Discovery Process” on page 49](#).
6. Click **OK**.
7. If you add or edit discovery seeds in the list using the Configuration Wizard, click **Next** to continue to the last page of the wizard and then click **Finish**.

## Enabling or Disabling Polling for a Device Class

To control the types of devices from which a NetVoyant poller collects data, you can select which device classes are automatically enabled for polling upon discovery.

The NetVoyant product discovers all devices within your discovery scope; however, it does not automatically enable polling for those device classes that are excluded from polling. If it discovers a new device and its class is not enabled for polling, it does not gather any data from the new device unless you enable polling for it after discovery.

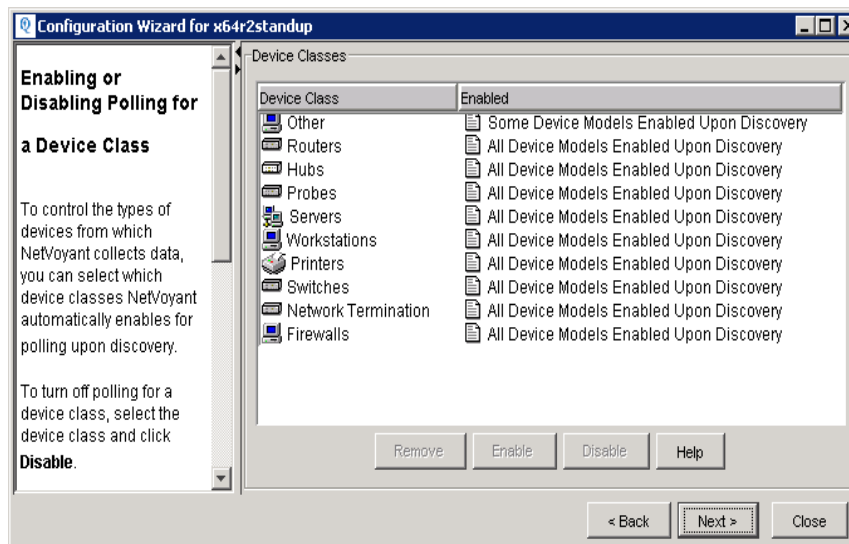
In a distributed NetVoyant system, configuration of device classes must be done on the Master server. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

**Note:** Enabling or disabling polling for a device class does not affect polling for devices that are already discovered.

**Important:** It is strongly recommended that you do not remove device classes from the NetVoyant Console. If you remove a device class, the NetVoyant Console defines all devices of this class as part of the “Other” device class and continues to poll the devices. If you do not want to poll a particular device class, disable that device class from polling.

### To set polling for device classes:

1. Access the Device Classes list in the NetVoyant Console in one of two ways:
  - From the **Tools** menu in the NetVoyant Console, select **Configuration Wizard** and click **Next** until the Device Classes screen appears.
  - Click the **Config** tab and select **Discovery > Device Classes**.
2. Enable or disable device classes.
  - To turn off polling for a device class, select the device class and click **Disable**.
  - To turn on polling for a device class that is disabled, select the device class and click **Enable**.



3. If you modify automatic polling for device classes using the Configuration Wizard, click **Next** to continue to the last page of the wizard and then click **Finish**.

## Initiating Discovery

After you complete configuration using the Configuration Wizard, start the discovery process so that the NetVoyant product can begin to discover your networks and devices. By default, it performs initial discovery when triggered from the Configuration Wizard. From then on, it performs a partial rediscovery every night at midnight (by default) to update device configuration information. You can configure the time at which partial and full rediscovery takes place on the **Config** tab. For more information, see [“Configuring Discovery Options” on page 52](#).

You can also initiate a rediscovery of an individual device, group of devices, or your entire network manually. For more information about manually rediscovering an individual device, see [“Rediscovering Devices and Groups” on page 152](#).

### To start the initial discovery from the Configuration Wizard:

1. On the **Tools** menu in the NetVoyant Console, click **Configuration Wizard**.
2. Click **Next** until the **Discovery Log** screen appears.

For more information about setting the discovery options before proceeding with the initial discovery, see [“Configuring Discovery Options” on page 52](#).

3. Click **Start Full Discovery**.

NetVoyant adds a discovery log to the list for each new device or network that it discovers.

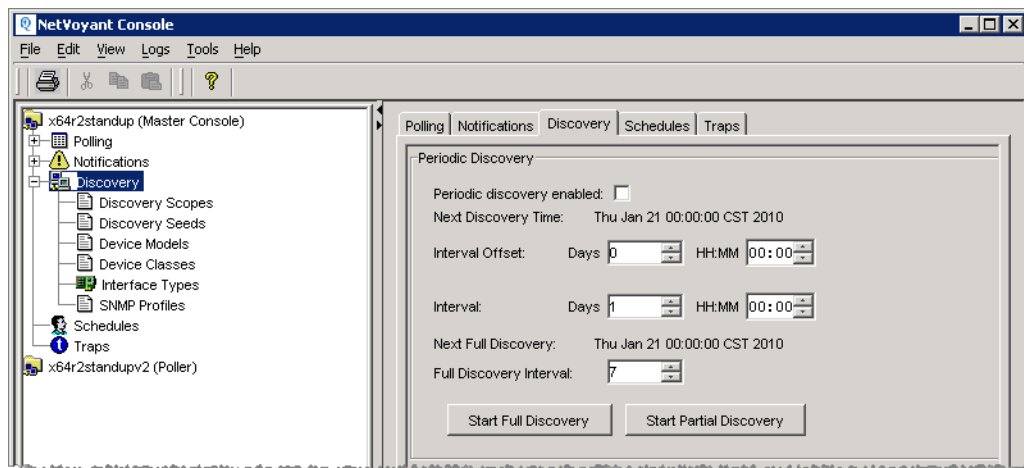
4. Click **Discovery Monitor** to verify that the NetVoyant product is discovering devices as expected. For more information, see [“Monitoring the Discovery Process” on page 47](#).

**Note:** For assistance with troubleshooting issues during the discovery process, see [“Troubleshooting NetVoyant Configuration” on page 65](#).

5. After discovery begins, click **Next** to review a summary of your configuration selections.
6. Click **Finish**.

### To start a rediscovery of your entire network:

1. In the NetVoyant Console, click the **Config** tab.
2. Click **Discovery**.



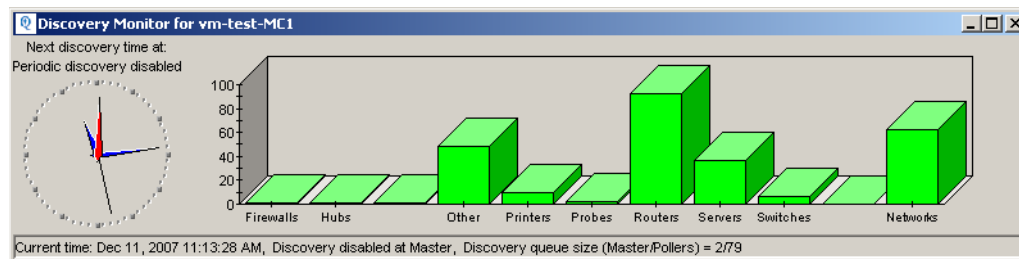
3. In the context panel, click one of the start discovery buttons

- To start a full discovery of your entire network, click **Start Full Discovery**.
- To start a partial discovery of your entire network, click **Start Partial Discovery**.

For more information about the differences between a full and partial discovery, see [“Using Full and Partial Discovery”](#) on page 49.

## Monitoring the Discovery Process

The Discovery Monitor can help you troubleshoot and monitor the discovery process as it is occurring. It provides information about what the NetVoyant product is currently discovering and when the next discovery process is scheduled to occur.



It is recommended that you monitor the initial full discovery of your network using the Discovery Monitor.

**Note:** For assistance troubleshooting issues during the discovery process, see [“Troubleshooting NetVoyant Configuration”](#) on page 65.

### To view the Discovery Monitor:

- From the **Tools** menu in the NetVoyant Console, select **Discovery Monitor**.

The Discovery Monitor opens.

The **Discovery Queue Size** at the bottom of the Discovery Monitor indicates the number of devices that are currently queued for discovery. The graphical breakdown by device class indicates how many devices of each class are currently discovered.

**To force a stop of the discovery process:**

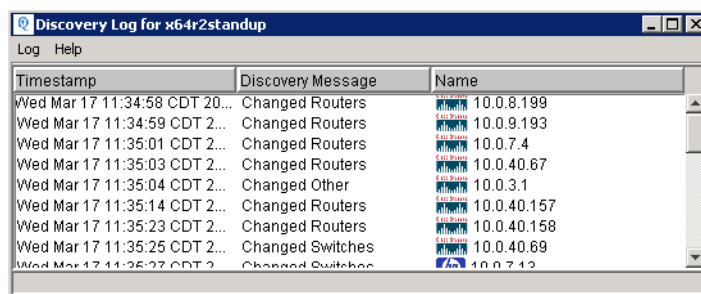
1. In the NetVoyant Console, click the **Services** tab.
2. Select the **Topology** service.
3. Click **Stop**.

This stops the discovery process.

**Note:** For more information about the Topology service and other NetVoyant services, see “Managing NetVoyant Services” on page 279.

## Viewing the Discovery Log

In addition to the Discovery Monitor, you can use the discovery log window to monitor the discovery process. This tool displays logs related to the discovery process. Any networks or devices that are discovered are added to the list as a separate log item.

**To view the discovery log window:**

- From the **Tools** menu in the NetVoyant Console, select **Discovery Log**.

The discovery log window displays the following information:

Parameter	Description
<b>Timestamp</b>	The date and time at which NetVoyant discovered the network or device.
<b>Discovery message</b>	A description of the type of discovery that was made.
<b>Name</b>	The name of the network or device that NetVoyant discovered.



## CONFIGURING DISCOVERY

When the NetVoyant product discovers your network, it finds the SNMP-manageable devices in your discovery scope. It also discovers which SNMP tables are supported by each discovered device. NetVoyant discovery is based on SNMP and ICMP.

To enable the NetVoyant product to discover devices on your network and to control what it discovers, you must configure the discovery process.

**Note:** You can perform all required steps to configure initial discovery in the Configuration Wizard. For more information, see “Using the Configuration Wizard” on page 33.

### The NetVoyant Discovery Process

The first discovery cycle that you initiate on the NetVoyant system is a full discovery. This first discovery is required so that the NetVoyant product can identify the devices on your network and determine what types of data it can collect from each device. After this initial discovery, you can make numerous configuration customizations to fine-tune rediscovery, polling, and data collection.

#### Using Full and Partial Discovery

The NetVoyant product can execute two different types of discovery: full and partial. As a NetVoyant administrator, you can determine how often the NetVoyant system does a partial discovery of known devices and how often it completes a full rediscovery of all devices on your network.

**Full Discovery.** When the NetVoyant product performs a full discovery, it attempts to discover all enabled datasets against each device. This is the required discovery process for initial discovery, and is also desirable for less frequent or manual rediscovery in order to capture new devices and dataset changes, such as which devices and datasets are enabled for or disabled from polling.

**Partial Discovery.** When the NetVoyant product performs a partial discovery, it attempts to rediscover only those datasets that were previously discovered on each device. This means that only new poll instances for an existing dataset on a known device will be discovered. Because most devices do not change functionality regularly, a partial discovery is desirable for regular daily rediscovery of your NetVoyant system. If you have a large number of devices, this can save a significant amount of processing time.

For more information about the sequence of events when the NetVoyant system performs a full and partial discovery, see the following section.

## Discovery Sequence of Events

By default, the NetVoyant product executes an automatic full rediscovery on a weekly basis. You can change this setting in the Discovery Options to be more or less frequent, and you can manually execute a full discovery at any time. For more information about setting the periodic rediscovery options and manually executing a full or partial rediscovery process, see [“Configuring Periodic Discovery” on page 52](#).

The NetVoyant product completes the full discovery process in the following sequence of events:

1. **Sends out a PING and queries with SNMP.** By default, the NetVoyant product sends a ping to each device within a discovery scope. You can use the broadcast ping option so that it captures a wider range of connected devices and networks. From the responses, it sends queries to determine the SNMP version supported by the responding device (if any) and the SNMP profile that will work with the device.
2. **Queues responding devices.** It then runs events 3 through 5 for devices in the queue. The NetVoyant product queues any additional devices that are discovered during these events.
3. **Classifies devices based on a configurable database of device models and classes.** Devices that it recognizes as part of a known device class are added to the related NetVoyant group.
4. **Polls devices with SNMP to discover poll instances.** The NetVoyant product queries any tables that are used by the default datasets for poll instances. Poll instances correspond to the SNMP rows in these tables.

For example, it queries the `frCircuitEntry` MIB table for poll instances in the pre-configured Frame Relay Circuit Statistics dataset. You can add custom datasets and compile new MIBs into the NetVoyant Console to extend what poll instances it discovers in this stage.

5. **Queries the device’s ARP cache and IP routing table to discover further devices.** The NetVoyant product completes this stage only if a device is configured as a discovery seed or set to extended discovery.

It queries the internal tables to look for additional devices on the LAN segment or adjacent LAN segments. This information is also used to map IP addresses to MAC addresses for devices that don’t respond to SNMP. This information is useful for RMON matrix reporting (the RMON data is based on MAC address).

The NetVoyant product also queries the `ipRouteEntry` table (IP routing table) to find the “next hop” networks. If these networks are in scope, it queries for discoverable devices.

6. **Continues events 3 through 5 with each discovered device until the discovery queue is empty.**

By default, the NetVoyant system also executes a partial rediscovery on a daily basis (midnight). This partial discovery process is designed to rediscover only those datasets that were previously discovered on each known device. You can modify the time of day and frequency of this automatic partial rediscovery, or manually execute a partial rediscovery in the Discovery Options.

The sequence of events for a partial discovery is a sub-set of a full discovery:

1. **Queues known devices that are enabled for polling.**
2. **Polls each device with SNMP to discover poll instances.** The NetVoyant product queries any tables that are used by the current datasets for poll instances. Reachability, Availability, and Interface Statistics are always queried.

## Configuration Settings that Affect Discovery and Polling

You can configure how the NetVoyant product discovers your network and polls discovered devices by performing the following administrative tasks:

Required?	Description	More information
No	<b>Set the discovery options.</b> You can configure the following: <ul style="list-style-type: none"> <li>• If and when periodic rediscoveries are performed</li> <li>• How time-outs and retries are handled during discovery.</li> <li>• How new devices are named upon discovery.</li> <li>• The amount of system resources allocated to the discovery process.</li> <li>• The default “time-to-live” for unresponsive or out-of-scope devices</li> <li>• Event retention and system resource allocation</li> </ul>	“Configuring Discovery Options” on page 52
Yes	<b>Add SNMP profiles.</b> Establishing access to the devices on your network from the NetVoyant Console depends on creating profiles that it can use for access and authentication. NetVoyant supports authentication to devices using SNMPv1, SNMPv2 and SNMPv3.	“Adding SNMP Profiles to the Console” on page 34
No	<b>Add discovery scopes.</b> The NetVoyant product discovers only networks and devices included in your discovery scope list.  We highly recommend that you add discovery scopes to limit the number of devices discovered, especially when connected to large networks (such as the Internet).	“Configuring the Discovery Scopes” on page 40
No	<b>Add discovery seeds.</b> Seeds are specific devices or networks that the NetVoyant product probes during the discovery process to find other devices and networks to discover.  You do not need to add discovery seeds; however, in some situations it can be useful to provide these “hints.”	“Adding Discovery Seeds” on page 43

Required?	Description	More information
No	<b>Enable or disable polling for a device class.</b> To control the types of devices from which the NetVoyant poller collects data, you can select which device classes are automatically enabled for polling upon discovery.	“Enabling or Disabling Polling for a Device Class” on page 45
No	<b>Enable or disable polling for a device model.</b> To control the types of devices from which the NetVoyant poller collects data, you can select which device models are automatically enabled for polling upon discovery.	“Enabling or Disabling Polling for a Device Model” on page 64
No	<b>Configure interface types.</b> To control how the NetVoyant product identifies interfaces using <code>ifType</code> , you can add, edit, or remove interface types in the NetVoyant Console.	“Configuring Interface Types” on page 57
No	<b>Enable or disable discovery for a device.</b> You can remove individual devices from the nightly rediscovery.  You can also set individual devices to extended discovery, so that they provide further information during the discovery process to aid the NetVoyant product in finding other devices and networks to discover.	“Editing Discovery Settings for a Device” on page 150
No	<b>Enable or disable discovery for a dataset.</b> You can remove datasets from the full rediscovery.	“Managing Discovery for a Dataset” on page 74

## Configuring Discovery Options

When the NetVoyant product discovers your network, it finds the SNMP-manageable devices in your discovery scope. It also discovers which SNMP tables are supported by the discovered devices. Discovery is based on SNMP and ICMP.

You can configure when it performs rediscovery, how time-outs and retries are handled during discovery, how it names new devices that it discovers, and the amount of system resources allocated to the discovery process.

### Configuring Periodic Discovery

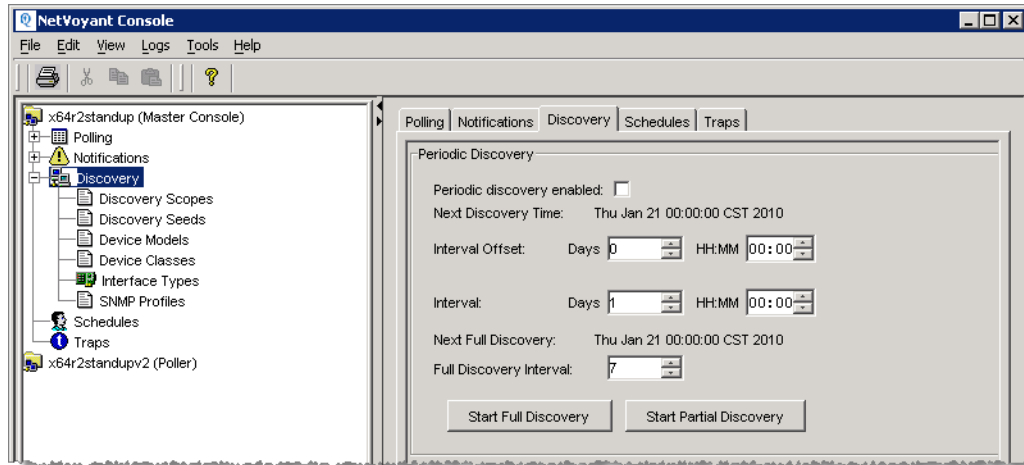
Periodic discovery, or *rediscovery*, is enabled by default and configured to occur at a daily interval at midnight. The NetVoyant product supports the scheduling of both full and partial rediscovery processes, with a default configuration of a partial rediscovery daily and a full rediscovery weekly. For more information about the differences between full and partial discovery, see “Using Full and Partial Discovery” on page 49.

From the **Config** tab, you can select the **Discovery** tab in the context panel and enable or disable periodic rediscovery, as well as modify the interval and timing for both full and partial rediscovery.

**To configure periodic discovery:**

1. In the NetVoyant Console (Master or standalone), click the **Config** tab.
2. Expand the Master and select **Discovery**.

The discovery options appear in the context panel.



3. Edit the following **Periodic Discovery** parameters as required:

Parameter	Description
<b>Periodic discovery enabled</b>	To turn off automatic rediscovery of your network, clear this check box. If you turn off rediscovery of your network, any new devices or configuration changes that you make to existing devices are not reflected in NetVoyant unless you manually add them.
<b>Interval Offset</b>	To configure when the starting point for rediscovery intervals will begin, select a time in hours, minutes, and seconds for the Interval Offset. If your NetVoyant system is already running periodic rediscovery (enabled), changing this setting (time in days, hours, and minutes) will shift the current discovery interval up or down accordingly.
<b>Interval</b>	To configure the frequency at which a partial rediscovery of your devices is performed, select a time in days, hours, minutes, and seconds for the Interval. By default, the NetVoyant product performs a partial rediscovery daily (an interval of 1 day and 00:00).
<b>Full Discovery Interval</b>	To configure the frequency at which a full rediscovery of your devices is performed, select the number of days for the interval. By default, the NetVoyant product performs a full rediscovery weekly (an interval of 7 days).

4. Click **Set** to save your changes.

**Note:** You can manually execute a full or partial rediscovery of your entire network. For a full rediscovery, click **Start Full Discovery**. For a partial rediscovery, click **Start Partial Discovery**.

## Configuring the Discovery Parameters

Use the Discovery Parameters to specify how rediscovery of your network is executed on your NetVoyant system and how the NetVoyant product manages previously discovered devices that are unresponsive, as well as devices that do not fully support SNMP polling or are currently out of scope.

### To configure discovery parameters:

1. In the NetVoyant Console (master or standalone), click the **Config** tab.
2. Expand the Master Console and select **Discovery**.

The discovery options appear in the context panel.

3. Scroll if necessary and edit the following **Discovery Parameters** as required:

Parameter	Description
<b>Timeout (sec)</b>	<p>Enter a length of time in seconds to configure how sensitive the NetVoyant product is to time-outs when performing SNMP queries to your devices during discovery.</p> <p>Longer time-outs significantly increase how long it takes to complete the discovery process.</p> <p><b>Note:</b> You can also configure time-outs and retries for individual devices. For more information, see <a href="#">“Editing Discovery Settings for a Device” on page 150</a>.</p>
<b>Retries</b>	<p>Enter the number of times that you want to retry each device for each SNMP profile when a timeout occurs.</p> <p>More retries can significantly increase how long it takes to complete the discovery process.</p> <p><b>Note:</b> You can also configure time-outs and retries for individual devices. For more information, see <a href="#">“Editing Discovery Settings for a Device” on page 150</a>.</p>
<b>Ping Sweep</b>	<p>Clear this check box to disable ping sweeps during rediscovery.</p> <p>If ping sweeps are disabled, the NetVoyant product uses directed broadcasts during rediscovery to create a list of devices to discover.</p> <p><b>Note:</b> As directed broadcast is often disabled in routers, it is recommended that you use ping sweep for the initial discovery of your network.</p>
<b>NPC Sync</b>	<p>Select this check box to enable the NetVoyant product to regularly synchronize data with NetQoS Performance Center.</p> <p><b>Note:</b> NetVoyant and either ReporterAnalyzer or SuperAgent must be added as data sources in the NetQoS Performance Center for this feature to function.</p>

Parameter	Description
<b>Device Expiration (days)</b>	<p>Modify this setting to change the number of days that a device remains in the system when it enters one of the states (Out-of-Scope, Does Not Resolve, or Unresponsive) that triggers a “time-to-live” expiration.</p> <p>When the number of days has transpired, the device is automatically removed at the next discovery process unless its state has changed.</p> <p>For more information about poll status for devices, see <a href="#">“Device Polling Status” on page 131</a>.</p>
<b>Device Unresponsive (days)</b>	<p>Modify this setting to change the number of consecutive, non-responsive days required for NetVoyant to set the device to an Unresponsive status, and trigger a “time-to-live” expiration.</p> <p>If the device responds before the expiration period, it will be returned to its previous status.</p> <p>For more information about poll status for devices, see <a href="#">“Device Polling Status” on page 131</a>.</p>
<b>Ignore Non-SNMP Devices</b>	<p>Select this check box to ignore all non-SNMP devices that are not explicitly scoped.</p> <p>By default, NetVoyant discovers all devices in a scope. If a device is not SNMP-capable, NetVoyant adds the device to the database and creates a Reachability poll table (poll instance) to enable a PING of the device and to obtain latency measurements.</p> <p>To specifically add a non-SNMP device to the scope when this option is selected, add the device address and mask, for example:</p> <p style="text-align: center;">192.168.123.1    255.255.255.255</p> <p>For more information about defining and using discovery scopes, see <a href="#">“Configuring the Discovery Scopes” on page 40</a>.</p>
<b>Detect Out-of-Scope Devices</b>	<p>Select this check box to retest out-of-scope devices during the “time-to-live” period.</p> <p>If an out-of-scope device is determined to be in scope during that time, NetVoyant returns the device to its previous status.</p> <p>This check box is selected by default; however, if you do not want to rediscover out-of-scope devices even if they are added to the discovery scope configuration, you can clear this check box so that NetVoyant will continue to expire all out-of-scope devices according to the <b>Device Expiration</b> setting.</p> <p>For more information about defining and using discovery scopes, see <a href="#">“Configuring the Discovery Scopes” on page 40</a>.</p>

- Click **Set** to save your changes.

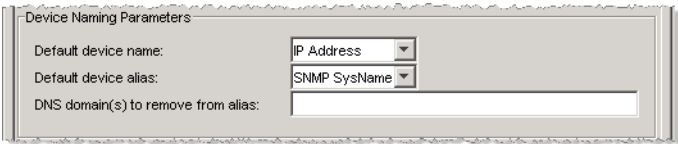
## Configuring the Device Naming Parameters

Use the Device Naming Parameters to specify how NetVoyant names the devices that it discovers on your network. Setting the naming parameters determines how devices appear in the NetVoyant Console and in reports.

**To configure device naming parameters:**

- 1. In the NetVoyant Console (master or standalone), click the **Config** tab.
- 2. Expand the Master Console and select **Discovery**.

The discovery options appear in the context panel.



- 3. Scroll if necessary and edit the following **Device Naming Parameters** as needed:

Parameter	Description
<b>Default device name</b>	Use the drop-down menu to select a default device name for your discovered devices using the IP address, DNS name, or SNMP sysName OID. <b>Note:</b> The device name is used to poll the device; therefore, this must be an IP address or a name that resolves to an IP address. Before selecting the SNMP Sysname option, ensure that your devices are set up so that the SNMP sysName resolves in DNS to an IP address.
<b>Default device alias</b>	Use the drop-down menu to select a default device alias for your discovered devices using the IP address, DNS name, or SNMP sysName OID. This is for display purposes and is the device alias that you see in the NetVoyant Console and for reporting. If you choose to use the sysName OID, the NetVoyant Console will use the device's DNS name or IP address for devices that do not have a sysName value.
<b>DNS domain(s) to remove from alias</b>	To remove the domain portion of your devices' name for display purposes in NetVoyant reports or in the Console, enter a comma-separated list of domain names in this field. For example, you could enter a domain of example.com. If NetVoyant discovers a device with a domain name of device5.example.com, it strips the domain suffix (example.com) from the device name. In the NetVoyant Console, the device is named device5.

- 4. Click **Set** to save your changes.



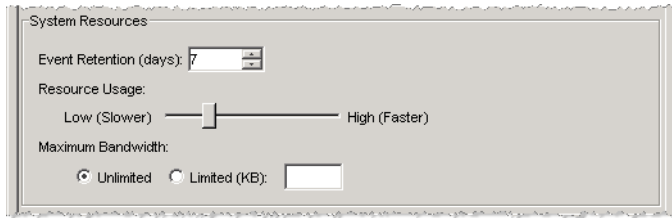
## Configuring the System Resources Parameters

Use the System Resources Parameters in the **Discovery** tab to specify how the NetVoyant product handles event retention and system bandwidth during rediscovery.

### To configure system resource parameters:

1. In the NetVoyant Console (Master or standalone), click the **Config** tab.
2. Expand the Master server and select **Discovery**.

The discovery options appear in the context panel.



3. Scroll if necessary and edit the following **System Resources** parameters as required:

Parameter	Description
<b>Event Retention (days)</b>	<p>To control how long topology change logs are retained, set the number of days in this field. In distributed systems, pollers retain any polling changes for the length of time indicated here.</p> <p>If a poller loses connectivity with the Master, topology change logs enable it to communicate topology changes that it discovers during this lapse in connectivity.</p>
<b>Resource Usage</b>	<p>To configure how many process threads and memory is allocated to the discovery process, change the slide bar setting for Resource Usage.</p> <p><b>Low (Slower)</b> values are the minimum values for these resources recommended for discovery to occur. A low value results in a slower discovery process. A high value results in a faster discovery process, but could impact reporting processes because of memory allocation.</p>
<b>Maximum Bandwidth</b>	<p>To restrict the amount of bandwidth that is allocated for the discovery process, select <b>Limited</b> and enter a maximum bandwidth in KB. By default, discovery is not restricted by bandwidth.</p>

4. Click **Set** to save your changes.

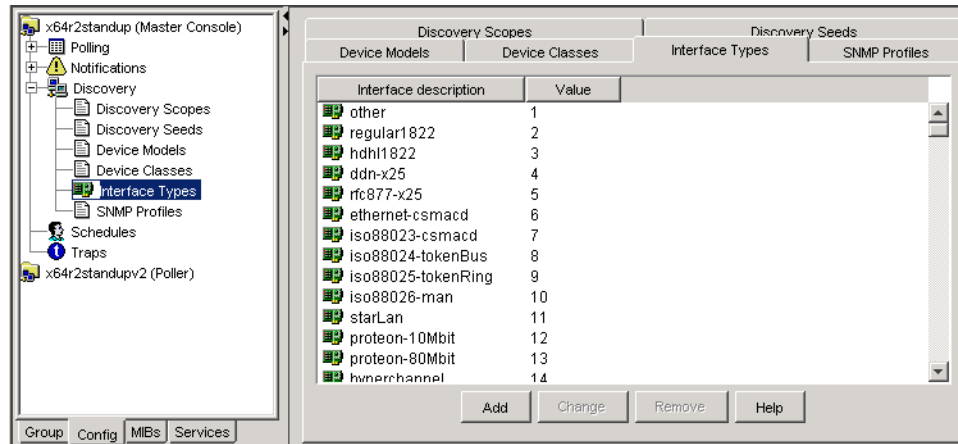
## Configuring Interface Types

The NetVoyant product has a preconfigured list of known interface types; however, you can add new interface types, change the identifying value for existing interface types, or completely remove interface types. To control how it identifies interfaces by `ifType`, you can add, edit, or remove interface types in the NetVoyant Console.

### To add or edit an interface type:

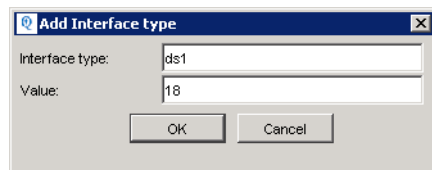
1. In the NetVoyant Console (Master or standalone), click the **Config** tab.
2. Expand the Master server.

3. Expand **Discovery** and select **Interface Types**.



4. In the context panel, do one of the following:

- To add a new interface type, click **Add**. This opens the **Add Interface Type** dialog box.
- To edit an existing interface type, select the interface type and click **Change**. This opens the **Change Interface Type** dialog box.



5. Enter or edit the following parameters as required:

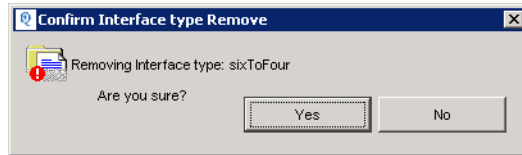
Parameter	Description
<b>Interface type</b>	For a new interface type, enter the name of the interface type in the Interface type field.
<b>Value</b>	Enter or edit the value for the Interface type. This is the value used in the ifType OID (or similar).

6. Click **OK**.

The NetVoyant product discovers new devices interface type according to your changes.

**To remove an interface type:**

1. In the NetVoyant Console (master or standalone), click the **Config** tab.
2. Expand the Master Console.
3. Expand **Discovery** and select **Interface Types**.
4. In the context panel, select the interface type from the list.
5. Click **Remove**.
6. In the confirmation dialog box, click **Yes**.



## CONFIGURING DEVICE CLASSES AND MODELS

The NetVoyant product determines the model of a device that it discovers by looking at the device's `sysObjectID`. It then determines the class of the device based on the device model.

As an administrator, you can configure how the NetVoyant product classifies discovered devices and enables polling of newly-discovered devices by performing the following tasks:

Task	Purpose	More information
Add a device class.	To control how the NetVoyant product identifies devices by class.	"Changing a Device's Classification" on page 61
Remove a device class.	To control how the NetVoyant product identifies devices by class.	"Removing a Device Class" on page 62
Add, edit, or remove a device model.	To control how the NetVoyant product identifies devices by model.	"Adding or Editing a Device Model" on page 63
Enable or disable polling for a device class.	To control the types of devices from which the NetVoyant poller automatically collects data.	"Enabling or Disabling Polling for a Device Class" on page 45
Enable or disable polling for a device model.	To control the types of devices from which the NetVoyant poller automatically collects data.	"Enabling or Disabling Polling for a Device Model" on page 64

## NetVoyant Device Classifications

The NetVoyant product automatically classifies new devices it discovers according to device model and class. Device classification helps determine the appropriate device group for each new device. For example, it places a device identified as a router in the Routers group.

Device class and model information also determine whether the NetVoyant product automatically enables or disables polling for new devices. You can disable polling for device classes or models to control how it gathers information from your network. And you can select the device models or classes that it automatically enables for polling upon discovery.

### Default Device Classes

The NetVoyant product includes a preconfigured list of known device models and their related sysObjectIDs; however, you can add new device models, change the class or sysObjectID for device models, or completely remove device models to control how the NetVoyant product classifies new devices that it discovers.

Default device classes include the following:

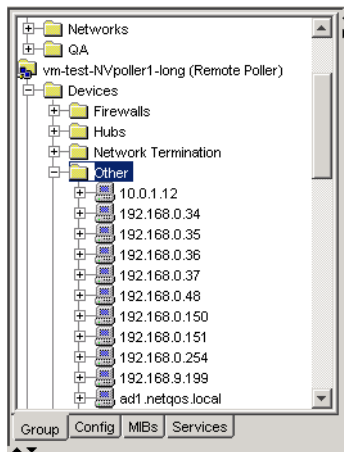
- Other
- Routers
- Hubs
- Probes
- Servers
- Workstations
- Printers
- Switches
- Network Termination
- Firewalls

### The “Other” Device Class

The NetVoyant product places all devices that it does not recognize as an identified device class in the Other device class. This happens when one of the following is true:

- The device is a model that it does not recognize.
- You removed the device class to which the device model belongs.

**Warning:** Do not remove the “Other” device class.



To help the NetVoyant product classify devices better, you can:

- Add device classes and assign device models to that class. For more information, see [“Changing a Device’s Classification” on page 61](#).
- Add device models to the NetVoyant Console and assign them to appropriate device classes. For more information, see [“Adding or Editing a Device Model” on page 63](#).

## Changing a Device’s Classification

You can change the device class assigned by the NetVoyant product. For example, if it assigned a router in the Other device class, you can manually re-assign it to the correct Routers device class for that device model.

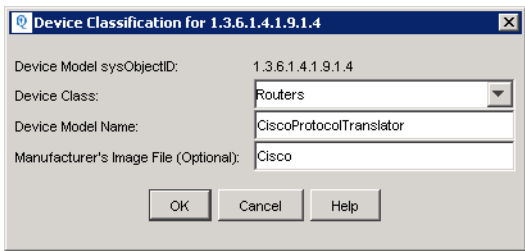
**Note:** You cannot change the device class for a generic device model. Devices with a `sysObjectID` such as 1.3.6.1.4.1.x, or with the term “generic” in the Device Model Name typically fall into this category.

### To change the device class for a device model:

1. In the NetVoyant Console (Master or standalone), click the **Config** tab.
2. Expand the Master server.
3. Expand **Discovery** and select **Device Models**.
4. Perform one of the following actions:
  - To add a device model and assign it to a device class, click **Add**.
  - To edit an existing device model and assign it to another device class, select the device model and click **Change**.

Alternatively, you can select a mis-classified device in the **Group** tab, right-click, and select **Change Classification** from the pop-up menu.

The **Device Classification** dialog box opens.



5. Enter or edit the following parameters:

Parameter	Description
<b>Device Model sysObjectID</b>	For a new device model, enter the sysObjectID. The device's SNMP agent uniquely identifies the device model using the sysObjectID. See your device's documentation to locate this number.
<b>Device Class</b>	Select the new Device Class; for example, Routers.
<b>Device Model Name</b>	The Device Model Name refers to the equipment model's name. For example, HP LaserJet Printer.
<b>Manufacturer's Image File</b>	<i>(Optional)</i> Enter the name of the device manufacturer's image file to control the icon that the NetVoyant Console displays for devices of this model on the <b>Group</b> tab. If you do not enter a custom image file, it displays the default icon for the device class. <b>Note:</b> Place the GIF image in the D:\NetVoyant\classes\redpoint\images directory on the NetVoyant server.

6. When you are finished defining or editing the device model, click **OK**.  
This creates the new device class and assigns this device model to the device class.
7. Repeat step 3 through 5 to assign more device models to the device class.  
After the initial device, when editing a device model, you can select the new device class from the Device Class list.
8. To view the device class, click the **Device Class** tab.

Removing a Device Class

If you remove a device class, the NetVoyant product defines all devices of this class as part of the Other device class and continues to poll devices in this device class that are not disabled from polling. Later, if you want to add the device class back into the NetVoyant product, you must manually recreate the device class by adding a new device class and reassigning device models.

**Warning:** It is strongly recommended that you do not remove device classes from the NetVoyant product. If you do not want the NetVoyant product to poll a device class, perform the following tasks instead of removing the device class:

Task	More Information
Disable the device class from polling so that new devices in this device class are disabled from polling.	<a href="#">“Enabling or Disabling Polling for a Device Class” on page 45</a>
Disable polling of all datasets for the device group that contains this device class so that current devices in this device class are disabled from polling.	<a href="#">“Configuring Polling for a Group” on page 123</a>

**Important:** Before removing a device class, assign each device model in the class to a different device class.

### To remove a device class from NetVoyant:

1. In the NetVoyant Console (Master or standalone), click the **Config** tab.
2. Expand the Master server.
3. Expand **Discovery** and select **Device Classes**.
4. In the list of device classes, select the device class and click **Remove**.

The NetVoyant product removes the device class and assigns all device models in this device class to the Other device class.

## Adding or Editing a Device Model

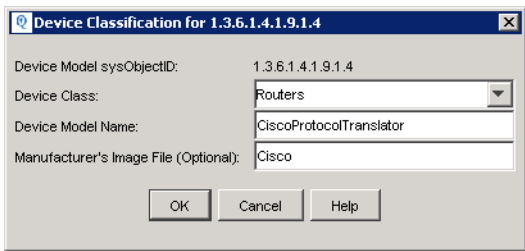
The NetVoyant product includes a preconfigured list of known device models; however, you can control how it identifies devices by model. You can add, edit, or remove device models in the NetVoyant Console by performing the following tasks:

- **Add new device models.** To add a new device model, you must know the associated `sysObjectID`. The device’s SNMP agent uniquely identifies the device model using the `sysObjectID`. See your device’s documentation to locate this number.
- **Change the class or `sysObjectID` for device models.**
- **Change how device models are placed into NetVoyant groups.**
- **Remove device models.** It is recommended that you do not remove device models from the NetVoyant product. If you remove a device model, it defines all devices of this model as part of the Other device class. If you later want to add the device model back into the NetVoyant product, you must manually recreate the device model using the `sysObjectID`.

### To add or edit a device model:

1. In the NetVoyant Console, click the **Config** tab.
2. Expand the Master Console, expand **Discovery**, and select **Device Models**.
3. Perform one of the following actions:
  - To add a new device model, click **Add**.
  - To edit an existing device model, select the device model and click **Change**.

The **Device Classification** dialog box opens.



4. Enter or edit the following parameters:

Parameter	Description
Device Model sysObjectID	For a new device model, enter the sysObjectID. The device’s SNMP agent uniquely identifies the device model using the sysObject ID. See your device’s documentation to locate this number.
Device Class	Select the Device Class for this device model; for example, Routers.
Device Model Name	The Device Model Name refers to the equipment model’s name; for example, HP LaserJet Printer.
Manufacturer’s Image File	<i>(Optional)</i> Enter the name of the device manufacturer’s image file to control the icon that the NetVoyant product displays for devices of this model on the <b>Group</b> tab.  If you do not enter a custom image file, it displays the default icon for the device class.  <b>Note:</b> Place the GIF image file in the D:\NetVoyant\classes\redpoint\images directory on the NetVoyant server.

5. When you finish defining or editing the device model, click **OK**.

**Warning:** It is strongly recommended that you do not remove device models from the NetVoyant product. If you remove a device model, the NetVoyant product defines all devices of this model as part of the “Other” device class. If you later want to add the device model back into the NetVoyant product, you must manually recreate the device model using the sysObject ID.

### Enabling or Disabling Polling for a Device Model

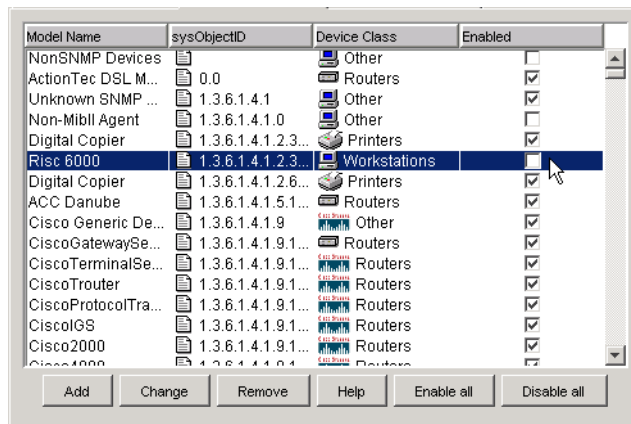
To control the types of devices from which the NetVoyant product collects data, you can select which device classes and device models are automatically enabled for polling upon discovery. The NetVoyant product discovers all devices within your discovery scope; however, it does not automatically enable polling for those device classes or models that you choose to exclude from polling. It does not gather data from these devices unless you specifically enable polling for them after discovery.

**Note:** Enabling or disabling polling for a device model does not affect polling for devices that the NetVoyant product has already discovered. When you disable a device model, it disables polling for new devices of this model when they are discovered. When you enable a device model, it enables polling for new devices of this model when they are discovered.



**To select the device models that are polled:**

1. In the NetVoyant Console, click the **Config** tab.
2. Expand the Master server and select **Discovery** beneath it.
3. Select **Device Models**.
4. Perform the following tasks to designate which models are enabled for polling:
  - To turn off polling, clear the **Enabled** check box next to the device model name.
  - To turn on polling for a device model that is disabled, select the **Enabled** check box.



## TROUBLESHOOTING NETVOYANT CONFIGURATION

The following questions and answers address some of the issues that might arise during NetVoyant configuration and discovery.

### **Q. The NetVoyant product did not discover devices. What's wrong?**

**A.** The following are some possible reasons why the NetVoyant product does not discover devices:

- You did not enter the correct SNMP profile information for your SNMP agents. For more information, see [“Adding SNMP Profiles to the Console” on page 34](#).
- Your devices might require that SNMP pollers be added to their access control list. For more information, see the next question and answer.
- You did not enter a correct discovery scope. The addresses and masks might be too restrictive. For more information, see [“Configuring the Discovery Scopes” on page 40](#).
- You might need to increase the timeout or retries for discovery. For more information, see [“Configuring Discovery Options” on page 52](#).
- You might have discovered devices, but not enabled them for polling. If you are not seeing some of your devices in the NetVoyant Console, you might not be showing devices that are disabled for polling. For more information, see [“Enabling and Disabling Polling” on page 85](#).

**Q. What is a Device Access Control List?**

**A.** Many routers and other network connectivity devices require that the address of SNMP pollers be entered into the device's access control list.

The access control list typically contains a list of trusted hosts that the device responds to using SNMP. You might need to add the NetVoyant poller that polls a device (distributed) or the Master Console (standalone) to the access control list for the device. Configuration of the access control list is typically performed using a proprietary interface to the router. Please check your device's documentation for assistance with this task.

**Q. I completed the Configuration Wizard. Why is there no data available in NetVoyant reports?**

**A.** The NetVoyant product does not collect data until the first polling cycle is initiated. The rolled up data that is presented in NetVoyant reports is generally not available until two rollup periods have passed (two hours by default).

The following are additional possible reasons that you do not see data:

- All of your poll instances are disabled. The NetVoyant product only collects data for enabled poll instances. For more information, see [“Configuring Polling for Poll Instances and Interfaces” on page 166](#).
- You might need to increase the SNMP timeout and retries for certain devices, such as devices across a slow WAN link. For more information, see [“Editing Discovery Settings for a Device” on page 150](#).

# Configuring Data Collection and Retention

---

The NetVoyant product organizes data that it collects from your devices and determines how it collects that data according to datasets. Each dataset is based on exactly one MIB table, from which data for that dataset is collected. In the NetVoyant Console, you configure polling, data retention, and baselines by dataset.

The NetVoyant product is pre-configured with many general-purpose datasets. These include Device Availability, Interface Statistics, Frame Relay Circuit Statistics, T1, T3, Cisco System Resources, Host Resource Storage, and others.

This chapter covers the following topics:

- [“NetVoyant Data Collection and Storage” on page 68](#)
- [“Managing Dataset Properties” on page 71](#)
- [“Creating and Configuring Custom Datasets” on page 80](#)
- [“Configuring Data Collection Frequency” on page 94](#)
- [“Configuring Data Rollup and Retention” on page 99](#)
- [“Configuring What Data to Gather” on page 104](#)

## NETVOYANT DATA COLLECTION AND STORAGE

The NetVoyant product organizes data that it collects from your managed devices according to datasets. It correlates each dataset with a MIB table and stores data that it gathers from a MIB table in a poll table in the correlated dataset.

For example, the NetVoyant Topology service obtains information for the Host Resource Storage dataset from the `hrStorageEntry` table, which is defined in the Host Resources MIB. If it polls a server for data stored in the `hrStorageEntry` MIB table, it stores the collected data in the Storage poll table in the Host Resource Storage dataset.

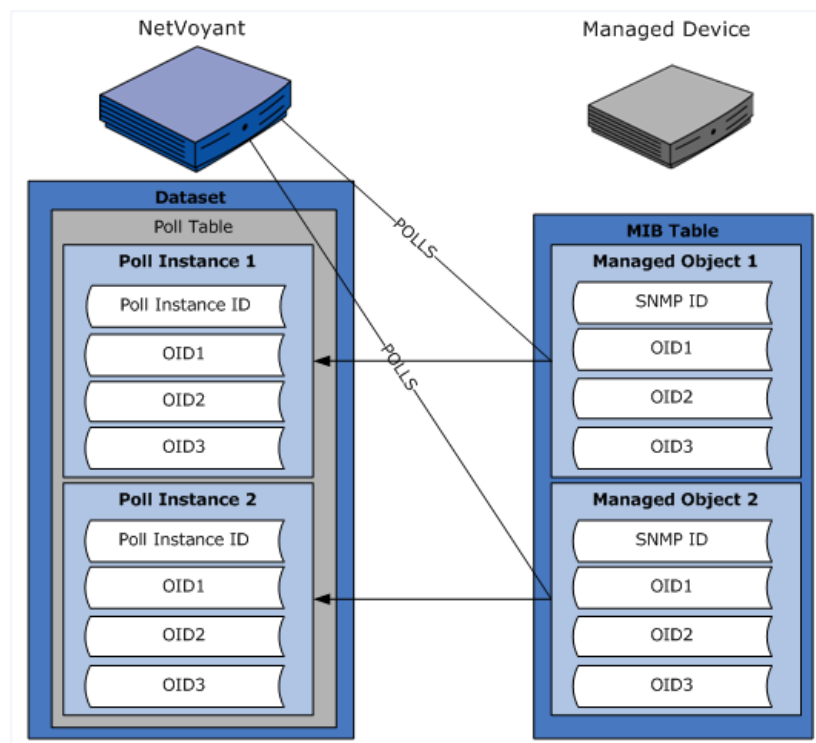
### Data Organization by Poll Instance

A MIB uses object identifiers (OIDs) to label each type of data that it describes. An OID is a permanent, unique name assigned to an object for storage (persistence).

When the NetVoyant Topology service gathers data from a device, it correlates all OID-labeled data for one managed object with one poll instance. If it gathers data from your server that supports the Host Resources MIB, it correlates data for all OIDs in that MIB (`hrStorageSize`, `hrStorageUsed`, `hrStorageAllocationFailures`) for one hard drive with one poll instance. The NetVoyant product correlates all data for all OIDs for another hard drive with a separate poll instance. If a device collects data for a polled MIB table from four managed objects, it has four correlated poll instances.

The following diagram provides a visual representation of how the NetVoyant product gathers data from a MIB table on a device and organizes it by poll instance, poll table, and dataset.

*NetVoyant data is organized by dataset, poll table, and poll instance.*

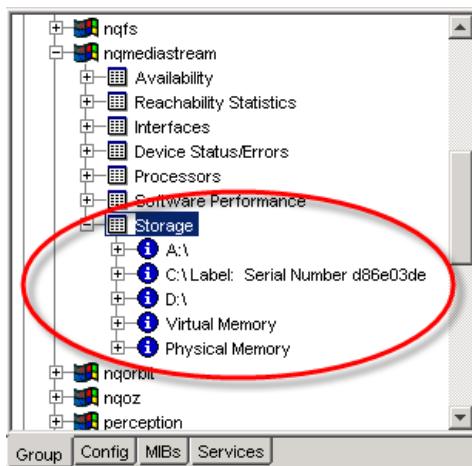


## Viewing and Configuring Data by Poll Instance

The NetVoyant product organizes poll instances and poll tables in the NetVoyant Console so that you can view your data organized by device, poll table, and poll instance. If a device supports a MIB table that is correlated with a dataset in the NetVoyant product, then it displays a poll table with poll instances for that dataset below the device on the **Group** tab of the NetVoyant Console.

For example, if a server supports the Host Resources MIB, the server displays a poll table called Storage when you select the server in the Group tab of the NetVoyant Console and expand it. This poll table contains several poll instances, each representing the data collected from a managed object on the server.

*Poll instances in the Storage poll table for the nqmediastream server*



If you want to configure how the NetVoyant product collects a certain type of data for a managed object on a device, you can configure settings for the related poll instance. For example, you could apply a polling group with a five minute polling rate to the Virtual Memory poll instance shown in the preceding figure. The NetVoyant product then gathers data about Virtual Memory from the hrStorageEntry MIB table on the nqmediastream server every five minutes.

In the NetVoyant product, you configure polling, data retention, baselines, and data validation by dataset. To configure how it gathers and stores data, you can perform the following tasks:

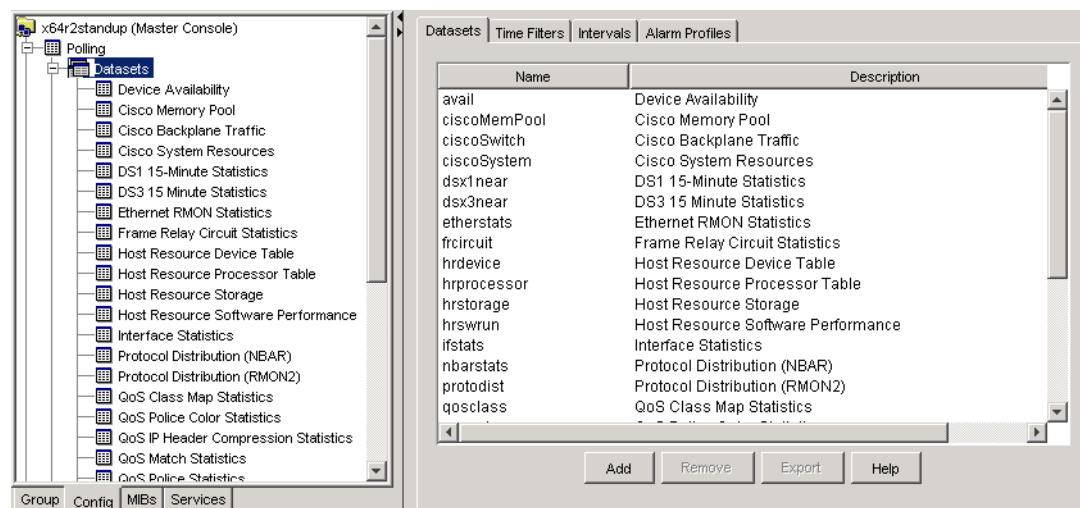
Task type	Task specifics	More information
Edit an existing dataset.	Edit configuration options for an existing dataset.	<a href="#">“Managing Dataset Properties” on page 71</a>
Create a custom dataset	To add functionality by compiling additional MIBs into the NetVoyant product, you must also create custom datasets in the NetVoyant Console based on the MIB tables from which you want to gather data.	<a href="#">“Creating and Configuring Custom Datasets” on page 80</a>

Task type	Task specifics	More information
Configure what data the NetVoyant product gathers for a dataset.	Create or edit the expressions that are gathered from the MIB table for the dataset.	“Creating or Editing a Dataset Expression” on page 105
	Add or edit baselines for the expressions in the dataset.	“Adding and Editing Baselines in the NetVoyant Console” on page 108
	Create data validation rules to ensure the integrity of the data.	“Using Data Validation Rules” on page 112
Configure the frequency for gathering the data for a dataset.	Create or edit polling groups that can be applied to poll instances in the dataset.	“Creating or Editing a Polling Group” on page 94
	Set a default polling group for the dataset.	“Changing the Default Polling Group for a Dataset” on page 96
	Modify the polling intervals used by the poll instances in the dataset.	“Configuring the Frequency for Polling and Rollups” on page 94
Configure how long the NetVoyant database retains data for a dataset.	Editing the rollup frequency or retention time for data in the dataset by editing the rollup settings for the dataset’s polling groups.	“Configuring Data Rollup and Retention” on page 99

## MANAGING DATASET PROPERTIES

You can configure basic parameters for a dataset such as the description of the dataset that is visible in the NetVoyant Console. You can also enable or disable discovery for a dataset and configure how the NetVoyant system discovers and names poll instances in a dataset.

View the list of existing datasets on the Master server (or a standalone) by selecting the **Config** tab and expanding **Polling > Datasets**.



**Note:** If you have a distributed NetVoyant system, all changes to datasets must be done on the Master.

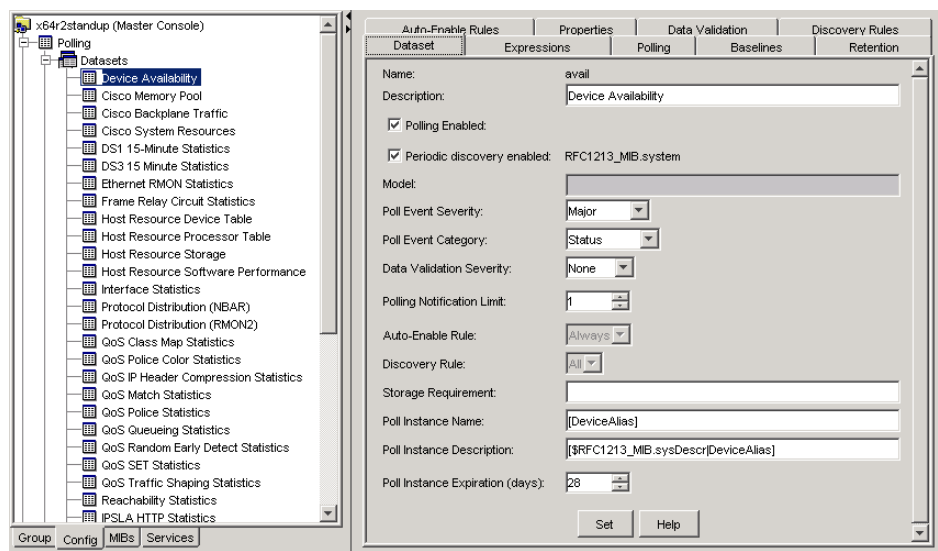
### Editing Dataset Details

The **Dataset** panel contains a number of settings for the dataset. These settings determine whether the NetVoyant system polls for the dataset, how it discovers and enables new poll instances for the dataset, and handling of polling events associated with the dataset. You can modify the settings for a default dataset or for custom datasets that you have created.

#### To edit detail settings for an existing dataset:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling > Datasets** and select the dataset.

The dataset's details appear in the context panel.



3. Enter or edit the following parameters:

Parameter	Description
<b>Description</b>	(Optional) Enter or edit the description of the dataset.
<b>Polling Enabled</b>	Select this check box to enable polling for the dataset. Clear the check box to disable polling for the dataset. For more information, see “Enabling and Disabling Polling for Datasets” on page 86.
<b>Periodic discovery enabled</b>	Select this check box to enable discovery for the dataset. For more information, see “Managing Discovery for a Dataset” on page 74.
<b>Model</b>	(Optional) Use this parameter to specify a string for selective discovery of poll instances. When specified, only devices with a matching sysObjectID are queried by the NetVoyant system to discover new poll instances. For more information, see “Selective Discovery by Device ID” on page 75. <b>Note:</b> Some standard datasets do not honor this setting and some others have a required setting. In these cases, the string cannot be specified or changed.
<b>Poll Event Severity</b>	Select a severity level from the list to control the severity that is assigned to polling failures for this dataset. The default setting for most datasets is <b>Unavailable</b> , to indicate that the device was unavailable for polling. If the NetVoyant product is not able to poll a device that supports the data in this dataset, it assigns the poll event severity for the dataset to this event and sends notifications that you have configured for poll events of this severity level. <b>Note:</b> If your NetVoyant system is registered with the NetQoS Performance Center as a data source, this severity level is reported in the Map and Map Event List.



Parameter	Description
<b>Poll Event Category</b>	<p>Use this setting to assign a category for poll events associated with the dataset.</p> <p><b>Note:</b> If your NetVoyant system is registered with the NetQoS Performance Center as a data source, this category is used to filter events in the Map and Map Event List.</p>
<b>Data Validation Severity</b>	<p>Use this drop-down list to set the severity associated with data validation log messages. Set this to <b>None</b> to turn off the logging of these messages for the dataset.</p>
<b>Polling Notification Limit</b>	<p><i>(Optional)</i> Enter the number of poll cycles for which the NetVoyant product is able to send a notification for a polling alarm. For more information, see <a href="#">“Using Polling Notification Limits” on page 249</a>.</p> <p><b>Note:</b> Setting a larger number of poll cycles raises the amount of traffic between the NetVoyant Polling and Notify services and the amount of database records required for exception reports. For more information about NetVoyant services, see <a href="#">“Managing NetVoyant Services” on page 279</a>.</p>
<b>Auto-enable Rule</b>	<p><i>(Optional)</i> Select whether you want to restrict polling on discovered poll instances in this dataset based on an auto-enable polling rule.</p> <p>This option is only configurable if you have created auto-enable polling rules for the dataset. For more information, see <a href="#">“Using Auto-Enable Polling” on page 88</a>.</p> <p><b>Note:</b> Auto-enable polling rules are created by default for the Interface Statistics dataset.</p>
<b>Discovery Rule</b>	<p><i>(Optional)</i> Set this option if you want to restrict discovery of poll instances for the dataset based on a discovery rule. The default setting, <b>All</b>, indicates that no discovery rules are applied and all poll instances are discovered.</p> <p>This option is only configurable if you have created discovery rules for the dataset. For more information, see <a href="#">“Selective Discovery by Poll Instance” on page 76</a>.</p>
<b>Storage Requirement</b>	<p><i>(Optional)</i> Enter an expression to dynamically restrict database storage for poll instances in the dataset.</p> <p>For more information, see <a href="#">“Restricting Database Storage” on page 103</a>.</p>
<b>Poll Instance Name</b>	<p><i>(Optional)</i> Enter the default name for poll instances in this dataset. You can use any OIDs in the MIB table for the dataset to create dynamically generated poll instance names.</p> <p>For more information, see <a href="#">“Naming Poll Instances and Interfaces” on page 78</a>.</p>

Parameter	Description
<b>Poll Instance Description</b>	<p>(Optional) Enter the default description for poll instances in this dataset. You can use any OIDs in the MIB table for the dataset to create dynamically generated poll instance descriptions.</p> <p>For more information, see <a href="#">“Naming Poll Instances and Interfaces” on page 78</a>.</p>
<b>Poll Instance Expiration (days)</b>	<p>Modify this setting to change the number of days that a poll instance for the dataset remains in the system when it is scheduled to be deleted (“time-to-live” expiration). When the number of days has transpired, the poll instance is automatically removed at the next discovery cycle unless its state has changed.</p> <p>For more information, see <a href="#">“Polling Status and Expiration” on page 161</a>.</p>

4. Click **Set** to save your changes to the dataset.

## Managing Discovery for a Dataset

By default, all datasets are included in rediscovery. If you do not want to discover any new poll instances for a dataset, you can disable discovery for that dataset. If you do not want to gather any data associated with a particular dataset, including existing poll instances, you can also disable polling of the dataset. For more information about disabling polling for the dataset, see [“Enabling and Disabling Polling for Datasets” on page 86](#).

When a dataset is enabled for discovery, the NetVoyant system discovers all poll instances and interfaces on all discovered devices. However, you can implement selective discovery to control which datasets are tested against a device during discovery.

In the NetVoyant Console, you can also control how the NetVoyant system names the discovered poll instances and interfaces.

### Enabling and Disabling Dataset Discovery

To remove a dataset from automatic rediscovery, you can disable discovery on the dataset’s **Details** tab. If you disable discovery, the NetVoyant product does not queue or update information related to this dataset during periodic rediscovery.

#### To enable or disable discovery for a dataset:

1. In the **Config** tab of the NetVoyant Console, expand the Master Console.
2. Expand **Polling > Datasets** and select the dataset.  
The dataset’s details appear in the context panel.
3. Change the option selection to enable or disable periodic discovery:
  - To disable the dataset for discovery, clear the **Periodic discovery enabled** check box.
  - To enable the dataset for discovery, select the **Periodic discovery enabled** check box.

The screenshot shows the configuration window for the 'avail' dataset. The 'Periodic discovery enabled' checkbox is checked and circled in red. The 'Model' field is empty. Other fields include Name: avail, Description: Device Availability, Polling Enabled: checked, Poll Event Severity: Major, Poll Event Category: Status, and Data Validation Severity: None.

4. Click **Set** at the bottom of the context panel to apply your changes.

## Selective Discovery by Device ID

In the NetVoyant Console, the **Dataset** tab for a selected dataset displays a **Model** parameter. This parameter controls which devices are tested against the dataset during discovery. When this parameter contains a specified string, only those devices with a matching `sysObjectID` will be queried for poll instances for the dataset.

This parameter takes a single entry (multiple entries cannot be specified) as a free-format string and the NetVoyant Console does not perform any specific data validation. If the specified string does not match the device's `sysObjectID`, or the beginning of its `sysObjectID`, the discovery of the dataset is skipped for that device.

Some of the more global datasets, such as Device Availability, Reachability, and Interface Statistics, do not honor this setting and a string cannot be specified. For other datasets where the NetVoyant product utilizes custom discovery code (such as NBAR and Cisco CB QoS), this parameter is ignored.

There are some standard datasets that are specific to Cisco MIBs (IPSLA, Memory Pool, System, and Backplane) where the model is already specified and cannot be modified. For example, in the Cisco Backplane Traffic dataset, only devices that have a `sysObjectID` starting with 1.3.6.1.4.1.9 are queried for `sysTrafficMeterEntry` poll instances. The result is that non-Cisco devices are not tested for this dataset.

The screenshot shows the configuration window for the 'ciscoSwitch' dataset. The 'Model' field is set to '1.3.6.1.4.1.9' and is circled in red. Other fields include Name: ciscoSwitch, Description: Cisco Backplane Traffic, Polling Enabled: checked, Periodic discovery enabled: checked, and Poll Event Severity: Minor.

Use this parameter to optimize the discovery process, particularly for custom datasets (MIBs) built for specific types of devices (such as F5, Nortel, and so on).

**Important:** Exercise caution when specifying a Model ID for common datasets. For example, it does not make sense to define an ID for the Frame Relay Circuit Statistics dataset because many different vendors support the standard Frame Relay MIB; however, the NetVoyant Console does allow an ID specification for this dataset, and if specified, it will be used.

## Selective Discovery by Poll Instance

In the NetVoyant Console, you can configure discovery rules for a dataset to control which poll instances are discovered based on OID variables. These discovery rules take the form of a “where” clause; for example, you could add the following clause as a discovery rule for the Interface Statistics (ifstats) dataset to limit discovery to certain types of interfaces:

```
ifType in (6, 20, 18, 45)
```

### Adding a Discovery Rule

You can add multiple discovery rules for a dataset on the **Discovery Rules** tab. Each rule is comprised of an SNMP requirement as an expression.

#### To create and apply a discovery rule for a dataset:

1. In the NetVoyant Console, expand the Master Console on the **Config** tab.
2. Expand **Polling > Datasets** and select the dataset.  
The details for the dataset appear in the context panel.
3. Click the **Discovery Rules** tab.
4. Click **Add** to add a rule for discovering poll instances or interfaces for that dataset.

This opens the **Add Expression** dialog box.

5. In the **Name** field, enter a descriptive name for the rule.
6. In the **SNMP Requirement** field, enter an expression that defines the discovery rule where the expression evaluates as true or false.

When the discovery rule is applied to the dataset, the NetVoyant Console limits discovery to those poll instances and interfaces for which the rule evaluates to true. For more information about constructing valid discovery rules, see the following section.

7. Click **OK** to add the rule name and expression to the Discovery Rules list for the dataset.
8. Click the **Datasets** tab to view the dataset’s details in the context panel.
9. From the **Discovery Rule** drop-down list, select the discovery rule.

Polling Notification Limit: 1  
 Auto-Enable Rule: Always  
 Discovery Rule: All  
 Storage Requirement: All  
 Poll Instance Name: loopback  
 Poll Instance Description: [ifName|ifDescr] - [portName|ifAlias]

10. Click **Set** to save your changes.

**Note:** If you want to delete a discovery rule for the dataset, it cannot be specifically selected (applied) in the **Dataset** tab.

### Constructing Discovery Rules

When constructing an SNMP requirement expression for a discovery rule, you are restricted to using the dataset OIDs as variables. This restriction is based on the tables that are queried during discovery for each dataset. For more information about creating expressions in the NetVoyant Console, see [“Creating or Editing a Dataset Expression” on page 105](#).

**Note:** If the dataset is part of a parent/child relationship (such as CBQoS), child poll instances are added even when the parent was skipped because of a discovery rule. However, this is not the case for interface types, such as T1 subinterfaces and DSX1/DSX3 poll instances.

The following is an expression for a Loopback discovery rule created for the Interface Statistics (ifstats) dataset:

```
ifType NOT IN ('24','0') AND ifSpeed > 0
```

Rule Name	Rule Expression
ifSpeed	ifSpeed > 0 AND ifDescr NOT LIKE "Loopback" OR ifDescr NOT LIKE "Null"
loopback	ifType NOT IN ('24','0') AND ifSpeed > 0

This rule evaluates as true for interfaces that are not loopbacks and have valid interface type values. If you apply this discovery rule to the Interface Statistics dataset, the NetVoyant product discovers or rediscovers only those interfaces that satisfy these requirements.

**Important:** This must result in a valid SnmpQL query. If the query is not valid, there will be **no** poll instances discovered for that particular dataset. If you have the logging level set to 4 or higher, you can use the **Test** button at the bottom of the **Add Expression** or **Change Expression** dialog box to test the validity before you apply the discovery rule to a dataset.

## Naming Poll Instances and Interfaces

NetQoS NetVoyant reports display the names of poll instances and interfaces and the NetVoyant Console tree-tab panel displays the descriptions. Both name and description appear on the NetVoyant Console **Details** tab for each poll instance and interface.

The screenshot shows the NetVoyant console interface. The top panel, titled "Interface List", displays a table of interfaces. The bottom panel shows the "Details" tab for a selected interface.

Name	ifType	ifIndex	Speed	Device	Polling Status	Polling Expiration
BethsRouter.QA.local - GigabitEthernet0/0/	ethernet-csmacd	1	1.00 Gbps	BethsRouter.QA.local	Enabled	Never
BethsRouter.QA.local - GigabitEthernet0/1/	ethernet-csmacd	2	100.00 Mbps	BethsRouter.QA.local	Enabled	Never
BethsRouter.QA.local - GigabitEthernet1/0/	ethernet-csmacd	3	1.00 Gbps	BethsRouter.QA.local	Enabled	Never
BethsRouter.QA.local - Null0	other	5	10.00 Gbps	BethsRouter.QA.local	Enabled	Never
Device155 - ATM Interface	ethernet-csmacd	1	100.00 Mbps	Device155	Enabled	Never
Device155 - cisco ls1010	atm	6	8.19 Mbps	Device155	Enabled	Never
Device155 - cisco ls1010	atm	2	8.19 Mbps	Device155	Enabled	Never
Device155 - edge network	ethernet-csmacd	4	100.00 Mbps	Device155	Enabled	Never
Device155 - Lab Backup	atm	3	8.19 Mbps	Device155	Enabled	Never
Device155 - Link to Nowhere	atm	5	8.19 Mbps	Device155	Enabled	Never

The bottom panel shows the "Details" tab for the selected interface "BethsRouter.QA.local - GigabitEthernet0/1/". The fields are as follows:

- Name: BethsRouter.QA.local - GigabitEthernet0/1/
- Description: GigabitEthernet0/1/
- Poling status: Enabled
- Poling rate: Fast (5 Mins)
- Polier: nvpoller
- ifIndex: 2
- ifDescr: GigabitEthernet0/1
- ifType: ethernet-csmacd
- ifPhysAddress: 00:1d:70:17:37:61
- Addresses: 10.0.7.9/24

By default, the name and description for a poll instance or interface is populated upon discovery using the name and description templates specified for the dataset. You can manually change the name or description for a specific poll instance or interface in the **Details** tab.

**Important:** If you manually change the contents of the **Name** or **Description** fields of a poll instance or interface, the name and description templates specified in the dataset are no longer applied to that poll instance or interface. To re-enable the name and description templates, delete the entries in these fields (blank) and save the poll instance or interface, then rediscover the device.

### Using the Poll Instance Name and Description Templates

By default, the name and description for a poll instance or interface is populated upon discovery using the name and description templates specified for the dataset. For more information about specifying dataset details, see [“Editing Dataset Details” on page 71](#).

The screenshot shows the templates for the Poll Instance Name and Description. The fields are as follows:

- Poll Instance Name: [DeviceAlias]
- Poll Instance Description: [\$RFC1213\_MIB.sysDescr[DeviceAlias]]

When defining the name or description for poll instances and interfaces, you can use any of the OIDs defined in the MIB table upon which a dataset is based. You can also use two internal NetVoyant variables, `DeviceAlias` and `DeviceName`, which dynamically map to the device's alias and name respectively upon discovery.

A parameter/variable is specified by enclosing it in brackets, such as `[DeviceAlias]`.

You can specify alternate parameters/variables by specifying them in order of priority, separated by pipes within the brackets, such as `[portname|ifAlias|ifName]`. In this example, the property uses the first parameter that has a populated value.

**Note:** When you specify the template for the **Poll Instance Description** in the Interface Statistics dataset, it determines the naming of interfaces for NetVoyant reports and for cross-product reporting in the NetQoS Performance Center. For more information about modifying the description templates for interfaces, see the following section.

## Cross-Product Interface Naming

When your NetVoyant installation is bound to the NetQoS Performance Center as a data source, the description information for poll instances and interfaces is also displayed in the NetQoS Performance Center views.

When the NetQoS Performance Center has multiple product data sources, it can display views with aggregated information. The NetVoyant and ReporterAnalyzer products both provide data for interfaces. By default, these products use the same interface naming templates so that the NetQoS Performance Center can recognize when data applies to the same interface and can be aggregated.

Aggregate interface information and population of views in the NetQoS Performance Center are based on the template specified in the **Poll Instance Name** field for the Interface Statistics dataset. The default template is as follows:

```
[DeviceAlias]::[ifName|ifDescr] - [portName|ifAlias]
```

Other NetVoyant reporting views are based on the template specified in the **Poll Instance Description** field for the Interface Statistics dataset. The default template is as follows:

```
[ifName|ifDescr] - [portName|ifAlias]
```

If you are running NetVoyant and ReporterAnalyzer installations that are registered in the NetQoS Performance Center, be sure that you make identical changes to the templates for interfaces. If the product data sources use different templates, the NetQoS Performance Center will be unable to properly aggregate and report data for interfaces.

## CREATING AND CONFIGURING CUSTOM DATASETS

If you want to add functionality to the NetVoyant product by compiling additional MIBs, you must also create custom datasets in the NetVoyant Console based on the MIB tables from which you want to gather data. You can create a new dataset using the Dataset Wizard.

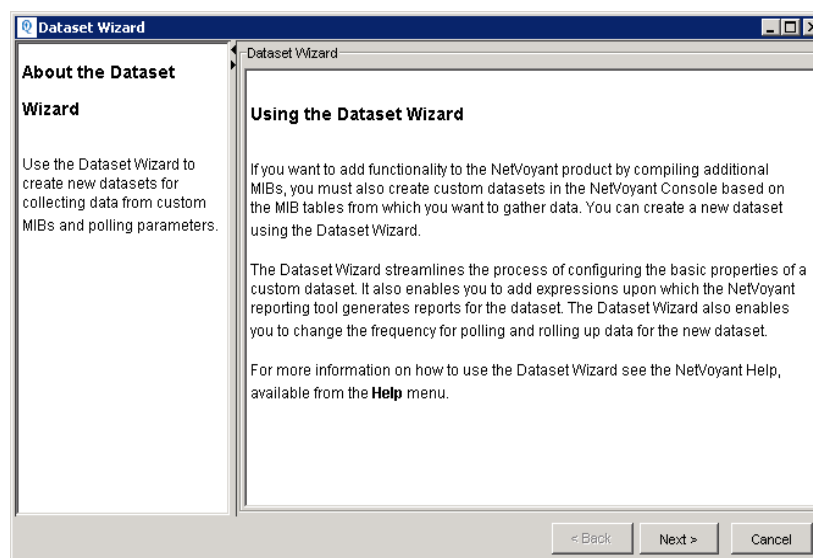
### Using the Dataset Wizard to Create a New Dataset

The Dataset Wizard streamlines the process of configuring the basic properties of a custom dataset. It also enables you to add expressions upon which the NetVoyant reporting tool generates reports for the dataset. You add the expressions to specify the data collected and customize the calculations used for reporting, thresholds, alarms, and notifications. Finally, the Dataset Wizard enables you to change the frequency for polling and rolling up data for the new dataset.

#### To use the Dataset Wizard to create a custom dataset:

1. From the **File** menu in the NetVoyant Console, select **New > Dataset**.

The **Dataset Wizard** opens.



2. Click **Next** to display the **MIBs** panel and select a MIB upon which to base the dataset.  
For more information, see “[Selecting a MIB in the Dataset Wizard](#)” on page 81.
3. Click **Next** to display the **Data Set** panel and configure the dataset and select a table from the MIB you selected in step 2.

For more information, see “[Managing Dataset Properties](#)” on page 71.

**Note:** You can edit configuration options after you exit the Dataset Wizard; however, you cannot change the MIB table upon which a dataset is based after the dataset has been created.

4. Click **Next** to display the **Expressions** panel and add expressions for the dataset based upon the OIDs in the MIB table you selected in step 3.

For more information, see “[Adding Expressions in the Dataset Wizard](#)” on page 82.



**Note:** You can add expressions after you exit the Dataset Wizard. For more information, see [“Creating or Editing a Dataset Expression” on page 105](#).

5. Click **Next** to display the **Poll Group List** panel and add polling groups and set a default polling group to define the frequency for polling and rolling up data for the dataset.

For more information, see [“Adding Polling Groups in the Dataset Wizard” on page 84](#).

**Note:** You can add and configure polling groups after you exit the Dataset Wizard. For more information, see [“Creating or Editing a Polling Group” on page 94](#).

6. Click **Next** to display the **Summary** panel and review the settings for the new dataset.
7. Click **Finish** to add the dataset and exit the wizard.

## Selecting a MIB in the Dataset Wizard

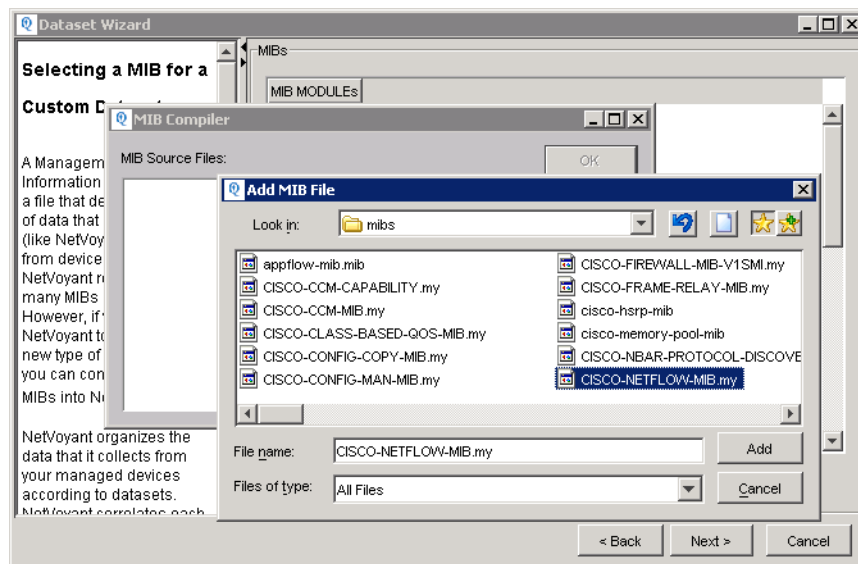
When selecting a MIB for a custom dataset, you can select an existing MIB (one that has already been compiled) or add a new MIB to your NetVoyant system.

Some MIBs have dependencies on other MIB modules. If you add a new MIB to the NetVoyant product, you must first compile its dependent MIBs. For more information about adding a new MIB to NetVoyant, see [“Adding MIBs to the NetVoyant Product” on page 185](#).

On a distributed system, datasets are synched from the Master server to the pollers, but only when the pollers are connected and running at the time a dataset is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

### To select a MIB for a new custom dataset:

1. Start the Dataset Wizard and click **Next** to display the **MIBs** panel.
2. Perform one of the following actions:
  - Select one of the pre-loaded MIBs from the list and skip to step 7.
  - Click **Add** to add a new MIB in the MIB Compiler and continue to step 3.
3. In the MIB Compiler, click **Add**.
4. Browse for and select the MIB source file and click **Add**.



The MIB source file is added to the list in the MIB Compiler.

5. Select the MIB source file and click **OK**.

This compiles the new MIB and adds it to the list of MIB modules in the Dataset Wizard.

6. Select the new MIB in the list of MIB Modules.
7. Click **Next** to continue through the rest of the Dataset Wizard.
8. On the last page of the wizard, click **Finish**.

## Adding Expressions in the Dataset Wizard

The NetVoyant product uses expressions in a dataset to create reportable data based upon the raw data collected from your devices. You can use the default expressions or create your own. If you create a custom dataset, you must also create the expressions used to render NetVoyant report views for the new dataset.

**Note:** There must be at least one expression in each dataset.

On a distributed system, datasets are synched from the Master server to the pollers, but only when the pollers are connected and running at the time a dataset is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

### To edit or add expressions to a new custom dataset:

1. Select **File > New > Dataset** to start the Dataset Wizard (Master or standalone).
2. Complete the steps until you reach the Expressions screen.
3. Perform one of the following tasks:
  - To add a new expression, click **Add**.
  - To edit an existing expression, select the expression and click **Change**.

The Expression editor opens.

OIDs	SYNTAX
availability	Expression
availability_bl	Expression
reboots	Expression
sysDescr	DisplayString
sysUpTime	TimeTicks
sysContact	DisplayString
sysName	DisplayString
sysLocation	DisplayString
sysServices	INTEGER

4. Enter or edit the following parameters:

Parameter	Description
<b>Name</b>	For a new expression, enter a name. The name is used to identify the expression in the NetVoyant product.
<b>Description</b>	Enter or edit the description for the expression. The description can help you identify what type of data an expression gathers.
<b>Expression Definition</b>	<p>Enter the expression in this field.</p> <ul style="list-style-type: none"> <li>To enter an OID, double-click the OID in the list or enter the OID name in the Expression Definition field. This list includes all the OIDs in the MIB table upon which the dataset is based.</li> <li>To enter an operator, click the operator button. You can also use the Operators listed in the Expression Editor. For more information about these operators, see <a href="#">“Changing Advanced Calculations for an Expression”</a> on page 107.</li> <li>To add a property, enter the name of the property preceded by a \$ symbol in the Expression Definition as in the following example: \$PropertyName. For more assistance with adding properties to your expression, see <a href="#">“Working with NetVoyant Properties”</a> on page 308.</li> </ul>

**Note:** Expressions can use the OIDs listed in the OID table at the right of the Expression editor.

OIDs	SYNTAX
availability	Expression
availability_bl	Expression
reboots	Expression
sysDescr	DisplayString
sysUpTime	TimeTicks
sysContact	DisplayString
sysName	DisplayString
sysLocation	DisplayString
sysServices	INTEGER

5. *(Optional)* To configure what types of calculations the NetVoyant product performs on the expression for use in NetVoyant report views, click **Advanced**.
  - a. Select the types of calculations you want performed. For more information on these calculations, see [“Changing Advanced Calculations for an Expression”](#) on page 107.
  - b. Click **OK**.
6. Click **Apply** to add the expression to the dataset and enter another expression.
7. Click **OK** to exit the Expression Editor.
8. Click **Next** to continue through the rest of the Dataset Wizard.
9. On the last page of the wizard, click **Finish**.

## Adding Polling Groups in the Dataset Wizard

In the NetVoyant product, a polling group defines the frequency for polling devices for a particular type of data, the intervals used for rolling up that data for reports, and how long to retain that data. By creating and editing polling groups, you can control the frequency of polls on your network, the relative granularity of your report data, and data retention time for your reports.

On a distributed system, polling groups are synched from the Master server to the pollers, but only when the pollers are connected and running at the time that polling groups are modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

### To add or edit polling groups for a new custom dataset:

1. Start the **Dataset Wizard** (Master or standalone).
2. Complete the steps until you reach the **Polling Group List** panel.
3. Perform one of the following actions:
  - To add a new polling group, click **Add**.
  - To edit an existing polling group, select the polling group and click **Change**.
4. In the **Add Poll Group** or **Edit Poll Group** dialog box, configure or edit the polling group.  
For more information, see [“Creating or Editing a Polling Group”](#) on page 94.
5. Click **OK**.
6. *(Optional)* Repeat steps 3 through 5 to add additional polling groups.  
**Note:** You can add and edit polling groups for the dataset after you exit the Dataset Wizard. For more information, see [“Creating or Editing a Polling Group”](#) on page 94.
7. Click **Next** to continue through the rest of the Dataset Wizard.
8. On the last page of the wizard, click **Finish**.

## ENABLING AND DISABLING POLLING

Within your discovery scope, the NetVoyant product polls all the SNMP devices that are enabled for polling. The NetVoyant Console provides a number of settings and features that you can use to determine what datasets and devices are enabled or disabled for polling and to monitor polling.

### Disabling Polling for Devices

If you want to stop polling a device or subset of devices, you can do any of the following:

Task	More information
Disable or enable polling by interface or poll instance on a device	<a href="#">“Configuring Polling for Poll Instances and Interfaces” on page 166</a>
Disable polling for a device.	<a href="#">“Changing the Polling Status for a Device” on page 148</a>
Disable polling for datasets that gather data from a device	<a href="#">“Enabling and Disabling Polling for Datasets” on page 86</a>
Disable polling for selected datasets in the network to which the device belongs	<a href="#">“Configuring a Polling Group for a Network” on page 124</a>
Disable polling for selected datasets in the group to which the device belongs	<a href="#">“Configuring Polling for a Group” on page 123</a>
Disable polling for a device class (the NetVoyant product automatically disables polling for new devices of this class that it discovers)	<a href="#">“Enabling or Disabling Polling for a Device Class” on page 45</a>
Disable polling for a device model. (the NetVoyant product automatically disables polling for new devices of this model that it discovers)	<a href="#">“Enabling or Disabling Polling for a Device Model” on page 64</a>
Disable all polling.	<a href="#">“Configuring Polling Settings” on page 85</a>

**Note:** To hide devices, poll instances, and interfaces that are disabled for polling in the NetVoyant Console, from the **View** menu, clear the **Show Disabled from Polling** option.

### Configuring Polling Settings

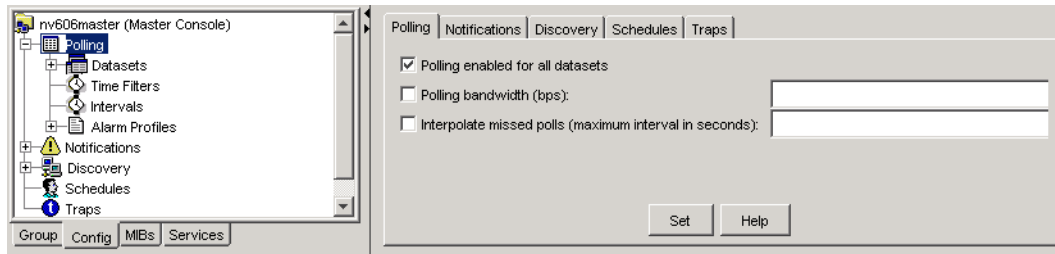
You can turn off all polling, reduce the bandwidth dedicated to polling, and configure how the NetVoyant product interpolates data for missed polls on the **Polling** tab.

On a distributed system, dataset polling settings are synched from the Master server to the pollers, but only when the pollers are connected and running at the time that polling settings are modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

#### To configure basic polling settings:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Select **Polling**.

This displays the **Polling** options appear in the context panel.



3. Edit the following parameters:

Parameter	Description
<b>Polling enabled for all datasets</b>	To disable polling for all datasets, clear this check box. This disables all gathering of data.
<b>Polling bandwidth</b>	To restrict the amount of bandwidth allocated for polling, select this check box and enter a bandwidth in bps. By default, polling is not restricted by bandwidth.
<b>Interpolate missed polls</b>	To enable the NetVoyant product to interpolate data for missed polls based on data before and after the missed polls, select this check box and enter the maximum interval in seconds for which you want to interpolate data. <b>Note:</b> If you enter too large an interval for interpolation, the interpolated data begins to lose reliability and accuracy.

4. Click **Set** to save your changes.

## Enabling and Disabling Polling for Datasets

To turn data collection for a dataset on or off, you can enable or disable polling for the entire dataset so that it applies to all poll instances. You can also enable or disable polling for a dataset within a specific device group so that it applies only to the poll instances within that group.

### Enabling and Disabling Polling Across Groups

On the **Config** tab in the NetVoyant Console, you can turn data collection on or off for a dataset so that it applies to all devices. Disabling polling for a dataset that you do not need is one way to make poll instance licenses available to other datasets that are of higher priority to your organization.

On a distributed system, dataset polling settings are synched from the Master server to the pollers, but only when the pollers are connected and running at the time that polling settings are modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

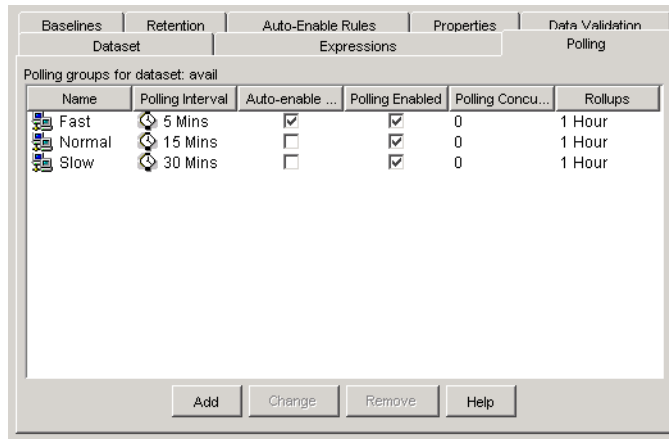
#### To enable or disable polling for a dataset across all groups:

1. In the NetVoyant Console (Master or standalone), expand the Master server on the **Config** tab.
2. Expand **Polling > Datasets** and select the dataset.

The details for the dataset appear in the context panel.

3. Perform one of the following tasks:

- To disable polling for a dataset, clear the **Polling Enabled** check box.
- To enable polling for a dataset, select the **Polling Enabled** check box.



4. Click **Set**.

## Changing Polling for a Dataset by Group

On the **Group** tab in the NetVoyant Console, you can turn data collection on or off for a specific dataset so that it applies to the devices in the group. Disabling polling by group for datasets that you do not need is one way to make poll instance licenses available to other datasets that are a higher priority to your organization.

On a distributed system, dataset polling settings are synched from the Master server to the pollers, but only when the pollers are connected and running at the time that polling settings are modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

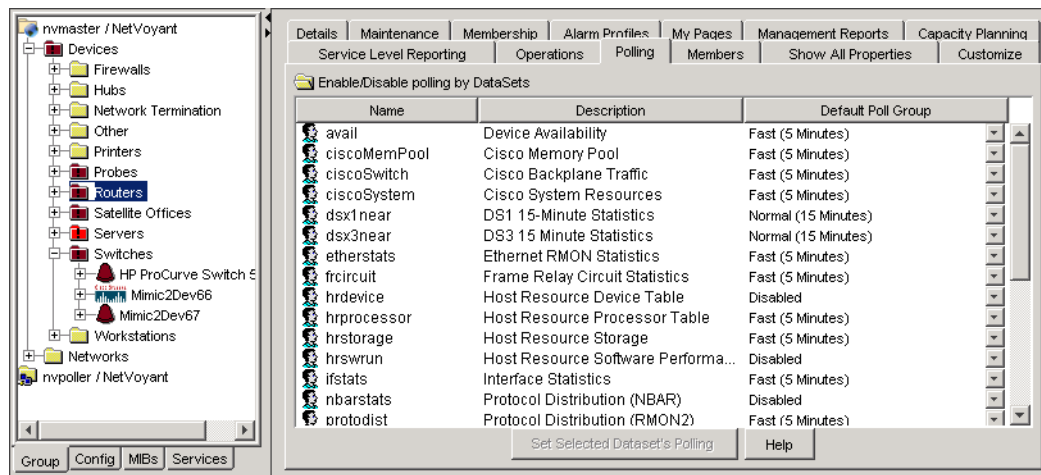
### To change polling for a dataset within a device group:

1. In the NetVoyant Console (Master or standalone), expand the group tree in the **Group** tab.
2. Select the group for which you want to change polling by dataset.

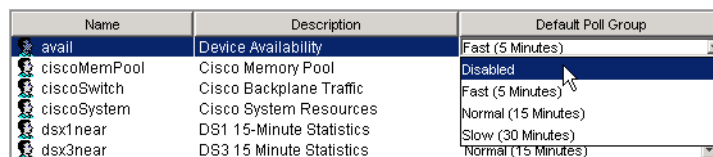
The details for the group appear in the context panel.

3. Click the **Polling** tab.

The context panel displays a list of all datasets with poll instances for the devices within the selected group.



4. In the context panel, select a dataset to be modified.
5. Click the drop-down arrow next to the default poll group for the selected dataset and choose a poll group setting:
  - To enable polling for a dataset, choose a polling group.
  - To disable polling for a dataset, select **Disabled**.



6. Click **Set Selected Dataset's Polling**.

## Using Auto-Enable Polling

Use the auto-enable polling feature to dynamically enable or disable polling for poll instances that the NetVoyant product discovers in a dataset based on the criteria that you set. For example, the following is an auto-enable rule that is created by default for the Interface Statistics dataset:

```
(ifInOctets+ifOutOctets)<>0
```

This rule checks interfaces for traffic and is named “Traffic Present.” If you apply this rule to the Interface Statistics dataset, when the NetVoyant product discovers or rediscovers interfaces, it only enables polling of the interface if the interface had traffic at any time.

Auto-enable polling rules are defined by default for the Interface Statistics dataset; however, you must activate auto-enabled polling for the Interface Statistics dataset in the **Dataset** tab for it to be applied. For all other datasets, you must create and name auto-enable polling rules before you can apply them to a dataset.

**Important:** If you modify an auto-enable rule that is applied to a dataset, you must open the dataset in the NetVoyant Console, select the **Auto-Enable Rules** tab, and click **Set** for the change to be applied to the dataset.



## Creating and Applying Auto-Enable Rules

In a distributed system, auto-enabled polling and auto-enable rules are automatically synched from the Master server to the pollers, but only when the pollers are connected and running at the time a rule is applied, added, or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

**Note:** Creating auto-enable polling rules for a dataset is an advanced configuration task. If an auto-enable rule is constructed improperly, it can result in all poll instances of a specified type being disabled. It is recommended that you contact NetQoS Technical Support for assistance with this task.

### To create and apply an auto-enable rule for polling a dataset:

1. In the NetVoyant Console (Master or standalone), expand the Master server on the **Config** tab.
2. Expand **Polling > Datasets** and select the dataset.

The details for the dataset appear in the context panel.

3. Click the **Auto-Enable Rules** tab.
4. Click **Add** to add a rule for automatically enabling polling for that dataset.

This opens the **Add Expression** dialog box.

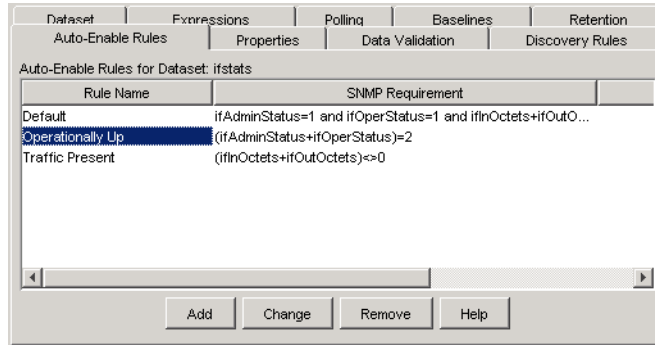
OIDs	SYNTAX
sysDescr	DisplayString
sysUpTime	TimeTicks
sysContact	DisplayString
sysName	DisplayString
sysLocation	DisplayString
sysServices	INTEGER

5. In the **Name** field, enter a descriptive name for the rule.
6. In the **SNMP Requirement** or **Properties Requirement** field, enter an expression that defines the auto-enable polling rule where the expression evaluates as true or false. When the auto-enable rule is activated for the dataset, the NetVoyant Console auto-enables polling for those poll instances for which the rule evaluates to true.

**Note:** When creating SNMP requirements for auto-enable polling rules, you can use object identifiers (OIDs) in the MIB table for the dataset. When creating property requirements for auto-enable polling, you can use any properties defined for the dataset on the **Properties** tab. For more information about creating expressions, see [“Creating or Editing a Dataset Expression”](#) on page 105.

The following is the expression for the Operationally Up auto-enable rule that is created by default for the Interface Statistics dataset:

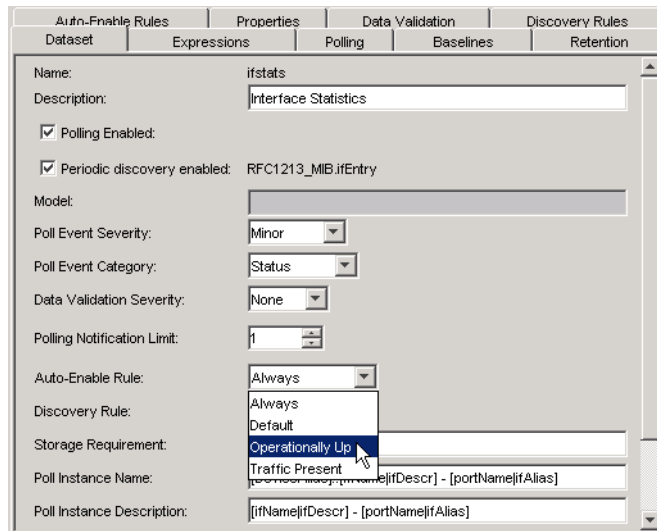
```
(ifAdminStatus+ifOperStatus)=2
```



This rule is identified as `ifstatsOpStatus` and evaluates as true for interfaces that are operational. If you apply this rule to the Interface Statistics dataset, when the NetVoyant product discovers or rediscovers interfaces, it enables polling of the interface only if the interface is operational.

Click **OK** to add the rule name and expression to the Auto-Enable Rules list for the dataset.

- Click the **Datasets** tab to view details for the dataset in the context panel.
- From the **Auto-Enable Polling** list, select the auto-enable rule.



- Click **Set** to save your changes.

**Note:** If you want to delete an auto-enable rule for the dataset, it cannot be currently selected (applied) in the **Dataset** tab.

## Disabling Polling for Non-Operational Interfaces

You can use an interface's operational status (`ifOperStatus`) to dynamically disable polling in the NetVoyant product for non-operational interfaces. This enables you to restrict poll instance usage and data storage for interfaces that are not in use.

You can disable polling for non-operational interfaces using the auto-enable polling feature. Auto-enable polling enables you to dynamically enable polling for poll instances that are discovered in a dataset based on the criteria that you set.

Auto-enable polling rules based on `ifOperStatus` are created by default for the Interface Statistics dataset. You must set an auto-enable polling rule for the dataset to disable polling for non-operational interfaces.

**Note:** When an interface is disabled from polling using an auto-enable rule, NetVoyant does not automatically disable the child interfaces, which can result in “false alarms.” You must manually disable both parent and child interfaces to resolve this.

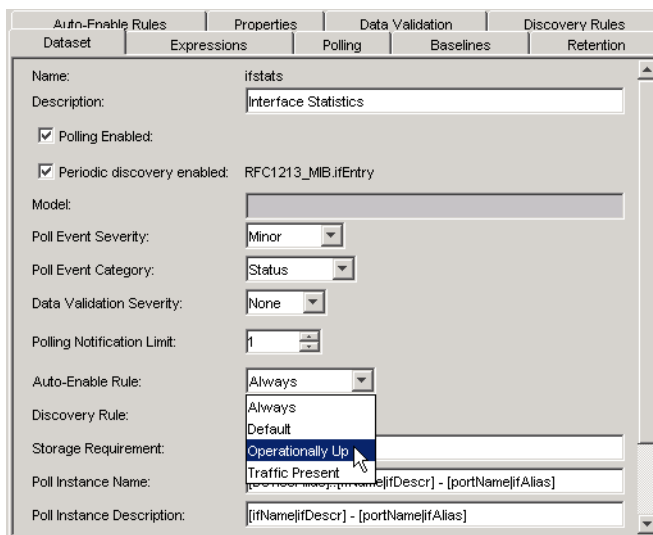
For more information about the auto-enable polling feature, see [“Using Auto-Enable Polling” on page 88](#).

### To disable polling for non-operational interfaces:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling > Datasets** and select the Interface Statistics dataset.

This displays the details for the dataset in the context panel.

3. From the **Auto-Enable Polling** list, select **Operationally Up**.



4. Click **Set** to save your changes.

When the NetVoyant product discovers or rediscovers interfaces, it disables polling of the interface if the interface has an `ifOperStatus` of “down.”

## Disabling Polling for Interfaces without Traffic

You can dynamically disable polling in the NetVoyant product for interfaces that have not seen network traffic at any time. This enables you to restrict poll instance usage and data storage for interfaces that are not in use.

You can disable polling for interfaces without traffic using the auto-enable polling feature. Auto-enable polling enables you to dynamically enable polling for poll instances that are discovered in a dataset based on the criteria that you set.

An auto-enable polling rule based on traffic is created by default for the Interface Statistics dataset. You must set an auto-enable polling rule for the dataset to disable polling for interfaces without traffic.

For more information about the auto-enable polling feature, see [“Using Auto-Enable Polling”](#) on page 88.

### To disable polling for interfaces without traffic:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling > Datasets** and select the Interface Statistics dataset.  
This displays the details for the dataset in the context panel.
3. From the **Auto-Enable Polling** list, select **Traffic Present**.
4. Click **Set** to save your changes.

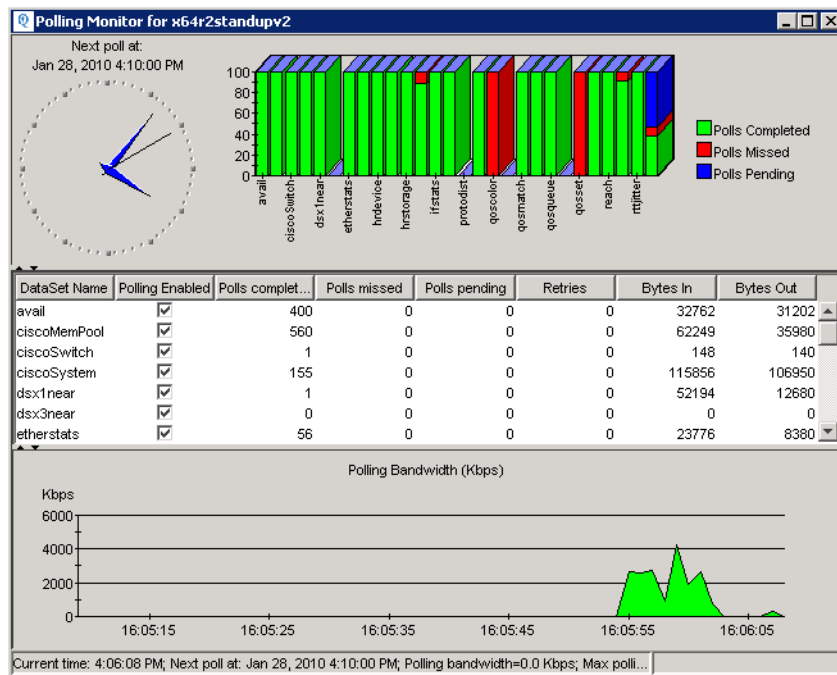
When interfaces are discovered or rediscovered, the NetVoyant product disables polling of the interface if the interface has had no network traffic.

## Monitoring Polling

The Polling Monitor provides the following information about NetVoyant polling activity:

- Date and time of the next scheduled poll
- Polls completed and missed in the most recent poll by dataset
- Polls pending in a poll that is currently occurring by dataset
- Number of retries required for the most recent poll by dataset
- How much bandwidth is being used for polling overall and by dataset

### The Polling Monitor during an active polling cycle



The clock in the upper-left corner of the Polling Monitor shows the next scheduled polling period. This polling period might not apply to all poll instances, depending on how polling groups are assigned to each poll instance. The real-time graph at the bottom shows traffic utilization generated by the polling process with values shown in Kbps. Watching this graph, you can view the traffic peaks caused by the polling process. You can also enable or disable polling for an entire dataset in the Polling Monitor.

#### To open the Polling Monitor:

- From the **Tools** menu in the NetVoyant Console, select **Polling Monitor**.

**Note:** In a distributed system, the Master server has no polling duties. When you view the polling monitor from the Master, it displays information for the last selected poller. If the last selected is the Master, it indicates that there is no polling information and Nothing scheduled.

## CONFIGURING DATA COLLECTION FREQUENCY

The NetVoyant product gathers network, device, and application performance statistics through SNMP-based polling of hosts, routers, probes, and other connection devices. These statistics are collected, rolled up, saved, and presented in reports.

### Configuring the Frequency for Polling and Rollups

The NetVoyant product gathers data by poll instance. For each poll instance, you can assign a polling group to change the frequency of polling and data rollups. Polling groups are created and defined at the dataset level.

To configure polling groups in the NetVoyant Console, you can do the following:

Task	More information
Create a new polling group or edit one of the existing polling groups	<a href="#">“Creating or Editing a Polling Group” on page 94</a>
Set a default polling group for a dataset	<a href="#">“Changing the Default Polling Group for a Dataset” on page 96</a>
Apply a polling group to a poll instance or interface	<a href="#">“Configuring Polling for Poll Instances and Interfaces” on page 166</a>
Apply a polling group to all interfaces of a particular type	<a href="#">“Performing Mass Operations by Interface Type” on page 173</a>
Apply a polling group to all poll instances in a dataset in a network	<a href="#">“Configuring a Polling Group for a Network” on page 124</a>
Apply a polling group to all poll instances in a dataset in a device group	<a href="#">“Configuring Polling for a Group” on page 123</a>

### Creating or Editing a Polling Group

In the NetVoyant product, a polling group defines the polling frequency for a particular type of data, the intervals used to roll up that data for reports, and how long it retains that data. By creating and editing polling groups, you can control how often the NetVoyant poller sends polls on your network, how granular your report data is, and how long the data is available for reports.

Polling groups are created and defined by dataset. When you create a polling group for a dataset, you then set poll instances in that dataset to the new polling group. When you edit a polling group, the NetVoyant product uses the new settings to poll those poll instances in the dataset that are in the polling group. You can also set a default polling group for new poll instances in a dataset.

**Note:** A poll instance can belong to only one polling group, and can be polled at one poll rate.

On a distributed system, dataset polling groups are synched from the Master server to the pollers, but only when the pollers are connected and running at the time a polling group is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

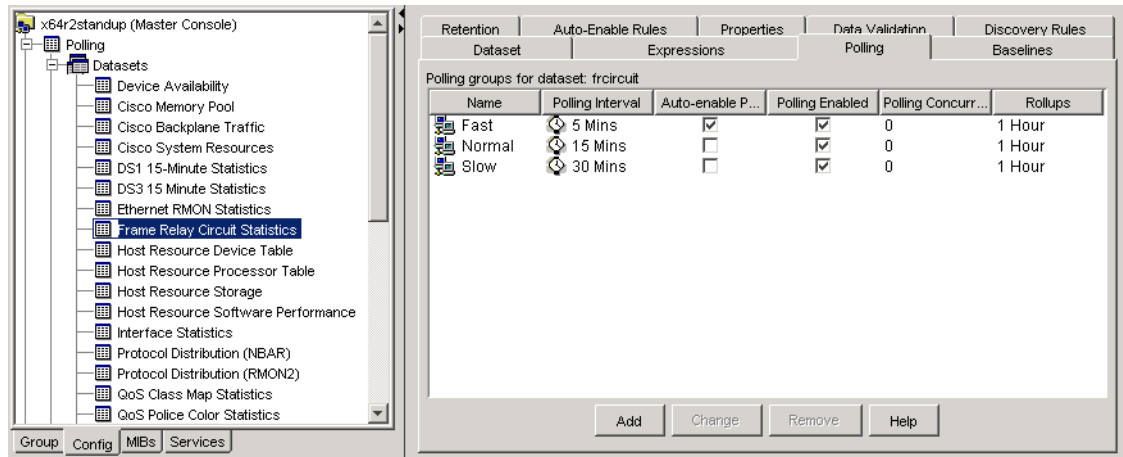
**To create or edit a polling group:**

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling > Datasets** and select the dataset.

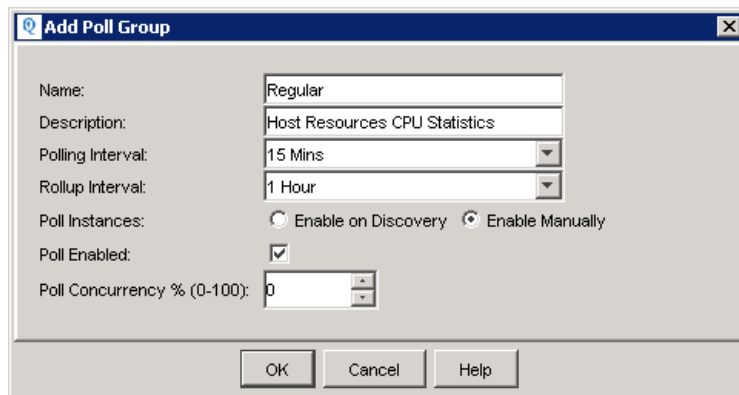
The context panel displays the details for the dataset.

3. In the context panel, select the **Polling** tab.

The tab lists the polling groups for the dataset.



4. Perform one of the following tasks:
  - To edit a polling group, select the polling group and click **Change**.
  - To add a new polling group, click **Add**.



5. In the **Change Poll Group** or **Add Poll Group** dialog box, enter or edit the following parameters:

Parameter	Description
<b>Name</b>	If you are creating a new polling group, enter a name. When you apply a polling group, you select it by name. Use a name that is descriptive of the type of polling group. For example, you could enter a name of "Very Fast" for a polling rate that is faster than the default polling group "Fast."
<b>Description</b>	(Optional) Enter or edit the description. The description can help you identify a polling group's properties.

Parameter	Description
<b>Polling Interval</b>	<p>Select a time interval from the list. This is the frequency for polling devices for this type of data.</p> <p>For example, if you select 1 Min, the NetVoyant product polls devices for data in this polling group each minute.</p> <p>You can add or edit the intervals that are available. For more information, see <a href="#">“Creating or Editing an Interval” on page 97</a>.</p>
<b>Rollup Interval</b>	<p>Select a time interval from the list. The NetVoyant product rolls up the raw data for this polling group for this length of time before discarding it.</p> <p>For more information about rollups and data retention, see <a href="#">“Configuring Data Collection Frequency” on page 94</a>.</p>
<b>Poll Instances</b>	<p>To make this polling group the default polling group for all new poll instances in this data set, select <b>Enable on Discovery</b>; otherwise, leave <b>Enable Manually</b> selected.</p> <p>For more information, see <a href="#">“Changing the Default Polling Group for a Dataset” on page 96</a>.</p>
<b>Poll Enabled</b>	<p>To disable polling for this polling group, clear this check box. You can use this option to quickly disable polling for poll instances in this polling group.</p> <p>For more information, see <a href="#">“Enabling and Disabling Polling for Datasets” on page 86</a>.</p>
<b>Poll Concurrency</b>	<p><i>(Optional)</i> Set this as a percentage between zero and 100.</p> <p>If a device does not support a get-bulk SNMP request, the NetVoyant product must submit multiple requests for polling data as get-next requests. Poll concurrency indicates how many get-next requests (as a percentage of the total requests) it sends to a device at one time.</p> <p>For example, if the NetVoyant poller is polling a router that does not support get-bulk requests and the router has 15 interfaces, it must perform 15 get-next requests. If the poll concurrency is set to zero, it sends each request individually. If the poll concurrency is set to 100, it sends all 15 requests at one time.</p>

6. Click **OK**.

You can apply this polling group to poll instances in this dataset to configure polling frequency and data retention for this dataset. For more information, see [“Configuring the Frequency for Polling and Rollups” on page 94](#) and [“Configuring Data Rollup and Retention” on page 99](#).

## Changing the Default Polling Group for a Dataset

The NetVoyant product automatically sets poll instances for new devices to the default polling group for the related dataset; however, you can designate a different default polling group for a dataset.

For example, if you set the default polling group to “Slow” for the Device Availability dataset, the NetVoyant product sets poll instances in the Availability dataset to Slow for new devices.

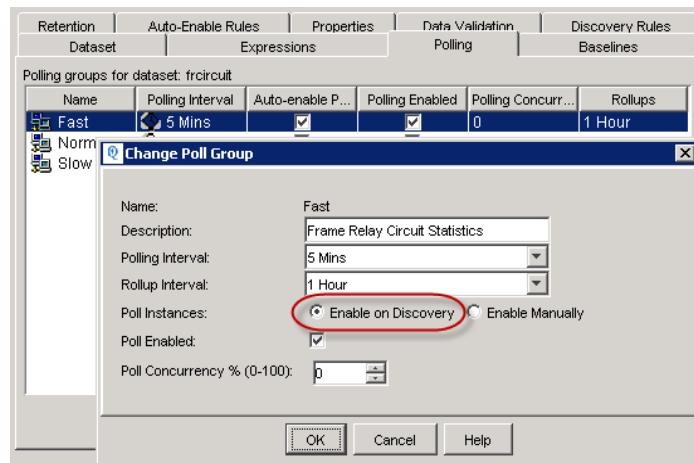
On a distributed system, dataset polling groups are synched from the Master server to the pollers, but only when the pollers are connected and running at the time a polling group is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.



### To change the default polling group for a dataset:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling > Datasets** and select the dataset.  
The dataset's details appear in the context panel.
3. In the context panel, select the **Polling** tab.  
The tab lists the polling groups for the dataset. You can create new polling groups or edit these polling groups for this dataset.
4. Select the polling group that you want to use as the default for poll instances in this dataset and click **Change**.

The **Change Poll Group** dialog box opens.



5. Select **Enable on Discovery** to make this the default polling group for the dataset.
6. Click **OK**.

On the **Polling** tab, the NetVoyant Console selects **Auto-enable Poll Instances** for the polling group, which indicates that it automatically assigns this polling group to new poll instances in the dataset.

## Creating or Editing an Interval

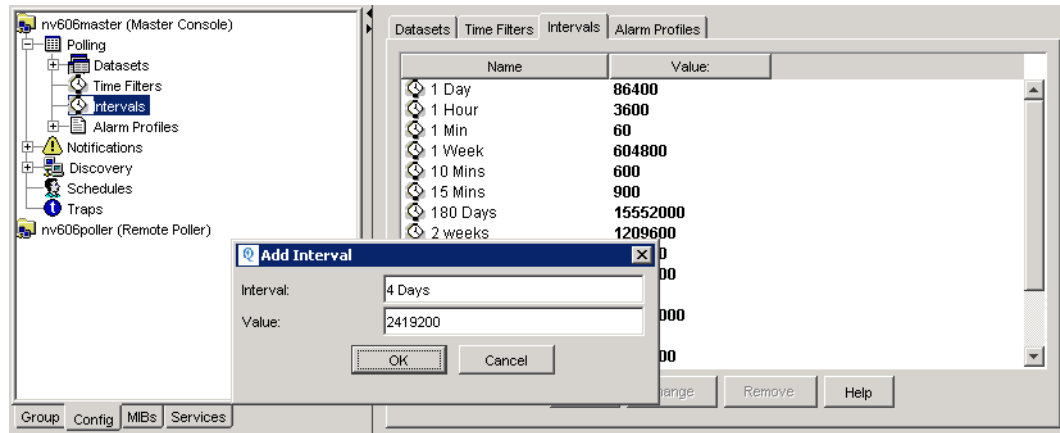
By creating or editing intervals, you can define the time intervals (in seconds) that are available for polling rates and rollups when configuring polling groups. For more information about polling groups, see [“Creating or Editing a Polling Group” on page 94](#).

For example, you could create an interval called “4 weeks” (with a value of 2,419,200 seconds). You could apply this interval to a rollup in a polling group so that the NetVoyant product performs the rollup every four weeks.

On a distributed system, dataset polling intervals are synched from the Master server to the pollers, but only when the pollers are connected and running at the time a polling interval is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

**To create or edit an interval:**

1. On the **Config** tab in the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling** and select **Intervals**.  
The tab lists the currently configured intervals in the context panel.
3. Perform one of the following tasks:
  - To add a new interval, click **Add**. This opens an **Add Interval** dialog box.
  - To edit an existing interval, select the interval and click **Change**. This opens a **Change Interval** dialog box.



4. Enter or edit the following parameters:

Parameter	Description
<b>Interval</b>	For a new interval, enter a name. This is the name that is used to identify the interval in the NetVoyant Console.  It is helpful if the name of the interval is the same as the amount of time that it represents, for example “30 Days.”
<b>Value</b>	Enter or edit the value of the interval in seconds.  For example, a one-minute interval has a value of 60 seconds.  Use a value of less than 60 seconds (sub-minute polling) only within recommended guidelines. For more information about implementing this type of polling interval, see the following section.

5. Click **OK**.

**Using Sub-Minute Polling Intervals**

**Sub-minute polling (intervals of less than 60 seconds) should be used very prudently and cautiously.** Polling this frequently produces a very large number of poll cycles for a dataset, and its corresponding tables in the database can grow quite large. By default, the raw data is retained for one week, requiring extraordinary amounts of disk space to store the data polled at this frequency. Additionally, when the Poll Rate tables in the database grow exceptionally large, performance degradation can result.

**Warning:** If the NetVoyant disk array becomes completely full, the NetVoyant system will fail to operate in its normal capacity and **loss of data** will occur.

Although the NetVoyant Console does not impose limits on sub-minute polling, the following table defines the configurations supported in the NetVoyant product. **Operating outside of these limits is not supported by NetQoS.**

Poll rate	Maximum number of poll instances supported per poller
1-minute	5,000
30-seconds	1,500
15-seconds	750
< 15-seconds	Not Supported

It is recommended that you apply sub-minute polling intervals to **only those poll instances or interfaces that are most critical or require it during troubleshooting**. To mitigate the risk of overloading the disk array, implement the following recommendations:

**Reduce Rate Data Retention.** Edit the Retention settings for datasets utilizing sub-minute polling so that the Poll Rate retention period is less than one week, such as 3 Days or 1 Day. For more information about changing the retention for a dataset, see [“Configuring Data Rollup and Retention” on page 99](#).

**Upgrade Disk Space.** Because disk space is required for storing many types of NetVoyant data, upgrading to a larger hard drive can protect against premature overloading of smaller disk drives. Contact your NetQoS Account Manager or Support to inquire about purchasing larger hard drives. Hard drive upgrades are not included in the ClientConnection maintenance program.

## Configuring Data Rollup and Retention

The NetVoyant product aggregates polling data into short-term and long-term rollups. Rollups are collections of reduced data optimized for database storage and NetVoyant reports.

For each polling group, the polling interval determines the granularity of the reportable raw data (rate records used for detailed trend reports). The rollup interval determines the intervals at which the raw data is aggregated for reporting. For the dataset, the rollup retention settings determines how long the rollup data is retained in the NetVoyant database.

You can configure how the NetVoyant product performs these data rollups according to polling groups, which are created and defined at the dataset level. For each polling group, you can configure the following:

- How often short-term rollups are performed (the rollup interval)
- How long each type of rollup is retained (rollup retention)

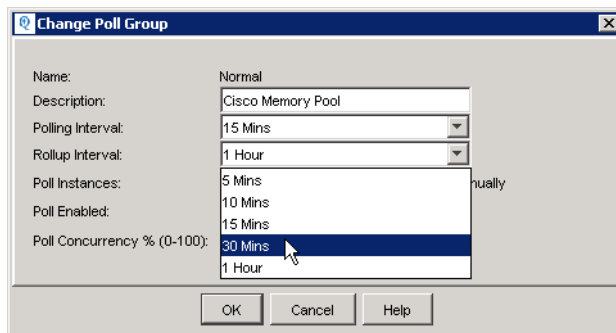
On a distributed system, polling groups are synched from the Master server to the pollers, but only when the pollers are connected and running at the time a polling group is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

For more information about creating and editing polling groups, see [“Creating or Editing a Polling Group” on page 94](#).

### To configure the frequency of short-term rollups for a dataset:

1. On the **Config** tab in the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling > Datasets** and select the dataset.
3. Select the **Polling** tab.
4. Select the poll group that you want to change.  
To select the default poll group, select the poll group that has the Auto-enable Polling option selected.
5. Click **Change** to open the **Change Poll Group** dialog box.
6. Change the **Rollup Interval** setting.

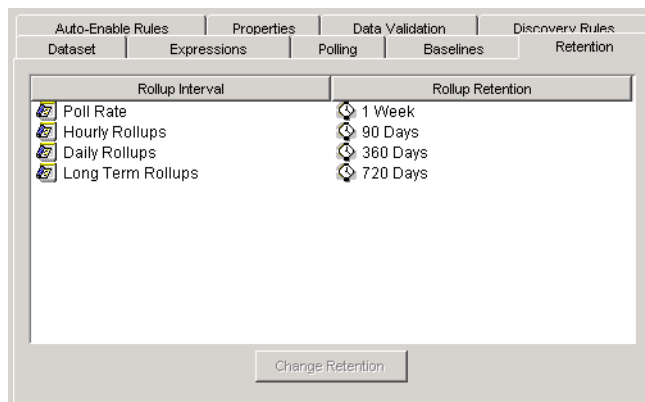
The NetVoyant product rolls up the raw data for this polling group for this length of time before discarding it. You can create or edit intervals to use as rollup intervals.



7. Click **OK**.

### To configure how long rollups are retained:

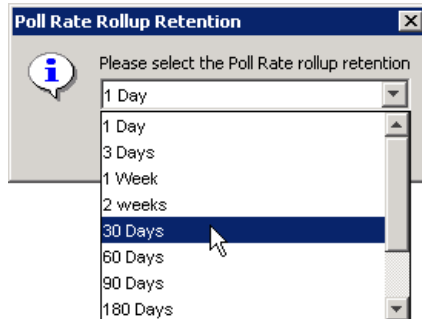
1. On the **Config** tab in the NetVoyant Console, expand the Master Console.
2. Expand **Polling > Datasets**.
3. Select the dataset and click the **Retention** tab.



This tabbed panel lists four rollup intervals:

- Poll Rate
- Hourly Rollups
- Daily Rollups

- Long Term Rollups
4. Select a rollup interval and click **Change Retention** or double-click the rollup interval. The **Retention** dialog box opens.
  5. Select a new retention interval from the drop-down list.



This length of time determines how long rollup data is retained after the data is collected.

6. Click **OK**.

## Configuring Time Filter Definitions

The NetVoyant polling configuration options allow for the definition of flexible time-period filters to be used for rollup intervals. These time filters affect the daily and long-term rollups, not the raw poll rate data or short-term (hourly) rollups.

For example, you can use hours of the day and days of the week to eliminate non-working hours or you can generate shift-based rollups if that is needed. These two settings specify the hours of the day (for daily rollups or longer) and days of the week (for weekly rollups and longer) included in the rollup.

When defining time filters, you can also apply a time-zone to the rollups. For example, you can specify that the valid time frame for rollups is Monday through Friday, 8:00am to 6:00pm, CST. If you add another time-zone, such as PST, the NetVoyant product creates two separate rollups—one for Central Standard and one for Pacific Standard.

**Note:** While you can configure different working hours, days of the week, and timezones, adding additional time filters/time zones greatly increases the amount of storage required to maintain rollup data. It is recommended that you do not use additional filters/time zones without a significant need or purpose.

On a distributed system, time filter definitions are synched from the Master server to the pollers, but only when the pollers are connected and running when a time filter is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

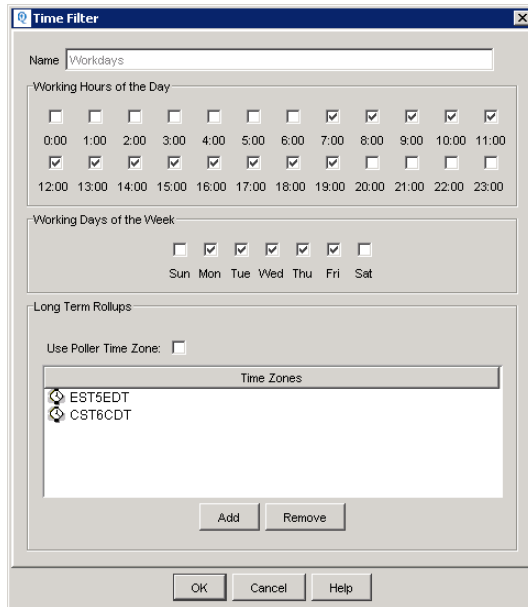
### To configure time filter definitions:

1. On the **Config** tab in the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling** and select **Time Filters**.

The context panel displays to time filter definition by default: All Hours and Workdays. You can modify these default time filters or add new time filters to the list.

3. To modify a time filter, such as Workdays, select it and click **Change**.

The **Time Filter** dialog box opens.



4. (Optional) Select the **Working Hours of the Day** and the **Working Days of the Week** for which you want to aggregate data.

If you clear the check box for an hour or day, data from this time period is not included in long-term rollups.

5. (Optional) Add or delete time zone definitions for long-term rollups.

- Click **Add** to add a new time zone definition.

In the **Time Zones** dialog box, select the item corresponding to the desired time zone.



- Select a time zone definition and click **Remove** to delete it from the time filter.
6. (Optional) To use the time zone as set on the system of the poller machine, select the **Use Poller Time Zone** check box.

**Warning:** If you use the time zone set on the poller and an administrator changes the time zone on that system, this will affect the historical data and report views displaying the long term rollups. When a time zone change occurs, the NetVoyant database will store subsequent long term rollup data separately, resulting in two line items until a full 90-day rollup window has passed since the time zone change.

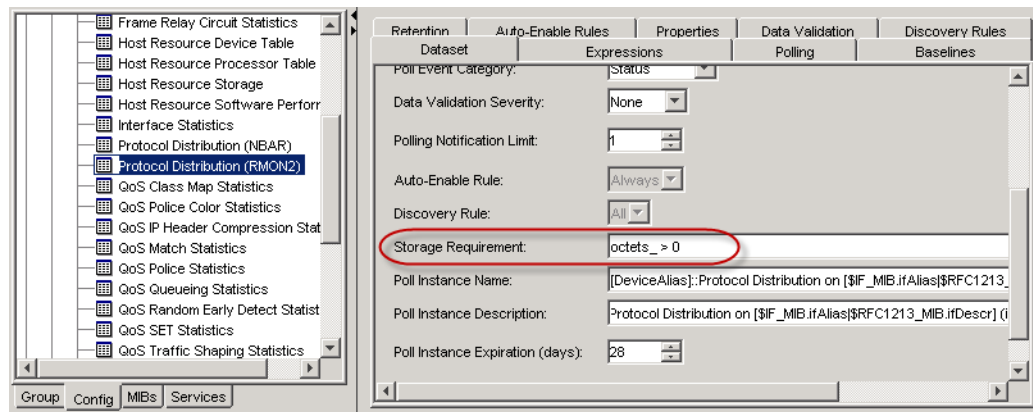
7. Click **OK**.

The NetVoyant product begins to rollup data according to your settings.

## Restricting Database Storage

The storage requirement expression in the **Dataset** details tab enables you to dynamically restrict database storage for poll instances in a dataset based on the criteria that you set in an expression. The NetVoyant product does not store data for poll instances that do not meet the criteria in the storage requirement expression.

If it exists, it evaluates the storage requirement expression during every polling cycle. It stores data for poll instances in the dataset for which the storage requirement expression evaluates to a positive number. It does not store data for poll instances in the dataset for which the storage requirement expression evaluates to zero or a negative number.



When creating your expression for storage requirement, you can use any OIDs in the MIB table for the dataset and any default or customized properties. For more information about creating expressions, see [“Creating or Editing a Dataset Expression” on page 105](#). For more information about using properties in NetVoyant expressions, see [“Using Properties in Dataset Expressions” on page 308](#).

On a distributed system, dataset parameters are synched from the Master server to the pollers, but only when the pollers are connected and running at the time a dataset is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

## CONFIGURING WHAT DATA TO GATHER

The NetVoyant product uses expressions in a dataset to create reportable data using the raw data on your devices. You can use the default expressions or create your own. If you create a custom dataset, you must create the expressions used to generate NetVoyant reports for the new dataset.

To configure what data is collected for a selected dataset, you can perform the following tasks:

Task	More information
Create or edit expressions	<a href="#">“Creating or Editing a Dataset Expression” on page 105</a>
Add and set values for dataset properties	<a href="#">“Using Dataset Properties” on page 111</a>
Add data validation rules	<a href="#">“Using Data Validation Rules” on page 112</a>
Add, edit, or remove the baselines for an expression	<a href="#">“Adding and Editing Baselines in the NetVoyant Console” on page 108</a>

### Using Expressions to Gather Data

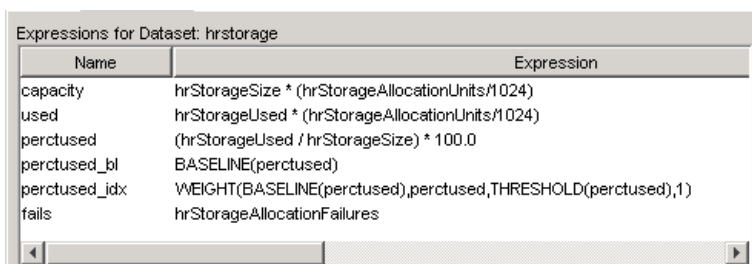
NetVoyant reports are based on expressions. Expressions are formulas applied to one or more OIDs from a dataset’s MIB table. Expressions can be based on OIDs, other expressions, properties, and any combination.

The computed values are the basis of NetVoyant thresholds and reports.

In some cases, expressions are based on a single OID, such as the expression “fails” in the figure where its value is simply the value of an OID. Other expressions are more complicated and involve some sort of calculation. For example, the “fails” expression could be turned into a “failures per second” expression by creating the following expression:

```
hrStorageAllocationFailures/duration
```

#### *Pre-configured expressions in the Host Resource Storage dataset*



Name	Expression
capacity	hrStorageSize * (hrStorageAllocationUnits/1024)
used	hrStorageUsed * (hrStorageAllocationUnits/1024)
perctused	(hrStorageUsed / hrStorageSize) * 100.0
perctused_bl	BASELINE(perctused)
perctused_idx	WEIGHT(BASELINE(perctused),perctused,THRESHOLD(perctused),1)
fails	hrStorageAllocationFailures

Expressions provide incredible flexibility for other situations in which a single OID is not meaningful by itself. For example, the `hrStorageSize` OID is meaningless unless you know the value for the OID `hrStorageAllocationUnits`. The expression “capacity” in the figure takes both of these OIDs into account to create an expression that is meaningful when used for reporting or calculating an alarm threshold.



In complex datasets, expressions can be chained to simplify them further. For example, the expression “perctused” could be changed to the following:

```
(used / capacity) * 100
```

You can set thresholds for expressions in the NetVoyant alarm profiles. If the value for an expression crosses a threshold, it generates a threshold event. For more information on thresholds, see [“Using Thresholds to Trigger Events” on page 204](#).

## Creating or Editing a Dataset Expression

Dataset expressions are equations that define how the NetVoyant product gathers data from the OIDs in the MIB table upon which a dataset is based. You can use the default expressions in the NetVoyant Console or create your own.

Expressions consist of the OIDs in the dataset’s MIB table, operators, and properties. For more information about NetVoyant properties and operators, see [Appendix A, “NetVoyant Properties and Operators” on page 307](#).

On a distributed system, dataset expressions are synched from the Master server to the pollers, but only when the pollers are connected and running at the time an expression is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

### To create or edit an expression for a dataset:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling > Datasets** and select the dataset.  
The context panel lists the details for the dataset.
3. Click the **Expressions** tab.
4. Perform one of the following tasks:
  - Click **Add** to open the **Add Expression** dialog box.
  - Select the expression and click **Change** to open the **Change Expression** dialog box.

**Change Expression**

Name: reboots  
Description: Device Resets

Operators:

+	-	*	/	(	)
>	<	>=	<=	AND	OR
IF	THEN	ELSE	MIN(	MAX(	BASLINE(
THRESHOLD(	VALUE(	WEIGHT(			

Advanced >>

Expression Definition:

```
if ((availability > 0) and (availability < 100)) then 1 else 0
```

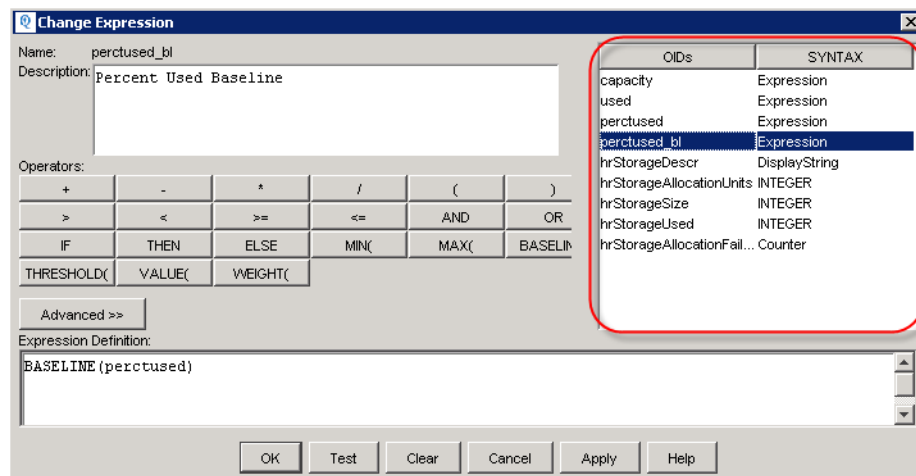
OIDs	SYNTAX
availability	Expression
availability_bl	Expression
reboots	Expression
sysDescr	DisplayString
sysUpTime	TimeTicks
sysContact	DisplayString
sysName	DisplayString
sysLocation	DisplayString
sysServices	INTEGER

OK Test Clear Cancel Apply Help

## 5. Enter or edit the following parameters:

Parameter	Description
<b>Name</b>	For a new expression, enter a name for the expression. The name is used to identify the expression in the NetVoyant Console.
<b>Description</b>	Enter or edit the description for the expression. The description can help you identify what type of data an expression gathers.
<b>Expression Definition</b>	<p>Enter the expression in this field.</p> <ul style="list-style-type: none"> <li>To enter an OID, double-click the OID in the list on the right or enter the OID name in the field. This list includes all the OIDs in the MIB table upon which the dataset is based. For more information, see <a href="#">“Working with Management Information Bases”</a> on page 177.</li> <li>To enter an operator, click one of the operator buttons. For more information about these operators in expressions, see <a href="#">“Using NetVoyant Operators in Expressions”</a> on page 319.</li> <li>To add a property, enter the name of the property preceded by a \$ symbol. For example: \$PropertyName. For more information, see <a href="#">“Using Dataset Expressions in Thresholds”</a> on page 206.</li> </ul> <p><b>Note:</b> The NetVoyant product does not set values for properties you add to expressions. If you create a property in an expression, we recommend that you use a VALUE function, which evaluates to another default value if the property itself has not been set for a poll instance. For example, you could create a property called PropertyName in an expression using the following VALUE function:</p> <pre>VALUE(\$PropertyName, 50)</pre> <p>In this example, the VALUE function evaluates to the \$PropertyName value if the property value has been set for an object, otherwise it evaluates to 50.</p>

**Note:** Expressions can use the OIDs listed in the **OID** table at the right of the Expression editor.

6. (Optional) To configure what types of calculations are performed on the expression for use in NetVoyant report views, click **Advanced**.

- Select the types of calculations you want to perform.
- Click **OK**.

For more information on these calculations, see [“Changing Advanced Calculations for an Expression” on page 107](#).

7. Click **Apply** after creating an expression to add that expression to the dataset and enter another expression.
8. Click **OK** to exit the dialog box.

**Important:** This must result in a valid SnmpQL query. If the query is not valid, there will be **no** data associated with that expression. If you have the logging level set to 4 or higher, you can use the **Test** button at the bottom of the **Add Expression** or **Change Expression** dialog box to test the validity before you save the expression for the dataset.

## Changing Advanced Calculations for an Expression

Advanced calculations are calculations that the NetVoyant product performs on data gathered for an expression. It performs these calculations during rollups for the data. These calculations are then available for use in NetVoyant reports.

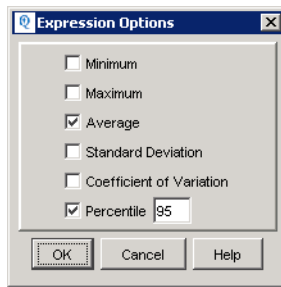
To configure what types of calculations are performed on an expression, you can configure the advanced calculations while editing the expression. For more information on how to edit an expression, see [“Creating or Editing a Dataset Expression” on page 105](#).

The following are the advanced calculations available in the NetVoyant product:

Calculation	Description
Minimum	The minimum value for expression data during the rollup period.
Maximum	The maximum value for expression data during the rollup period.
Average	The average value for expression data during the rollup period.
Standard Deviation	The standard deviation of expression data during the rollup period.
Coefficient of Variation	The coefficient of variation for expression data during the rollup period.
Percentile	<p>The Nth percentile for expression data during the rollup period where N is a whole number less than 100 that you enter.</p> <p>For example, you could enter 95 for this calculation. The NetVoyant product would then calculate the 95th percentile, for which 95% of data for the rollup fell below this value.</p>

### To select advanced calculations to perform for an expression:

1. While editing the expression in the **Add Expression** or **Change Expression** dialog box, click **Advanced>>**.  
The **Expression Options** dialog box opens.



- Select the types of calculations you want to perform.
- Clear those calculations that you do not want to perform.

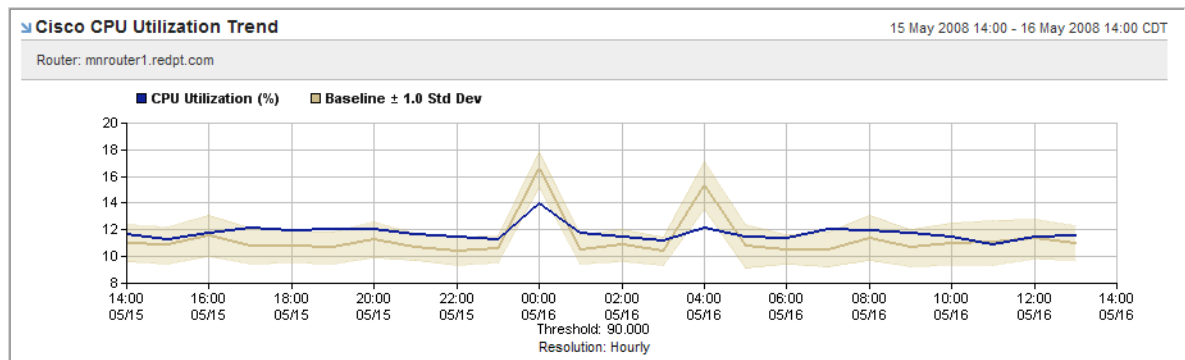
**Warning:** Although removing an advanced calculation for an expression does save database space, it also eliminates your ability to create many types of reports. It is strongly recommended that you **not** remove advanced calculations that are configured by default.

2. To add a percentile calculation, select **Percentile** and enter a whole number less than 100.
3. When you are finished selecting the calculations that you want NetVoyant to perform, click **OK**.

## Using Baselines

Baselines are an average measurement of an expression over a period of time. By comparing to the baseline, you can determine whether values are normal for a given period of time. The NetVoyant product calculates hourly and monthly baselines for many expressions with a default 30-day moving baseline for each hour of the day.

Users can view baseline data on Trend views in NetVoyant and NetQoS Performance Center report pages. For more information, see the *NetVoyant User Guide*.



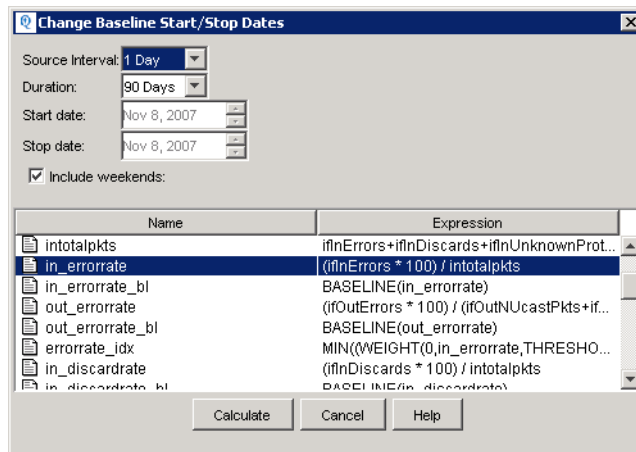
## Adding and Editing Baselines in the NetVoyant Console

The NetVoyant Console provides the ability to add baselines for the expressions in a dataset, and to edit the intervals and duration for which baselines are calculated.

On a distributed system, dataset parameters are synched from the Master server to the pollers, but only when the pollers are connected and running at the time a dataset is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

**To add or edit a baseline:**

1. In the **Config** tab of the NetVoyant Console (standalone or Master), expand the Master server.
2. Expand **Polling > Datasets** and select the dataset.  
The dataset's details appear in the context panel.
3. Click the **Baselines** tab.  
The currently configured baselines appear in the context panel.
4. Perform one of the following actions:
  - To create a new baseline, click **Add**. This opens the **Calculate Baseline** dialog box.
  - To edit an existing baseline, select the baseline and click **Change**. This opens the **Change Baseline Start/Stop Dates** dialog box.



5. Edit the following parameters:

Parameter	Description
<b>Source Interval</b>	Select the interval over which you want the NetVoyant product to calculate the baseline.  For example, if you want an hourly average, select 1 Hour.
<b>Duration</b>	Select the length of time that you want the NetVoyant product to store each baseline calculation. This is also the length of time over which it uses each baseline calculation as a means for comparison in a baseline report.  For example, if you select 30 Days for the Duration on a baseline calculated hourly, it stores each hourly calculation for the expression for 30 days.  If you then compare a value for the expression for 8:00 AM to the baseline, it compares the expression to the average baseline calculated at 8:00 AM for the past 30 days.
<b>Start date</b>	If you want to specify a fixed duration, select the date on which you want the NetVoyant product to start calculating this baseline for the expression.  <b>Note:</b> This option is available only when the <b>Duration</b> is set to None.

Parameter	Description
<b>Stop date</b>	If you want to specify a fixed duration, select the date on which you want the NetVoyant product to stop calculating this baseline for the expression. <b>Note:</b> This option is available only when the <b>Duration</b> is set to None.
<b>Include Weekends</b>	Select this check box if you want the NetVoyant product to include values for the expression on Saturdays and Sundays in baseline calculations.

- From the list of expressions at the bottom of the dialog box, select the expression for which you want to calculate a baseline.

This list is populated with the expressions for the dataset.

- Click **Calculate**.

This adds the baseline calculation to the list of baselines and the NetVoyant product begins calculating and storing baselines for the expression as indicated.

## Removing Baselines from a Dataset

When the NetVoyant product calculates and stores baseline data for a dataset, it requires additional space in the NetVoyant database. If you have added custom baselines and no longer require the information for reporting purposes, you can remove these baselines from the dataset.

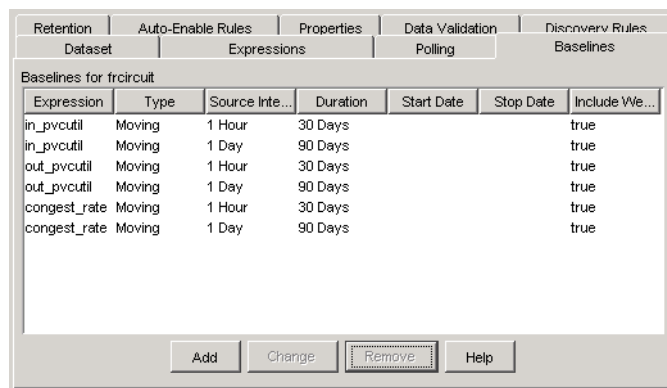
**Warning:** If you remove a baseline, you lose all baseline data for the expression. It is strongly recommended that you do not remove any of the default baselines for a dataset.

On a distributed system, dataset parameters are synched from the Master server to the pollers, but only when the pollers are connected and running at the time a polling group is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

### To remove a baseline:

- In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
- Expand **Polling > Datasets** and select the dataset.  
The dataset's details appear in the context panel.
- Click the **Baselines** tab.

The currently configured baselines appear in the context panel.



4. To remove a baseline, select the baseline and click **Remove**.
5. Click **Yes** to verify.

## Using Dataset Properties

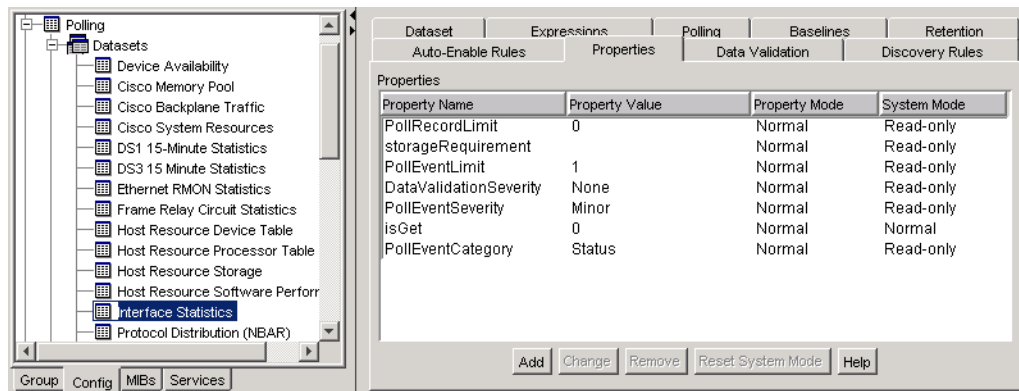
Properties are variables used to customize the definition of objects, such as datasets, devices, or poll instances. You can use properties in expressions, thresholds, notifications, and reports.

On a distributed system, dataset properties are synched from the Master server to the pollers, but only when the pollers are connected and running at the time a dataset property is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

**Warning:** Altering dataset properties can significantly affect polling and data collection. We recommend that you modify these properties only under the supervision of NetQoS Technical Support or Professional Services staff.

### To modify the properties for a dataset:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling > Datasets** and select the dataset.  
The dataset's details appear in the context panel.
3. Click the **Properties** tab.



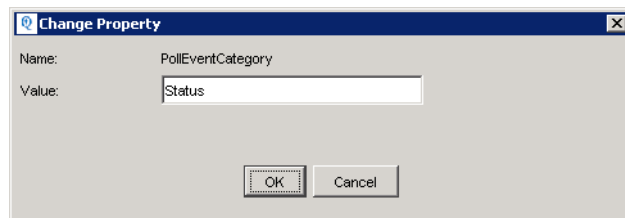
The currently configured dataset properties appear in the context panel with the following parameters for each property:

Parameter	Description
<b>Property Name</b>	The name of the property used to identify it.
<b>Property Value</b>	The value of the property for this dataset; for example, for a Protocol Distribution dataset, the PollEventLimit property could have a value of 1.

Parameter	Description
<b>Property Mode</b>	<p>The property mode of a property indicates whether you can edit the value for a property. The property mode can be set to one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Normal</b> - You can edit the value of a dataset property with a normal property mode.</li> <li>• <b>Read-only</b> - You cannot edit the value of a dataset property with a read-only property mode.</li> </ul>
<b>System Mode</b>	<p>The system mode of a property indicates whether the value for a property can be modified by the system at discovery. The system mode can be set to one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Normal</b> - All default NetVoyant properties are initially set to Normal, indicating that it can edit the property value during rediscovery.</li> <li>• <b>Read-Only</b> - All properties that you create are initially set to Read-Only, indicating that it cannot edit the property value during rediscovery. If you manually edit the value for a property, the NetVoyant product changes the system mode to read-only so that it does not overwrite your entry.</li> </ul>

4. Perform one of the following actions:

- To create a new property for the dataset, click **Add**. This opens the **Add Property** dialog box.
- To edit an existing property, select the property and click **Change**. This opens the **Change Property** dialog box.



5. If it is a new property, enter a name for the property in the **Name** field.
6. In the **Value** field, enter a value for the property.
7. Click **OK** to close the dialog box

## Using Data Validation Rules

Many of the default datasets have data validation rules that check the integrity of the data. When the NetVoyant product polls a device, each row retrieved for the dataset must pass these rules (evaluate to true/non-zero) in order for the data to be processed. Use these rules to check the validity of the data, such as having enough packets for the octets received, or making sure that the RTT is less than the timeout.

On a distributed system, data validation rules are synched from the Master console to the pollers, but only when the pollers are connected and running at the time a data validation rule is added or modified. If a poller is not operational when the configuration change is made on the Master, the change will be synchronized when communication with the poller is restored.

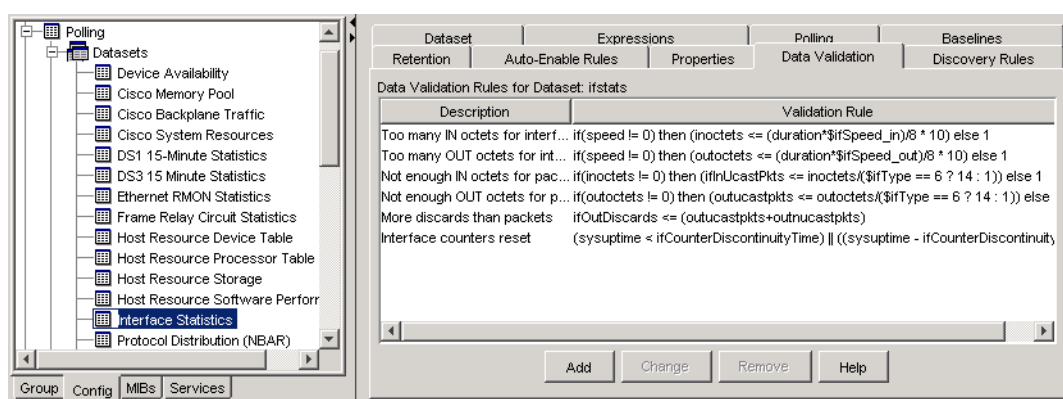


Adding, changing, or deleting data validation rules requires that the poll service be restarted. For more information about stopping and restarting NetVoyant services, see “Starting and Stopping Individual Services on the Services Tab” on page 281.

**Warning:** Altering data validation rules can significantly affect polling and data collection. It is recommended that you modify data validation rules only under the supervision of NetQoS Technical Support or Professional Services staff.

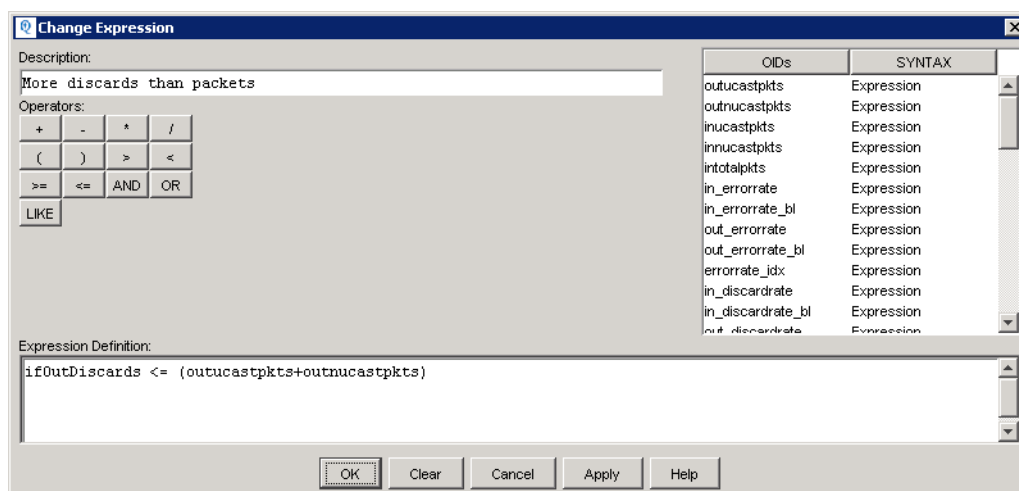
### To modify the data validation rules for a dataset:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Polling > Datasets** and select the dataset.  
The dataset’s details appear in the context panel.
3. Click the **Data Validation** tab.



The currently configured data validation rules appear in the context panel.

4. Perform one of the following actions:
  - To create a new data validation rule, click **Add**. This opens the **Add Expression** dialog box.
  - To edit an existing data validation rule, select the rule and click **Change**. This opens the **Change Expression** dialog box.



5. In the **Description** field, enter a description for the rule that makes it easy to identify the validity test.

6. In the **Expression Definition** field, enter the expression.

You must write the expression so that it evaluates to true or a non-zero value when the data is valid. You can use any of the OIDs available for the dataset. For more information about using the Expression editor, see [“Creating or Editing a Dataset Expression” on page 105](#).

7. Click **OK** to close the Expression editor and save your changes.

**Important:** This must result in a valid SnmpQL query. If the query is not valid, there will be **no** data validation rule applied. If you have the logging level set to 4 or higher, you can use the **Test** button at the bottom of the **Add Expression** or **Change Expression** dialog box to test the validity before you save the expression for the validation rule.

# Managing Your Devices and Networks

---

After you complete the initial configuration of the NetVoyant product and discover your network, you can begin to manage and organize the devices and networks. Device and network management tasks take place in the NetVoyant Console on the **Groups** tab.

If your installation of the NetVoyant product is bound to the NetQoS Performance Center as a data source, the devices and networks discovered by the NetVoyant product are also displayed in the NetQoS Performance Center web interface. Managed objects and groups that are reported to the NetVoyant product by the NetQoS Performance Center are visible in the NetVoyant Console, but can be modified only in the NetQoS Performance Center or the underlying NetQoS product data source. For more information, see the *NetQoS Performance Center Administrator and User Guide*.

This chapter covers the following topics:

- “Manually Adding Networks and Devices” on page 116
- “Working with NetVoyant Groups” on page 118
- “Managing Devices In NetVoyant” on page 130
- “Configuring Protocol Data” on page 157
- “Working with Poll Instances and Interfaces” on page 161

## MANUALLY ADDING NETWORKS AND DEVICES

During initial discovery, the NetVoyant product detects devices on your network automatically; however, you can also add devices and networks to the NetVoyant Console manually. While it will typically pick up new devices or networks during the nightly rediscovery, you might want to add one manually so that you can modify its configuration options.

### Adding a Network

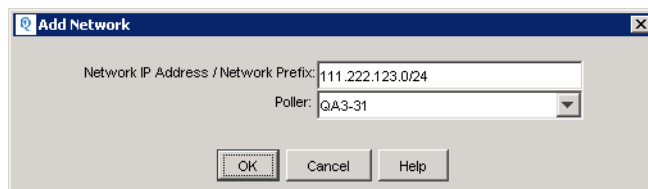
Adding a network is a very straightforward task. The NetVoyant product can detect and add a network using its IP address.

On a distributed system, networks are synched from the Master server to the pollers, but only when the pollers are connected and running at the time that polling settings are modified. If a poller is not operational when the network is added on the Master, the change will be synchronized when communication with the poller is restored.

#### To add a network to the discovery scope and discover it:

1. From the **File** menu in the NetVoyant Console, select **New > Network**.
2. Enter the network as the IP address/network prefix; for example:

111.222.123.0/24



3. If you are using a distributed system, designate a poller for the network.
4. Click **OK**.

### Adding a Device

Use the Device Wizard to add an individual device to the discovery scope and immediately discover the device. This tool guides you through the process of adding a new device and setting discovery options.

**Note:** On a distributed NetVoyant system, it is recommended that you add devices on the Master and specify the appropriate poller. If a poller is not operational when the change is made on the Master, the change will be synchronized when communication with the poller is restored.

#### To add an individual device to the discovery scope and discover it:

1. From the **File** menu in the NetVoyant Console, select **New > Device**.

The Device Wizard opens.

- Click **Next** to step through the wizard.
- Click **Back** to step backwards to a previous step.

2. Enter the device name or IP address.
3. If it is a distributed NetVoyant system, assign a poller for the new device.

Device name/IP address:  
192.168.123.2

Poller for this device:  
vm-test-NVpoller1-long

SNMP Discovery:

☐ Discover only this device.

☒ Discover this device and use the information from this device to discover other devices (Extended discovery).

**Note:** When you add the device, the NetVoyant product will check for any existing scopes for the device. If it finds one, the poller specified here will be discarded.

4. In the **SNMP Discovery** options, choose to do one of the following:
  - Choose the first option to set the device for normal discovery.
  - Choose the second option to set the device for Extended Discovery.

If you configure a device for extended discovery, the NetVoyant product discovers this device and other devices in the ARP cache for this device.

5. Click **Next**.
6. Review and confirm the device configuration.
7. Click **Finish**.

The NetVoyant product discovers the device and adds it to the tree in the **Group** tab according to device class.

**Note:** If you cannot locate a device after the NetVoyant product has discovered it, check the Other device class. If it does not recognize a device model or if the device does not respond to SNMP requests, the NetVoyant Console places the device in the Other device class. For more information about device models and classes, see [“Configuring Device Classes and Models” on page 59](#). For more information about NetVoyant groups, see [“Working with NetVoyant Groups” on page 118](#).

## WORKING WITH NETVOYANT GROUPS

NetVoyant groups enable you to logically organize your devices and networks. Groups function similar to a tree file structure, with each group containing subgroups, networks, or devices.

Properly organizing your devices and networks according to groups enables you to better manage and organize your NetVoyant reports, assign user permissions appropriately, and create events and alarms according to meaningful groups.

On a distributed system, groups are synched from the Master server to the pollers, but only when the pollers are connected and running at the time of the modification. If a poller is not operational when the group change is made on the Master, the change will be synchronized when communication with the poller is restored.

### Default NetVoyant Groups

The NetVoyant product includes two default high-level groups, which provide a functional grouping of devices:

- **Devices group:** Provides sub-groupings of devices according to device class. For example, it places servers in the Servers subgroup, and places routers in the Routers subgroup. For more information about how the NetVoyant product classifies devices, see [“Configuring Device Classes and Models” on page 59](#).
- **Networks group:** Provides groups of devices according to network connectivity. Each network that is discovered has a subgroup under Networks. The NetVoyant product includes devices that are connected to a network in the network’s subgroup. It includes devices with interfaces on more than one network in multiple network subgroups.

During discovery, the NetVoyant product places devices that it discovers in these default groups, according to the device’s characteristics. For more information about the discovery process, see [“Configuring Discovery” on page 49](#).

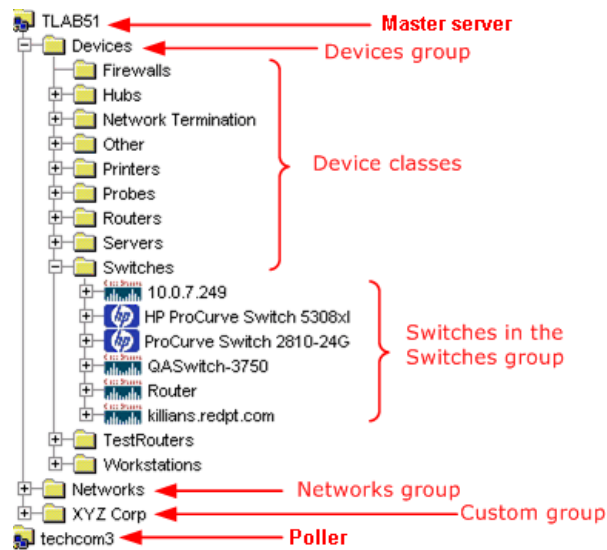
### Groups in the NetVoyant Console

The **Groups** tab in the NetVoyant Console displays your groups using a familiar file folder structure, similar to a disk’s directory structure.

In a standalone configuration, the NetVoyant Master server is at the top level of the Group tree. In a distributed configuration, the NetVoyant Master server and pollers are at the top level of the Group tree. Underneath each of these servers, there is a group tree structure.

**Note:** The devices underneath a poller are polled by that poller. **You cannot copy and paste devices between pollers.**


### Group tree structure in the NetVoyant Console

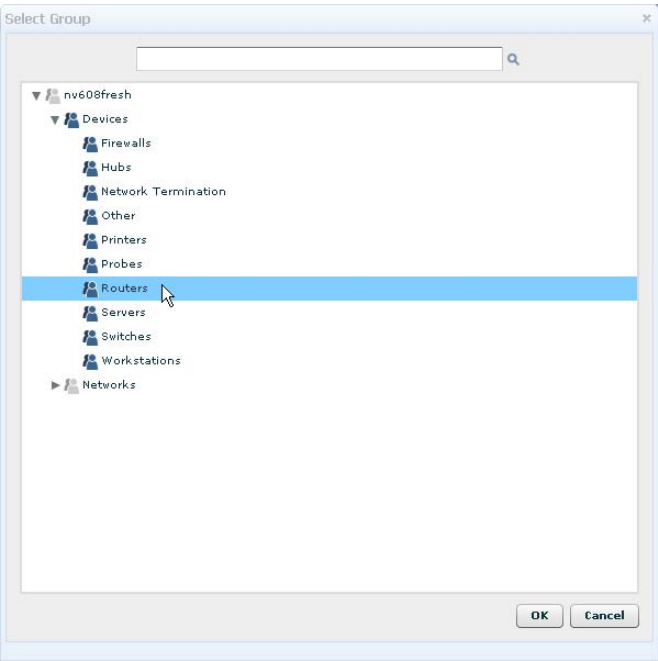


You can configure devices and their related poll instances or interfaces according to group. For more information, see [“Adding a New Custom Group” on page 121](#).

On a distributed system, groups and group membership are synced from the Master server to the pollers, but only when the pollers are connected and running at the time of the modification. If a poller is not operational when the group change is made on the Master, the change will be synchronized when communication with the poller is restored.

## Groups in the Reporting Interface

The **Group** menu in the NetVoyant reporting tool displays groups in a list menu. You can click the group selector (  **Group:** ) at the top of a report page to select a group from an expandible tree.



When you select a group on a report page, the views on that page reflect only the devices and poll instances in that group.

You can also use the search page to display a list of groups.

### Group list in the NetVoyant reporting interface

Selected Groups		
Group List		
Path	Members	Description
Devices	0	
Devices/Firewalls	0	
Devices/Hubs	0	
Devices/Network Termination	1	
Devices/Other	5	
Devices/Printers	1	
Devices/Probes	2	
Devices/Routers	8	
Devices/Servers	7	
Devices/Switches	4	
1 2 3 4		Max Per Page: 10

### Managing Groups in the NetQoS Performance Center

If your installation of the NetVoyant product is bound to the NetQoS Performance Center as a data source, the groups created in the NetVoyant Console are available and can be edited in the NetQoS Performance Center web interface. Groups created in the NetQoS Performance Center are visible in



the NetVoyant Console, but can be edited or deleted only in the NetQoS Performance Center. For more information about managing reporting groups for data sources in the NetQoS Performance Center, see the *NetQoS Performance Center Administrator and User Guide*.

## Group Membership

Devices, networks, poll instances, and interfaces can be members of more than one group.

If a device belongs to a group, you can exclude or include its poll instances and interfaces from the group. If you exclude a poll instance from a device in a group, the device is shown as a member of that group even if not all poll instances from that device are members of the group.

For example, if a device has two interfaces, interface 1 and 2, the interfaces do not have to be in the same group. Interface 1 can be in group A, but not in group B. Interface 2 can be in group B, but not in group A. The device is a member of both groups, but its interfaces are members of only the groups in which they are included.

For more information on how to include or exclude poll instances or interfaces from a group, see [“Adding Devices, Poll Instances, or Interfaces to Groups” on page 125](#) and [“Including and Excluding Poll Instance or Interface Data” on page 129](#).

In the NetVoyant Console, you can also define rules for automatically grouping devices during discovery. For more information about defining rules for automated grouping, see [“Automatic Grouping” on page 125](#).

## Adding a New Custom Group

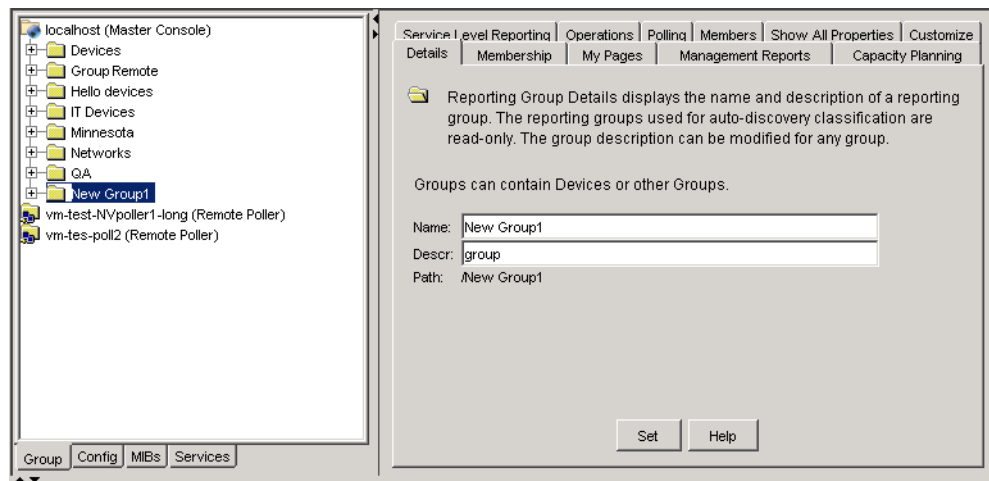
Create custom groups to organize your networks and devices. This enables administrators to control access to the data within your organization and enables users to view report data that is appropriate and meaningful.

On a distributed system, groups and group membership are synched from the Master server to the pollers, but only when the pollers are connected and running at the time of the modification. If a poller is not operational when the group change is made on the Master, the change will be synchronized when communication with the poller is restored.

### To add a new group:

1. On the **Group** tab in the NetVoyant Console, select the level in the group tree at which you want to add the group.
2. From the **File** menu, select **New > Group**.

The new group's details appear in the context panel.



3. On the **Details** tab in the context panel, enter the **Name** for the new group.
4. Enter a description of the group in the **Descr** field.
5. Click **Set**.
6. Populate the group with networks or devices.

For more information about this task, see [“Adding Devices, Poll Instances, or Interfaces to Groups”](#) on page 125.

## Adding and Modifying Group Settings

When you are using custom groups to manage your networks and devices in the NetVoyant Console, you will work with the group settings to configure how data is collected, aggregated, and reported.

**Note:** If your installation of the NetVoyant product is bound to the NetQoS Performance Center as a data source, the groups created in the NetVoyant Console are available and can be edited in the NetQoS Performance Center web interface. Groups created in the NetQoS Performance Center are visible in the NetVoyant Console, but can be edited or deleted only in the NetQoS Performance Center. For more information about managing reporting groups for data sources in the NetQoS Performance Center, see the *NetQoS Performance Center Administrator and User Guide*.

### Editing the Name and Description of a Custom Group

You can modify the name and description information for a custom group at any time in the group’s **Details** tab. This information helps you to identify the group for management and reporting purposes.

**Note:** On a distributed system, group details and group membership are synched from the Master server to the pollers, but only when the pollers are connected and running at the time of the modification. If a poller is not operational when the group change is made on the Master, the change will be synchronized when communication with the poller is restored.

### To edit the name and description of a group:

1. On the **Group** tab in the NetVoyant Console, select the group.

The group’s details appear in the context panel.

- On the **Details** tab in the context panel, edit the **Name** for the new group.

Groups can contain Devices or other Groups.

Name: Custom Group

Descr: group

Path: /Custom Group

- Edit the description of the group in the **Descr** field.
- Click **Set**.

### Configuring Polling for a Group

A poll group determines the polling rate and the short-term roll-ups (less than a day). To configure these for a group of devices, you can modify the poll group to which the poll instance belongs.

For example, you can apply a polling group with a polling rate of five minutes to the Device Availability dataset in the Routers group. The NetVoyant product then polls devices in the Routers group for data about Device Availability every five minutes.

**Note:** In a distributed system, if you make a group-level polling modification on a poller, only those devices assigned to that poller are affected by the change. So, for example, if you change the poll group for the Routers group on a poller, only those routers polled by that poller are changed. To ensure that all devices within a group are modified, make group level changes on the Master server.

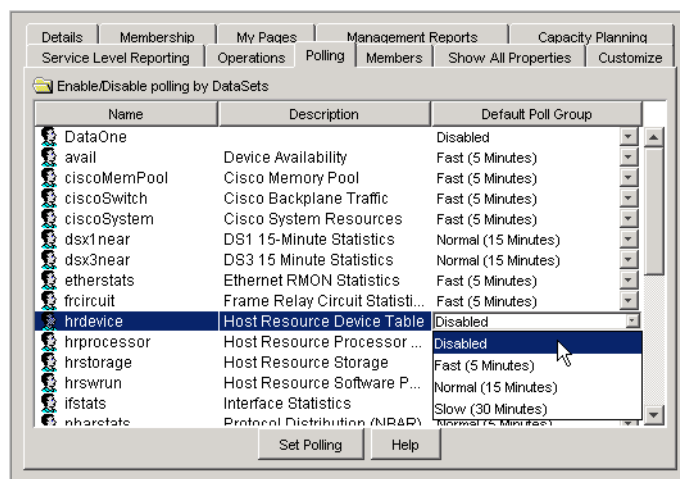
You can also enable or disable polling by dataset for a group on the group's **Polling** tab.

### To configure polling by dataset for a group:

- On the **Group** tab in the NetVoyant Console, expand the Master Console and group structure to locate the group.

The group details appear in the context panel.

- In the context panel for the group, select the **Polling** tab.
- To disable polling for a dataset, under the **Default Poll Group** column for the dataset, select **Disabled** from the drop-down menu.



4. To set the polling rate for a dataset, under **Default Poll Group** column for the dataset, select a polling group from the list.
5. Click **Set Polling**.

## Configuring a Polling Group for a Network

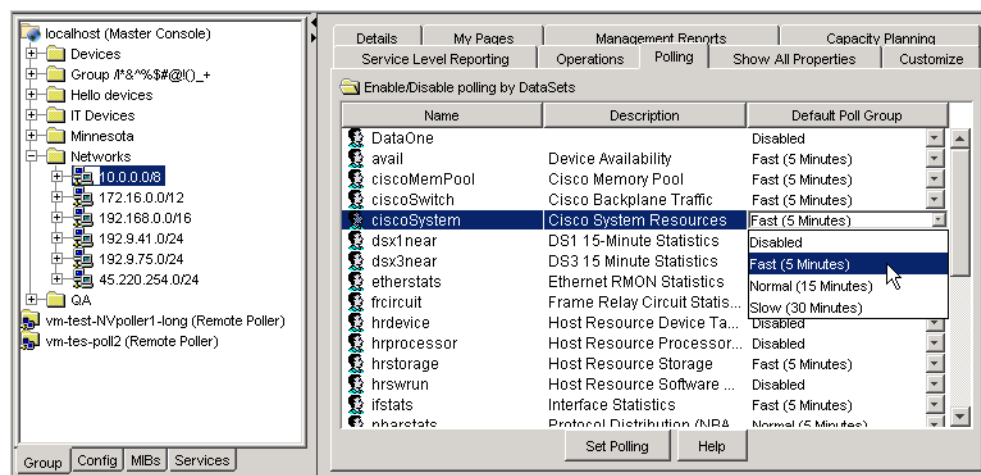
To configure polling for a network, you can apply a different polling group to the datasets in that network on the network's **Polling** tab. This sets how often the NetVoyant product polls devices in this network for data relating to each dataset.

For example, you can apply a polling group with a polling rate of five minutes to the Device Availability dataset in a network. It then polls devices in that network for data about Device Availability every five minutes.

**Note:** In a distributed system, if you make a group-level polling modification on a poller, only those devices assigned to that poller are affected by the change. So, for example, if you change the poll group for the a network on a poller, only those devices within the network that are polled by that poller are changed. To ensure that all devices within a network are modified, make network-level changes on the Master server.

### To configure polling by dataset for a network:

1. On the **Group** tab in the NetVoyant Console, expand the Master Console and locate the network. The network details appear in the context panel.
2. In the context panel for the network, select the **Polling** tab.
  - To disable polling for a dataset, under the **Default Poll Group** column for the dataset, select **Disabled** from the list.
  - To set the polling rate for a dataset, under the **Default Poll Group** column for the dataset, select a polling group from the list.



3. Click **Set Polling**.

## Adding Devices, Poll Instances, or Interfaces to Groups

After you create a custom group, you can populate it with devices and configure the poll instances that you need to manage the group. In a distributed configuration, you create or populate groups from the NetVoyant Console on the Master server.

**Note:** You can create and modify only NetVoyant groups in the NetVoyant Console. If your NetVoyant system is registered in the NetQoS Performance Center as a data source, the NetVoyant Console displays the groups created there, but you cannot modify them.

There are three methods for adding devices, poll instances, and interfaces to groups in the NetVoyant Console:

- Automatic grouping by device class or membership rules
- Copy and paste method (devices only)
- Including an individual poll instance or interface in a group

### Automatic Grouping

By default, the NetVoyant product automatically classifies new devices it discovers according to device model and class. It uses this classification to determine which device group to place new devices in. For example, it places a device identified as a router in the Routers group. You can define membership rules for automatic group population during discovery as well as manually change a device's classification and model.

To configure how the NetVoyant product groups new devices that it discovers, you can edit or add device classes and models. For example, you can add a device class called Linux Servers. You can then edit server device models that are Linux servers in your network to be in the Linux Server device class. When the NetVoyant product discovers new servers of this model, it automatically places them in the Linux Server group. For more information, see [“Changing a Device's Classification” on page 61](#) and [“Adding or Editing a Device Model” on page 63](#).

On a distributed system, groups and group membership are synched from the Master server to the pollers, but only when the pollers are connected and running at the time of the modification. If a poller is not operational when the group change is made on the Master, the change will be synchronized when communication with the poller is restored.

**Note:** You can use automatic group membership for NetVoyant groups only. If your NetVoyant installation is bound to the NetQoS Performance Center as a data source, you can view the NPC groups in the NetVoyant Console, but you cannot modify them.

You can also use expressions to define rules for automated grouping. The NetVoyant product evaluates these rules during discovery. When a “match” is found, it adds the poll instance or network to the group. You can use the following attributes to define auto-include expressions:

- Device Name
- Device Alias
- Device Class
- Device Model

- SNMP sysName
- SNMP sysDescr
- SNMP sysContact
- SNMP sysObjectId
- SNMP sysLocation
- Poller (for distributed systems)
- Poll-Instance Name
- Poll-Instance Description
- Device Property (any defined device property)
- Poll-Instance Property (any defined pollinst property)

**Note:** If automated population rule definitions are modified after a group has been automatically populated during discovery, the NetVoyant product does not remove those devices that no longer match during the next discovery. You must remove them manually if you want to omit them from the group.

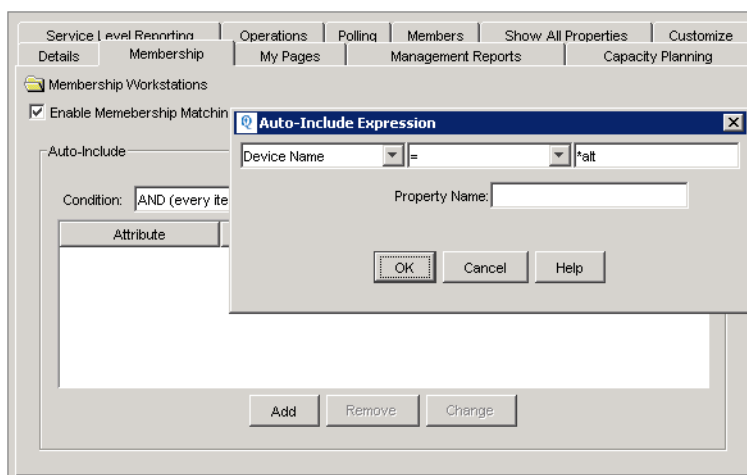
### To automatically populate a group during discovery:

1. On the **Group** tab in the NetVoyant Console (Master or standalone), select the group.
2. Click the **Membership** tab in the details panel.
3. Select **Enable Membership Matching**.

This enables the auto-population of groups using the defined criteria. You can clear this check box at any time to disable automated membership without deleting your definitions. This is useful when a group is currently populated and device matching is not required during discovery.

4. Use the **Condition** drop-down list to set the conditional type for the Auto-Include rules.
  - Select OR (any item matches) to include devices where the auto-include expression evaluates to true.
  - Select AND (every item must match) to include only those devices where all auto-include expressions evaluate to true.
5. Click **Add** to define the first auto-include expression.

The **Auto-Include Expression** dialog box opens.



6. Use the options at the top of the dialog box to build an auto-include expression (an attribute, an operator, and a value):

- Use the first drop-down list to select an attribute.
- Use the second drop-down list to choose an operator.

Operators are case sensitive except for the LIKE and NOT LIKE operators. For more information about the operators used in NetVoyant expressions, see [“Using NetVoyant Operators in Expressions”](#) on page 319.

- Use the box on the top-right to enter a value.

This field supports wild card values using the \* symbol. For example, an expression where Device Name = \*alt would evaluate to true for any device where the name ends with alt.

If you choose Device Property or Poll-Instance Property as the attribute, you must enter the name of the defined property in the **Property Name** field. For other attributes, this field remains empty.

7. Click **OK** to add the expression to the list in the **Membership** tab.
8. If you want to define additional auto-include expressions, click **Add** again to define another expression.
9. During the process of constructing a list of expressions, click **Remove** to delete an expression from the list or **Change** to change the expression.

**Note:** Having group membership enabled using auto-include expressions does **not** prevent you from manually modifying a group. Devices that do not match the criteria can be manually added to a group.

## Copying and Pasting a Device into a Group

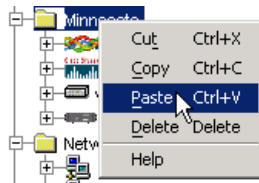
You can move devices from one group into another using copy and paste. When you copy and paste a device from one group into the other, the device becomes a member of both groups.

On a distributed system, groups and group membership are synched from the Master server to the pollers, but only when the pollers are connected and running at the time of the modification. If a poller is not operational when the group change is made on the Master, the change will be synchronized when communication with the poller is restored.

### To copy and paste a device into a group:

1. On the **Group** tab in the NetVoyant Console (Master or standalone), select the device.
2. From the **Edit** menu, select **Copy**.
3. Select the group or subgroup to which you want to add the device.
4. From the **Edit** menu, select **Paste**.

**Note:** You can also right-click the selected device and use the pop-up menu to select copy and paste functions.



This adds the device to the selected group.

**Note:** If your NetVoyant system is registered in the NetQoS Performance Center as a data source, the groups created in the NetVoyant Console are available and can be edited in the NetQoS Performance Center web interface. Groups created in the NetQoS Performance Center are visible in the NetVoyant Console, but can be edited or deleted only in the NetQoS Performance Center. For more information about managing reporting groups for data sources in the NetQoS Performance Center, see the *NetQoS Performance Center Administrator and User Guide*.

### Removing a Device From a Group

As you are managing reporting groups for your organization, you will need to remove a device from a group. This might be necessary if the device is taken out of service or if the device is re-deployed in another capacity. Removing a device from a group is a relatively simple task.

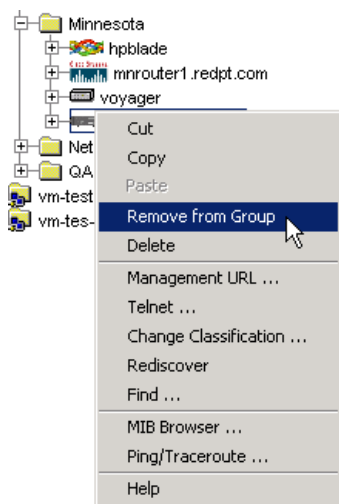
On a distributed system, groups and group membership are synched from the Master server to the pollers, but only when the pollers are connected and running at the time of the modification. If a poller is not operational when the group change is made on the Master, the change will be synchronized when communication with the poller is restored.



**Warning:** Do not delete a device to remove it from a group because this deletes the device and all related data from the NetVoyant product.

### To remove a device from a group:

- ▶ On the **Group** tab in the NetVoyant Console (Master or standalone), right-click the device and choose **Remove from Group**.



**Note:** If your NetVoyant system is registered in the NetQoS Performance Center as a data source, the groups created in the NetVoyant Console are available and can be edited in the NetQoS Performance Center web interface. Groups created in the NetQoS Performance Center are visible in the NetVoyant Console, but can be edited or deleted only in the NetQoS Performance Center. For more information about managing reporting groups for data sources in the NetQoS Performance Center, see the *NetQoS Performance Center Administrator and User Guide*.

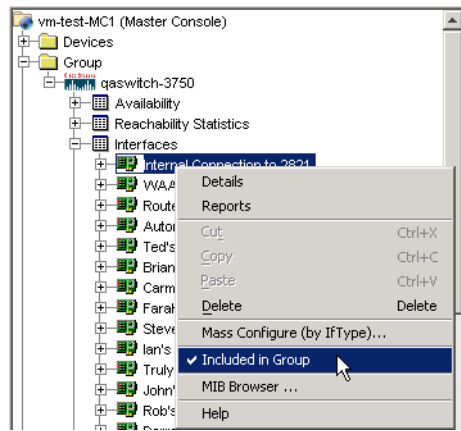
### Including and Excluding Poll Instance or Interface Data

Including a device's poll instances or interfaces in a custom group to which the device belongs makes the associated data available in reports generated for that custom group. If you do not include a poll instance or interface in a custom group, the poll instance or interface is not included in the group's reports and is not accessible by users who are limited to viewing only devices or poll instances for that group.

An administrator with the proper group permissions can exclude a device's poll instances or interfaces from a group to which the device belongs. Excluded poll instances or interfaces are omitted from the group's reports and are not accessible by users limited to viewing data for that group.

### To exclude one or more poll instances or interfaces from a custom group:

1. On the **Group** tab in the NetVoyant console, select one poll instance or interface or select multiple items from a common parent within a custom group.
2. Right-click the selection and clear **Included in Group**.



When this item is unchecked in the menu, the NetVoyant reporting tool does not include the selected object or objects in group-based reporting.

### To include one or more poll instances or interfaces in a custom group:

1. On the **Group** tab in the NetVoyant console, select one poll instance or interface or select multiple items from a common parent within a custom group.
2. Right-click the selection and select **Included in Group**.

## MANAGING DEVICES IN NETVOYANT

The NetVoyant console provides a number of ways to view information about your devices. While managing your devices you can access many types of useful information:

- View the details for a device, including polling and discovery configuration settings.
- View the alarms for a device.
- View reports about the device.
- View the interfaces on a device.
- View the poll tables for a device.
- View real-time graphs of data on a device.

### Managing Device Polling and Maintenance

Managing the polling status for devices provides the ability to exclude devices or groups of devices from impacting reporting (such as availability and reachability), as well as event and alarm conditions. Administrators often service equipment with little notice, taking the device offline, preventing SNMP polling tools from communicating with these devices. When this occurs and the device is part of the polling pool, the device appears as unavailable or in a distressed state and falsely sends alarms and tracks negative statistics that invalidate reports.

The NetVoyant Console provides both automated and manual mechanisms for managing the polling of devices and groups of devices so that servicing and other conditions do not interrupt the collection and display of accurate and useful data. By applying a Maintenance-Auto or Maintenance-Manual status, service/availability reporting is not impacted with “bad” data during known periods when

devices are taken down for servicing, reconfiguring, moving, or other occurrences. This also ensures that alarms are not logged and notifications are not sent for devices that are known to be out of normal service.

## Device Polling Status

Devices can fall into any one of these polling states, which dictates whether NetVoyant is currently polling the device:

Polling status	Description
Enabled	<p>In this state, the device is enabled for polling. All poll instances that are enabled are polled by the NetVoyant product according to the configuration settings. This is the normal, default state for devices.</p> <p>For more information about enabling a device for polling, see <a href="#">“Changing the Polling Status for a Device”</a> on page 148.</p>
Disabled	<p>In this state, the device is disabled from polling. All poll instances are disabled and poll instance licenses are not used and made available. A device can be disabled on an individual basis or as part of a disabled device class.</p> <p>For more information about disabling a device from polling, see <a href="#">“Changing the Polling Status for a Device”</a> on page 148.</p>
Maintenance-Manual	<p>In this state, the device is disabled from polling; however, poll instances remain in their pre-maintenance state. Poll instance licenses remain intact so that they cannot be used by other devices and polling can resume when the device is enabled. This state must be applied manually in the NetVoyant console and have polling enabled manually when it is no longer in need of exclusion.</p> <p>For more information about maintenance schedules, see <a href="#">“Applying a Manual Maintenance Exclusion”</a> on page 135.</p>
Maintenance-Auto	<p>This state is identical to the Maintenance-Manual state, except that it occurs only as a result of a maintenance window schedule for the device. NetVoyant automatically excludes the device from polling and enables it based on the schedule.</p> <p>For more information about maintenance schedules, see <a href="#">“Using Maintenance Schedules”</a> on page 132.</p>
Out-of-Scope	<p>This state is applied by the NetVoyant console automatically when it is determined at discovery that the device is no longer in scope. When a device enters this state, its “time-to-live” clock starts and it is scheduled for removal.</p> <p>For more information about setting discovery options for device expiration and removal, see <a href="#">“Configuring Discovery Options”</a> on page 52.</p>
Does-Not-Resolve	<p>This state is applied by the NetVoyant console automatically when it is determined at discovery that the device no longer resolves. When a device enters this state, its “time-to-live” clock starts and it is scheduled for removal.</p> <p>For more information about setting discovery options for device expiration and removal, see <a href="#">“Configuring Discovery Options”</a> on page 52.</p>

Polling status	Description
Unresponsive	<p>This state is applied by the NetVoyant console when a device does not respond to discovery queries over an established period of time. When a device enters this state, its “time-to-live” clock starts and it is scheduled for removal.</p> <p>For more information about setting discovery options for device expiration and removal, see <a href="#">“Configuring Discovery Options” on page 52</a>.</p>
Offline	<p>In this state, device expiration is stopped. This state must be applied manually, and it can be changed to Enabled or the device can be manually deleted by an administrator.</p> <p>For more information about setting discovery options for device expiration and removal, see <a href="#">“Configuring Discovery Options” on page 52</a>.</p>

## Using Maintenance Schedules

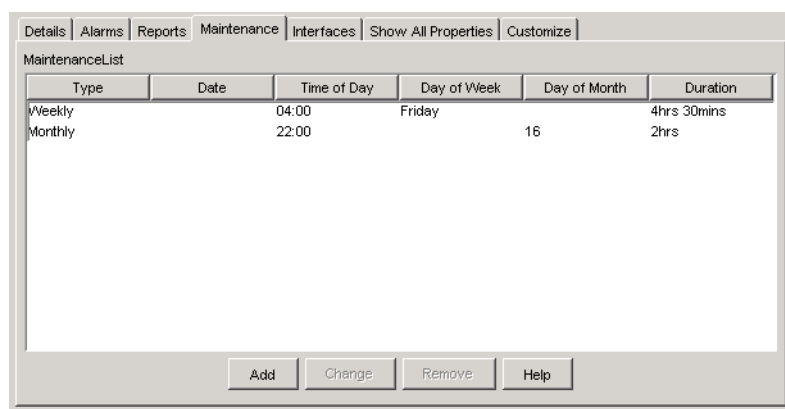
NetVoyant polling data is used to calculate aggregations for reporting purposes. These aggregations are only as accurate as the underlying data. If the NetVoyant system is polling devices that should not be included in reporting aggregations, high-level management reports are much less useful.

When you set a maintenance schedule window for a device or group, the NetVoyant console automatically suppresses polling, alarms, and event notifications for the device according to the start and stop times of the window.

**Note:** In a distributed NetVoyant system, maintenance schedules are defined and applied only on the Master server. You cannot add or change maintenance schedules on a poller.

### To view the maintenance schedule for a device or group:

1. On the **Group** tab in the NetVoyant Console (Master or standalone), select the group or the individual device.
2. Click the **Maintenance** tab.



The tab panel displays any existing maintenance schedule items, providing the following details for each item:

Parameter	Description
<b>Type</b>	This is the type of schedule, based on the recurrence. NetVoyant supports Monthly, Weekly, Daily and One-time maintenance window types.
<b>Date</b>	If the Type is One-time, this indicates the scheduled date for the start of the maintenance window.
<b>Time of Day</b>	This indicates the start time for maintenance window
<b>Day of Week</b>	If the Type is Weekly, this indicates the day of week when the maintenance window is scheduled to start.
<b>Day of Month</b>	If the Type is Monthly, this indicates the date in the month when the maintenance window is scheduled to start.
<b>Duration</b>	This indicates the duration of the maintenance window in hours.

## Adding and Editing Maintenance Schedules

You can add a maintenance schedule item for a selected device or group in the NetVoyant Console. When the scheduled time period occurs, the device or group of devices is automatically changed to a Maintenance-Auto polling status. When the time period ends, the device or devices within the group are returned to their previous state.

**Note:** In a distributed NetVoyant system, maintenance schedules are defined and applied only on the Master server. You cannot add or change maintenance schedules on a poller.

### To add or edit a maintenance schedule window:

1. On the **Group** tab in the NetVoyant console, select the group or the individual device.
2. Click the **Maintenance** tab.
3. Perform one of the following:
  - To add a new maintenance window, click **Add**.
  - To edit a maintenance window, select the item in the list and click **Change**.

This opens the **Maintenance Schedule** dialog box.

## 4. Set the options according to the type of schedule you want:

Frequency	Option settings
One-time	<p>Set these options to schedule a one-time maintenance window:</p> <ul style="list-style-type: none"><li>Under <b>Schedule Type</b>, select <b>Once</b> and click the date button to select the date from the <b>Select Date</b> dialog box.</li></ul>  <p>The 'Select Date' dialog box displays a calendar for February 2009. The date 12 is highlighted in blue. The calendar grid shows days of the week (Sun to Sat) and dates (1 to 28). Below the calendar are 'Ok' and 'Cancel' buttons.</p> <ul style="list-style-type: none"><li>Set the <b>Start Time</b>.</li><li>Set the <b>Duration</b> to specify the length of the window. This can be any number of days and hours. To specify a window of 24 hours, simply set the <b>Days</b> to 1 and leave the <b>HH:MM</b> at 00:00. To specify a 36-hour window, set the Days to 1 and the HH:MM to 12:00.</li></ul>
Daily	<p>Set these options to schedule a daily maintenance window:</p> <ul style="list-style-type: none"><li>Under <b>Schedule Type</b>, select <b>Daily</b>.</li><li>Set the <b>Start Time</b>.</li><li>Set the <b>Duration</b> to specify the length of the window. This can be any number of days and hours. To specify a window of 12 hours, simply set the <b>Days</b> to 0 and set the HH:MM to 12:00.</li></ul>
Weekly	<p>Set these options to schedule a weekly maintenance window:</p> <ul style="list-style-type: none"><li>Under <b>Schedule Type</b>, select <b>Day of Week</b> and choose the day of the week to start the window from the drop-down list.</li><li>Set the <b>Start Time</b>.</li><li>Set the <b>Duration</b> to specify the length of the window. This can be any number of days and hours. To specify a window of 24 hours, simply set the <b>Days</b> to 1 and leave the <b>HH:MM</b> at 00:00. To specify a 36-hour window, set the Days to 1 and the HH:MM to 12:00.</li></ul>
Monthly	<p>Set these options to schedule a monthly maintenance window:</p> <ul style="list-style-type: none"><li>Under <b>Schedule Type</b>, select <b>Day of Month</b> and choose the date of the month to start the window from the drop-down list.</li><li>Set the <b>Start Time</b>.</li><li>Set the <b>Duration</b> to specify the length of the window. This can be any number of days and hours. To specify a window of 24 hours, simply set the <b>Days</b> to 1 and leave the <b>HH:MM</b> at 00:00. To specify a 36-hour window, set the Days to 1 and the HH:MM to 12:00.</li></ul>

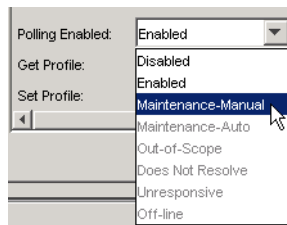
5. Click **OK** to close the dialog box.

## Applying a Manual Maintenance Exclusion

Scheduling a maintenance window is an automated way to place devices or groups into a maintenance state so that polling and alarming are temporarily suppressed. However, in the event that a maintenance or disruptive event occurs without planning or warning, you can manually apply a maintenance status to a device. When you are ready to resume polling and alarming, you must then manually change the polling status back.

### To manually apply a maintenance exclusion to a device:

1. On the **Group** tab in the NetVoyant Console, select the individual device.
2. In the context panel for the device, select the **Details** tab.
3. For the **Polling Enabled** setting, select **Maintenance-Manual** from the drop-down list.



**Note:** Maintenance-Auto, Unresponsive, Out-of-Scope, and Does Not Resolve are states applied automatically by NetVoyant according to maintenance schedules and occurrences at discovery. You cannot manually apply one of these states.

4. Click **Set**.

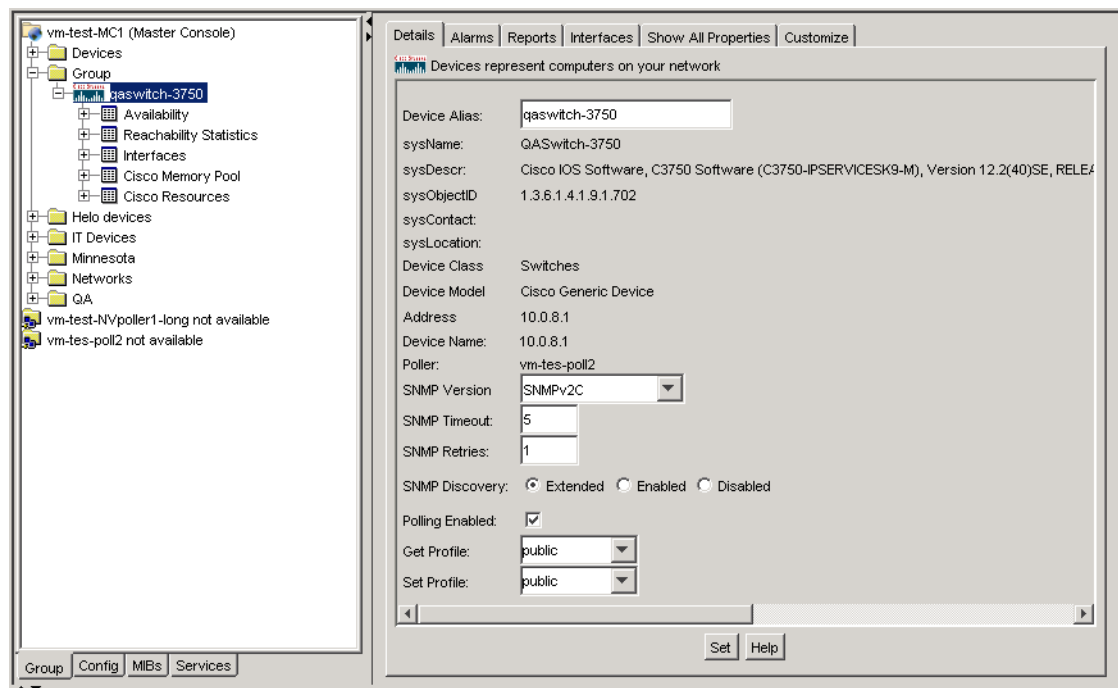
## Configuring Details for a Device

When you have a device selected, the **Details** tab in the NetVoyant Console provides access to its basic configuration information. You can modify some of this information directly in this tab, as well as access other device-specific information.

### To view details for a device:

1. On the **Group** tab in the NetVoyant Console, select the device.

The device's details appear in the context panel.



- On the **Details** tab you can view the following details for a device:

Parameter	Description
<b>Device Alias</b>	The device's name in the NetVoyant product. By default, devices are named using the device's DNS name or, for unresolvable names, the device's IP address. You can also edit the device alias to another value on the device's Details tab. For more information, see <a href="#">“Editing a Device Alias” on page 148</a> .
<b>sysName</b>	The device's name as identified in the <code>sysName</code> OID on the device. You can configure the NetVoyant product to apply names to your discovered devices using the <code>sysName</code> OID. For more information, see <a href="#">“Configuring Discovery Options” on page 52</a> .
<b>sysDescr</b>	The device's description as identified in the <code>sysDescr</code> OID on the device.
<b>sysObjectID</b>	The device's SNMP agent uniquely identifies the device model using the <code>sysObjectID</code> .
<b>sysContact</b>	The device's contact person as identified in the <code>sysContact</code> OID on the device.
<b>sysLocation</b>	The device's location as identified in the <code>sysLocation</code> OID on the device.
<b>Device Class</b>	The device's class as identified by the NetVoyant product during discovery. For more information, see <a href="#">“Configuring Device Classes and Models” on page 59</a> .
<b>Device Model</b>	The device's model as identified by NetVoyant during discovery. For more information, see <a href="#">“Configuring Device Classes and Models” on page 59</a> .
<b>Address</b>	The device's IP address.
<b>Device Name</b>	The device's DNS name or, for unresolvable names, the device's IP address. <b>Note:</b> If you change the IP address for the device, you must also add the updated address to the discovery scope. Otherwise, the device will be assigned an Out-of-Scope status during the next rediscovery and polling for the device will be suspended.



Parameter	Description
<b>Poller</b>	The NetVoyant server that polls the device for SNMP statistics. In a distributed configuration, the Poller is the NetVoyant server that polls the device. In a standalone configuration, the Poller is always the Master server.
<b>SNMP Version</b>	The SNMP version used for polling the device.
<b>SNMP Timeout</b>	The length of time in seconds that the NetVoyant product waits for an SNMP reply from the device before it considers the request to have timed out. Longer timeouts significantly increase how long it takes to complete the discovery process.
<b>SNMP Retries</b>	The number of times the NetVoyant product retries the device for each SNMP profile if an SNMP request times out. More retries significantly increase how long it takes to complete the discovery process.
<b>SNMP Discovery</b>	<p>Indicates how the device is configured for discovery. For more information, see <a href="#">“The NetVoyant Discovery Process”</a> on page 49.</p> <p>The following are possible values for SNMP Discovery:</p> <ul style="list-style-type: none"> <li>• <b>Extended</b> indicates that the device is set to extended discovery. The NetVoyant product rediscovers this device’s characteristics during its rediscovery process. It also uses information in the ARP cache and IP routing table for this device to discover other devices to discover.</li> <li>• <b>Enabled</b> indicates that the device is enabled normally for discovery. The NetVoyant product rediscovers this device’s characteristics during its rediscovery process.</li> <li>• <b>Disabled</b> indicates that discovery is disabled for the device. The NetVoyant product does not rediscover this device’s characteristics during its rediscovery process.</li> </ul>
<b>Polling Enabled</b>	<p>Indicates the polling status for the device.</p> <p>You can use this drop-down list to change the device’s polling status.</p> <p>If polling is Enabled, the NetVoyant product is gathering data for the device. If polling is Disabled, all poll instances are disabled and are not utilizing poll instance licensing. Other polling status options are used for device maintenance exclusions and discovery issues with the device.</p> <p>For more information about polling status, see <a href="#">“Device Polling Status”</a> on page 131.</p>

Parameter	Description
<b>Get Profile</b>	<p>The profile that the NetVoyant product uses for SNMP get (read) operations on the device.</p> <p>Profiles are used by SNMP-enabled devices to verify the identity of requesting managers. The NetVoyant product uses the profiles supported by your devices for these devices to respond to discovery and polling SNMP requests. If you do not want to use a profile, you can simply enter a valid community string in this text box (no verification).</p> <p>For more information, see <a href="#">“Setting SNMP Profiles for a Device” on page 149</a>.</p>
<b>Set Profile</b>	<p>The profile that the NetVoyant product uses for SNMP set (write) operations on the device.</p> <p>Profiles are used by SNMP-enabled devices to verify the identity of requesting managers. If you do not want to use a profile, you can simply enter a valid community string in this text box (no verification).</p> <p>If you plan to configure IP SLA operations for a device directly from the NetVoyant Console, you must enter the set profile for the device. For assistance with this task, see <a href="#">“Setting SNMP Profiles for a Device” on page 149</a>.</p>

## Viewing the Alarms for a Device

View the alarms related to a device and all of its poll instances and interfaces on the **Alarms** tab for the device. This tab also allows you to acknowledge alarms that have been remedied, which is similar to acknowledging alarms in the alarm log panel.

By default, the Alarms tab displays information using a color-coded list. If you want to change the colors used to display this list, select **Event Severity** in the **Logs** menu.

For more information about alarms, see [“Using Events and Alarms” on page 190](#).

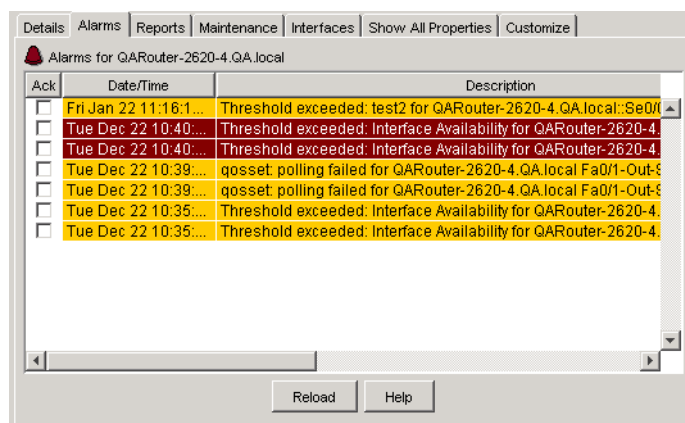
### To view and acknowledge alarms for a device:

1. On the **Group** tab in the NetVoyant Console, select the device.

The device’s details appear in the context panel.

**Note:** If the Alarms tab does not appear in the context panel, click the **Customize** tab to select the **Alarms** tab for display.

2. Click the **Alarms** tab.



This tab displays a color-coded list of alarms for the selected device with the following details for each alarm:

Parameter	Description
<b>Ack</b>	This check box enables you to acknowledge an alarm event that you have already addressed.
<b>Date/Time</b>	The server date and time at which the alarm occurred.
<b>Description</b>	A description of the alarm that occurred.
<b>Source</b>	The service or device that initiated the alarm.
<b>Severity</b>	The severity level of the alarm. Alarms can be one of the following severity levels: Warning, Minor, Major, or Critical. The NetVoyant product labels alarm logs by color according to their severity. It also labels the device and group that was the source of the alarm log in the Group tab of the tree-tab panel.
<b>Type</b>	The type of alarm. Possible alarm types include threshold, polling, and trap.
<b>Category</b>	The event category. Possible categories are status, threshold, performance, or configuration.
<b>Error code</b>	A code to assist technical support in diagnosing issues.
<b>Server</b>	The server on which the service that initiated the alarm resides.

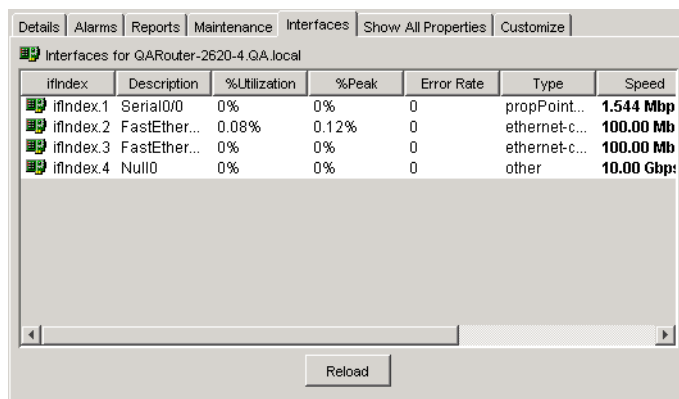
- To acknowledge an alarm, select the **Ack** check box next to the alarm.

## Viewing the Interfaces for a Device

The **Interfaces** tab in the context panel provides a list of the interfaces that are on a selected device. For more information about managing individual interfaces on a device, see [“Working with Poll Instances and Interfaces” on page 161](#).

### To view the interfaces on a device:

- On the **Group** tab in the NetVoyant Console, select the device.  
The device’s details appear in the context panel.
- Click the **Interfaces** tab.



**Note:** If the Interfaces tab does not appear in the context panel, click the **Customize** tab to select the Interfaces tab for display.

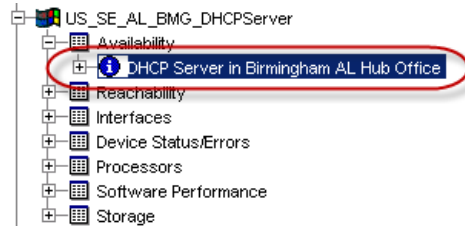
The **Interfaces** tab displays a list of interfaces on the selected device and their details. Click **Reload** to reload the details on this tab. The following details are shown for each interface:

Parameter	Description
<b>ifIndex</b>	The index for an interface's SNMP ifEntry table.
<b>Description</b>	The description for an interface as configured in NetVoyant.
<b>%Utilization</b>	The average utilization of an interface over the past 24 hours as a percent of total bandwidth.
<b>%Peak</b>	The peak utilization of an interface over the past 24 hours as a percent of total bandwidth.
<b>Error Rate</b>	The average error rate for an interface over the past 24 hours.
<b>Type</b>	An interface's type as defined by the ifType field in the SNMP ifEntry table.
<b>Speed</b>	<p>An interface's speed as defined by the ifSpeed field in the SNMP ifEntry table.</p> <p><b>Note:</b> You can configure an interface's speed by double-clicking the this field for the interface.</p> <p>For more information, see <a href="#">“Editing the Interface Speeds” on page 170</a>.</p>
<b>ifOperStatus</b>	<p>The physical status of an interface, which can be one of the following values:</p> <ul style="list-style-type: none"><li>• <b>Up</b> - The interface is operational.</li><li>• <b>Down</b> - The interface is not operational.</li></ul> <p>You can use an interface's operational status (ifOperStatus) to dynamically disable polling for non-operational interfaces. This enables you to restrict poll instance usage and data storage for interfaces that are not in use.</p> <p>For more information, see <a href="#">“Disabling Polling for Non-Operational Interfaces” on page 91</a>.</p>
<b>ifAdminStatus</b>	<p>The configured status of an interface, which can be one of the following values:</p> <ul style="list-style-type: none"><li>• <b>Up</b> - The interface is operational.</li><li>• <b>Down</b> - The interface is not operational.</li></ul>
<b>Physical Address</b>	The physical address of an interface according to the SNMP ifEntry table.

## Viewing Poll Tables for a Device

The NetVoyant product organizes poll instances into poll tables referenced and defined by dataset. If a device supports the MIB table upon which a dataset is based, it creates a poll table for the device in the dataset. It then places poll instances for that device in the correlated poll table.

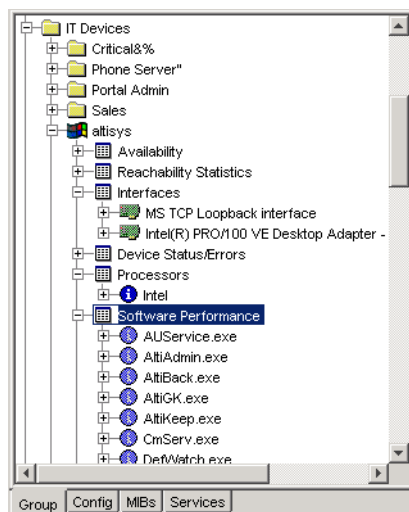
If a device supports a dataset, it has a poll table and poll instances representing the data collected for that dataset. For example if a device supports the Device Availability dataset based on a table defined in the RFC1213 MIB, the NetVoyant product creates an Availability poll table for the device and places poll instance representing availability data in this poll table.



**Note:** For more information about the poll instances in the poll tables, see “Working with Poll Instances and Interfaces” on page 161.

### To view the poll tables for a device:

1. On the **Group** tab in the NetVoyant Console, locate the device.
2. Expand the device by clicking the + sign next to it.



3. To view the poll instances in a poll table, expand the poll table by clicking the + symbol next to it.

## Poll Instance and Interface Icons

In the NetVoyant Console, poll instances and interfaces appear under devices in poll tables. Each poll instance and interface in a poll table has an icon next to it to indicate its type and status.

The icons for a poll instance or interface indicate the following:



The poll instance is included in the group under which it currently appears in the NetVoyant Console and polling is enabled on the poll instance.



Polling is disabled for the poll instance. If polling is disabled for a poll instance, the NetVoyant poller does not gather data for the poll instance. For more information, see [“Configuring Polling for Poll Instances and Interfaces” on page 166](#).



The interface is included in the group under which it currently appears in the NetVoyant Console and polling is enabled on the interface.



Polling is disabled for the interface. If polling is disabled for an interface, the NetVoyant product does not gather data for the interface. For more information, see [“Configuring Polling for Poll Instances and Interfaces” on page 166](#).



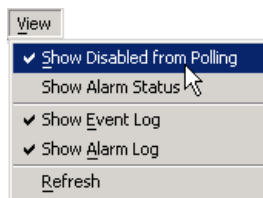
The poll instance or interface has triggered an alarm. This icon can also be red or cyan, depending on the severity level of the alarm. For more information, see [“Viewing and Acknowledging Alarms” on page 167](#).

## Showing and Hiding Disabled Poll Instances

In the NetVoyant Console, you can choose to show or hide disabled devices, poll instances, and interfaces. Hiding those items that are disabled removes the extraneous items from the NetVoyant workspace, making it easier to locate the devices, interfaces, and poll instances that are of importance to you.

### To show or hide disabled devices, poll instances, and interfaces:

- Select **View > Show Disabled from Polling** in the main menu.



A check mark appears next to this menu command when the setting is selected (active), indicating that disabled objects are currently visible.

When the setting is not selected (inactive), it does not have a check mark, indicating that disabled objects are not currently visible.

**Note:** Some poll instances act as a parent container to child poll instances. In this situation, the parent poll instance can be disabled even when one or more of the child poll instances are enabled. If you do not have the **Show Disabled from Polling** option selected, these child poll instances do not appear even though they are enabled.

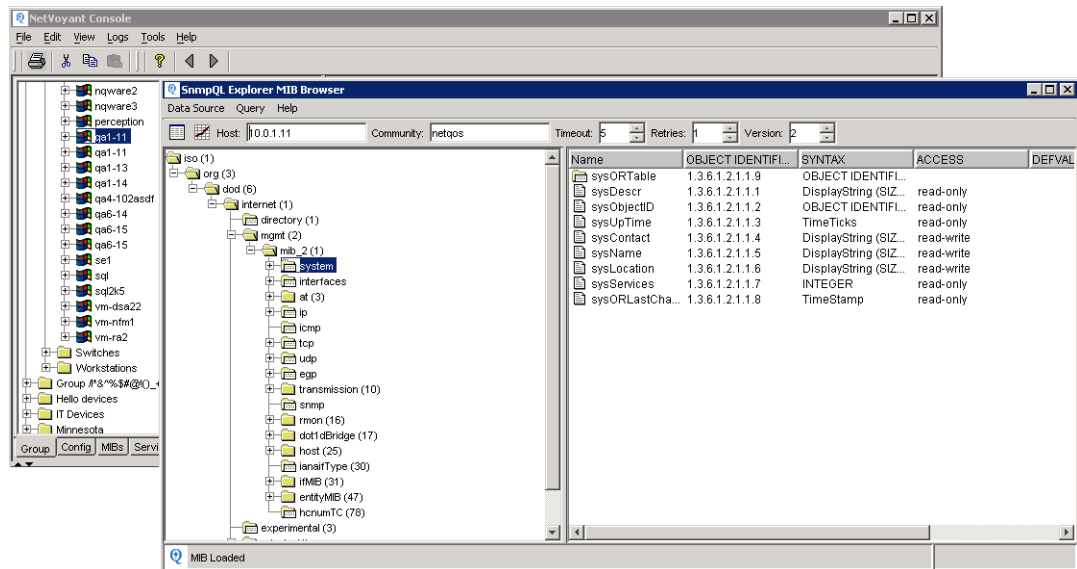
## Viewing the MIBs Supported by a Device

The MIB Browser enables you to browse the SNMP Management Information Bases (MIBs) currently recognized by your NetVoyant system. You can also use the MIB Browser to view all the MIBs that are compiled into the NetVoyant product.

For more information about managing MIBs in the NetVoyant Console, see [Chapter 5, “Working with Management Information Bases”](#) on page 177.

### To view the MIBs supported by a device in the MIB Browser:

- On the **Group** tab in the NetVoyant Console, right-click a device and select **MIB Browser**.



The MIB Browser opens and displays all MIBs that are compiled into the NetVoyant system.

## Viewing Real-Time Graphs for a Device

To troubleshoot whether the NetVoyant system can get data relating to a selected MIB for a device, you can use real-time graphs in the MIB browser.

You can also view the following real-time graphs for MIB values:

- Real-time graphs for an interface. For more information, see [“Viewing a Real-Time Graph for an Interface”](#) on page 172.
- Real-time graphs for a selected OID in a MIB by device. For more information, see [“Performing an SNMP Query on a Device”](#) on page 145.

### To view a real-time graph for values in a MIB table on a device:

1. On the **Group** tab in the NetVoyant Console, browse for and locate the device.
2. Right-click the device and select **MIB Browser**.

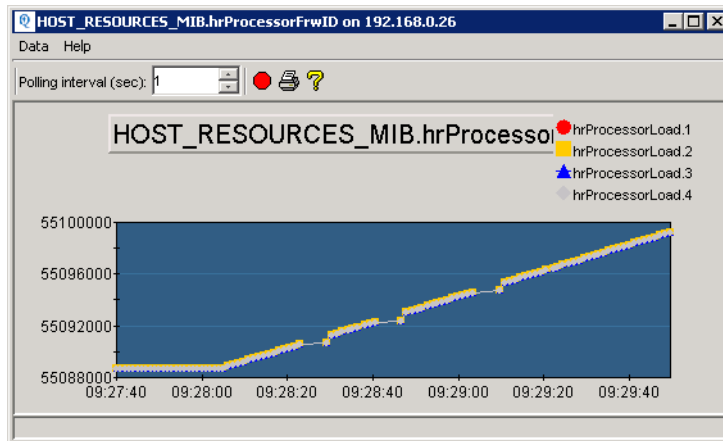
The MIB browser opens and displays the selected device as the Host.

3. Browse for and select the MIB in the MIB tree.

The OIDs for the selected MIB appear in the OID panel.



4. Click the graph icon (  ) at the top of the MIB browser to display a real-time graph for data in the tables for the selected MIB on the device.

A real-time graph displays data for each OID plotted as separate lines on the graph.



5. (Optional) To configure the frequency for adding plot points to the graph, edit the **Polling interval**. You can lower the polling interval to as low as 1 second for a real-time graph.
6. (Optional) To print the graph, click the printer icon.  
Printing the real-time graph is only possible if there is a printer installed for the NetVoyant server where you are accessing the MIB browser.

**Troubleshooting a Real-time Graph.** If a real-time graph displays no data after a few seconds, then one of the following might be true:

Problem	Solution
The device does not support the selected MIB.	Check your device vendor's documentation for more information on which MIBs the device supports.
The device is not configured for SNMP or is not SNMP capable.	Check your device vendor's documentation for more information on SNMP support.
The device is not available to the NetVoyant product.	Check network connectivity for the NetVoyant Master Console and the device.
The polling interval for the real-time graph is too high.	You can lower the Polling interval to as low as 1 second for a real-time graph.
You have stopped polling for the real-time graph.	You can stop polling on a real-time graph at any time by clicking the red stop button  . To restart polling, click the green go button  .




## Performing an SNMP Query on a Device

To view data relating to a selected MIB for a device, use the querying feature in the MIB browser. This sends a specific query for the MIB so that you can determine how it is supported on the device.

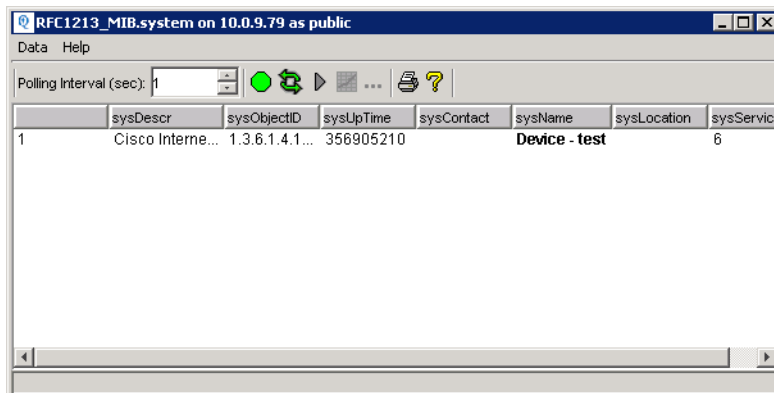
### To view query data relating to a MIB for a device:

1. On the **Group** tab in the NetVoyant Console, browse for and locate the device.
2. Right-click the device and select **MIB Browser**.







The MIB browser displays with the device selected as the Host.

3. Perform one of the following:
  - From the **Query** menu, select one of the pre-configured queries and skip to step 5.  
The query window opens.
  - To perform a custom query on a MIB, browse for and select the MIB.  
The OIDs for the selected MIB appear in the OID panel.
4. Click the query icon  at the top of the MIB browser to display data in the tables for the selected MIB on the device.

The query window opens and displays data for each OID entered in a separate field.



5. You can perform the following tasks in the query window:

Task	Description
Query real-time data from the device	<p>To get real-time data in the query table, enable polling for the data. This updates the data in the query window according to the Polling Interval.</p> <ul style="list-style-type: none"> <li>Click the green go button .</li> <li>Stop polling on a real-time graph at any time by clicking the red stop button .</li> <li>Edit the <b>Polling Interval</b> to configure the frequency for updating the query data.</li> </ul>
Edit a value for an OID	<p>To edit a value for an OID in the query window:</p> <ul style="list-style-type: none"> <li>Double-click the field and enter the new value.</li> <li>Click the update icon  to update the selected field on the device. An error message appears at the bottom of the query window if the NetVoyant product is unable to make the change.</li> <li>Click the reload icon  to verify that the NetVoyant product was able to update the information on the device.</li> </ul>
Print the query information	<p>To print the query information, click the printer icon .</p> <p>You must have a printer installed on the NetVoyant server on which you are accessing the MIB browser to print the real-time graph.</p>
View a real-time graph of the values for a selected OID	<p>To display a real-time graph for values for an OID on the selected device:</p> <p>Select the cell that contains the OID value in the query window and click the graph icon .</p> <p>For more information about displaying real-time graphs for a device, see <a href="#">“Viewing Real-Time Graphs for a Device”</a> on page 143.</p>

**Note:** If no data appears in a query after a few seconds, see [“Troubleshooting a Real-time Graph”](#) on page 144 for possible issues with the query.

## Configuring Devices in the NetVoyant Console

Perform the following tasks to configure how the NetVoyant product displays and collects information for your devices:

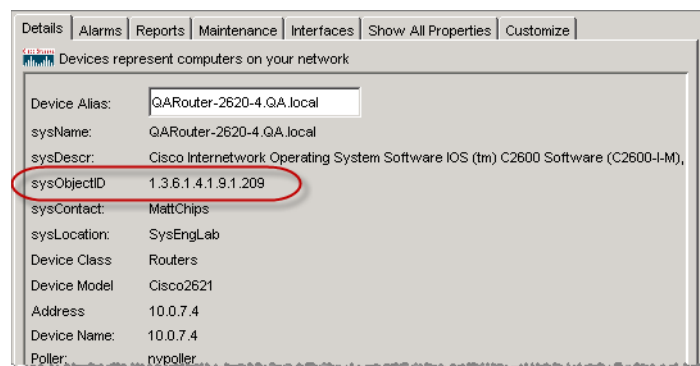
- Edit the device class.
- Edit the device alias.
- Configure the discovery settings for the device.
- Enable or disable polling for a device.
- Enter or edit the SNMP profiles for the device.
- Add or set values for properties for a device.
- Configure the default poll instance and interface names (by dataset).
- Rediscover a device.
- Start a Telnet session with a device.
- Disable polling for non-operational interfaces.
- Disable polling for interfaces without traffic.

### Classifying Devices

The class and model of a device determine what group the NetVoyant product places the device in upon discovery. The device class and model is determined from the `sysObjectID` of the device, which is determined during the discovery process.

You can add or edit the device class for the `sysObjectID` for a device to configure what device class and model the NetVoyant product considers the device to be. For more information, see [“Configuring Device Classes and Models” on page 59](#).

You can view a device’s `sysObjectID` on the **Details** tab for the device in the NetVoyant Console. For more information, see [“Configuring Details for a Device” on page 135](#).



## Editing a Device Alias

The device alias is the name used for the device in the NetVoyant product. By default, it names devices using the DNS name for the device or, for unresolvable names, the device's IP address. You can edit the device alias that it sets for a device on the **Details** tab for the device.

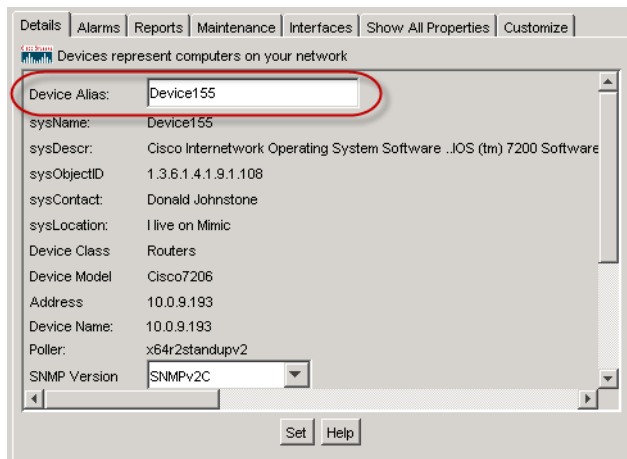
**Note:** You can also configure the NetVoyant product to set aliases for your devices using the IP address or sysName OID, or to automatically strip the domain name from the device alias. For more information, see [“Configuring the Device Naming Parameters” on page 56](#).

### To edit the alias of a device:

1. In the **Group** tab of the NetVoyant Console, expand the group structure to locate and select the device.

The device's details appear in the context panel.

2. In the context panel for the device, select the **Details** tab.
3. Edit the **Device Alias**.



4. Click **Set**.

## Changing the Polling Status for a Device

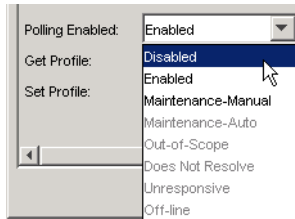
In the **Details** tab, you can change the polling for a device. If you disable polling for a device, the NetVoyant product does not gather information from the device and any used poll instance licenses are returned to the pool so that they are available to other enabled devices. There are additional polling states that are used for suppressing polling and alarming for devices.

For more information about how to utilize polling status to manage polling and alarming, see [“Managing Device Polling and Maintenance” on page 130](#).

### To change the polling status for a device:

1. On the **Group** tab in the NetVoyant Console, browse for and locate the device.
2. In the context panel for the device, select the **Details** tab.

3. For the **Polling Enabled** setting, do one of the following:
  - To enable polling for the device, select **Enabled** from the drop-down list.
  - To disable polling for the device, select **Disabled** from the drop-down list.
  - To manually apply a maintenance exclusion to the device, select **Maintenance-Manual** from the drop-down list.
  - If the device is currently in an Unresponsive, Out-of-Scope, or Does Not Resolve state and you want to keep it from being automatically removed, select **Off-line** from the drop-down list.



**Note:** Maintenance-Auto, Unresponsive, Out-of-Scope, and Does Not Resolve are states applied automatically by NetVoyant according to maintenance schedules and occurrences at discovery. You cannot manually apply one of these states.

4. Click **Set**.

**Note:** To hide devices, poll instances, and interfaces that are disabled for polling in the NetVoyant Console, clear the **Show Disabled from Polling** option in the **View** menu.

## Setting SNMP Profiles for a Device

The NetVoyant product uses profiles in order to establish access to the devices on your network. In defining a profile, you create an identity used for authentication when performing SNMP queries and sets. The NetVoyant Console supports authentication to devices using SNMPv1, SNMPv2C, and SNMPv3.

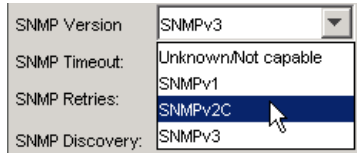
The NetVoyant product needs to know the read profile (the get profile) supported by your devices in order for them to respond to discovery and SNMP polling requests. If you plan to configure IP SLA tests for a device from the NetVoyant Console, you must enter the read and write profiles (the get and set profiles) for the device. Configure these profiles directly in the Configuration Wizard or **Config** tab, and set them manually for a device in the **Details** tab.

During initial discovery, the NetVoyant product attempts to discover devices using the profiles in the SNMP profiles list, testing them according to their priority order in the list and assigning the first successful match. If you want to change a device to a profile using another SNMP version after initial discovery, you can remove the currently assigned SNMP version by setting it to **Unknown/Not capable**, and then rediscover the device. You can also manually change the get and set profiles to the known SNMP profile and then rediscover the device.

### To set the SNMP profiles for a device:

1. On the **Group** tab in the NetVoyant Console, browse for and locate the device.
2. In the context panel for the device, select the **Details** tab.

3. Use the **SNMP Version** setting to specify the SNMP version used to access the device.



The screenshot shows a configuration window with four rows: 'SNMP Version', 'SNMP Timeout', 'SNMP Retries', and 'SNMP Discovery'. Each row has a corresponding dropdown menu. The 'SNMP Version' dropdown is open, showing a list of options: 'SNMPv3', 'Unknown/Not capable', 'SNMPv1', 'SNMPv2C' (which is highlighted with a mouse cursor), and 'SNMPv3'.

If you want NetVoyant to automatically determine the SNMP version and profile using the priority order of the SNMP Profiles list, select **Unknown/Not capable**.

4. Enter or edit the following parameters:

Parameter	Description
<b>Get Profile</b>	The profile to use for SNMP get (read) operations on the device. Use the drop-down list to select a defined SNMP profile or to select the “blank” item at the top of the list so that NetVoyant automatically assigns a profile at discovery based on the priority order of the SNMP profile list.
<b>Set Profile</b>	The profile to use for SNMP set (write) operations on the device. Use the drop-down list to select a defined SNMP profile or to select the “blank” item at the top of the list so that NetVoyant automatically assigns a profile at discovery based on the priority order of the SNMP profile list. If you plan to configure IP SLA operations for a device directly from the NetVoyant Console, there must be a set profile for the device.

5. Click **Set**.

For more information about configuring SNMP profiles for accessing your devices, see [“Defining SNMP Profiles”](#) on page 35.

## Managing Device Discovery

The NetVoyant product performs a nightly rediscovery by default. When you modify discovery settings for devices you can control the discovery process and which devices it includes in discovery.

### Editing Discovery Settings for a Device

To remove a device from the scheduled rediscovery, you can disable discovery for the device. The NetVoyant product does not update information from devices that are disabled for discovery.

You can also edit the SNMP timeouts and retries for a device to change how sensitive the NetVoyant product is to timeouts and retries for this device during the discovery process.

**Note:** During rediscovery, the NetVoyant product does not queue or update information for a disabled device. It uses information in the ARP cache and IP routing tables of devices set to extended discovery. For more information about how it uses information from devices set to extended discovery, see [“The NetVoyant Discovery Process”](#) on page 49.

### To edit the discovery settings for a device:

1. On the **Group** tab in the NetVoyant Console, browse for and locate the device.
2. In the context panel for the device, select the **Details** tab.

The details for the device appear in the context panel.

3. Scroll down to view the discovery settings for the device.

The screenshot shows a configuration window for a device named 'QARouter-2620-4.QA.local'. The 'Details' tab is active. The 'SNMP Version' is set to 'SNMPv2C', 'SNMP Timeout' is '5', and 'SNMP Retries' is '1'. The 'SNMP Discovery' section has three radio buttons: 'Extended' (unselected), 'Enabled' (selected), and 'Disabled' (unselected). The 'Polling Enabled' dropdown is set to 'Enabled'. The 'Get Profile' and 'Set Profile' dropdowns are both set to 'netqos'. At the bottom are 'Set' and 'Help' buttons.

4. Edit the following parameters:

Parameter	Description
<b>SNMP Version</b>	Use the drop-down list to set the SNMP version to be used to query the device.
<b>SNMP Timeout</b>	Enter a length of time in seconds to configure how sensitive the NetVoyant product is to timeouts when performing SNMP queries to this device. Longer timeouts significantly increase how long it takes to complete the discovery process.
<b>SNMP Retries</b>	Enter the number of times that you want the NetVoyant product to retry the device for each SNMP profile when performing SNMP queries to this device. More retries significantly increase how long it takes to complete the discovery process.
<b>SNMP Discovery</b>	<p>Select one of the following for SNMP Discovery:</p> <ul style="list-style-type: none"> <li>• To set the device to extended discovery, select <b>Extended</b>.</li> <li>• To set the discovery as enabled normally for discovery, select <b>Enabled</b>.</li> <li>• To disable discovery for the device, select <b>Disabled</b>.</li> </ul>

5. Click **Set** to apply your changes.

## Rediscovering Devices and Groups

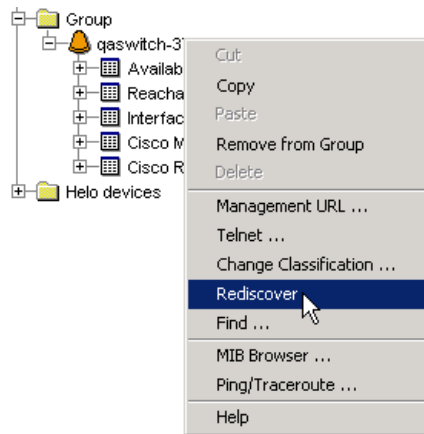
The NetVoyant product performs initial discovery of a device when a full discovery is initiated from the Configuration Wizard or when you add the device using the Device Wizard.

**Note:** For more information about using the Configuration Wizard to perform a discovery of your entire network, see [“Using the Configuration Wizard” on page 33](#).

From then on, the NetVoyant system performs a partial rediscovery nightly (midnight by default) and a periodic full rediscovery (once a week by default) to update device configuration information. It also performs a full rediscovery for a device when it detects a reset (based on `sysUpTime`) or when an IP SLA test is added or removed. You can also manually initiate a full rediscovery of an individual device or group of devices at any time.

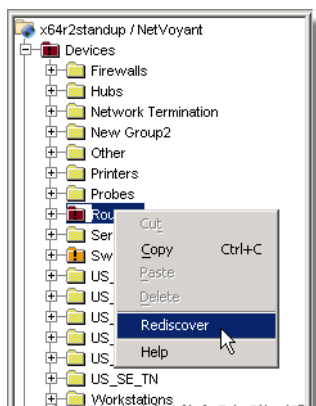
### To initiate a full rediscovery of an individual device:

- In the **Group** tab of the NetVoyant Console, right-click a device and select **Rediscover**.



### To initiate a full rediscovery for a group of devices:

- On the **Group** tab, right-click a group and select **Rediscover**.



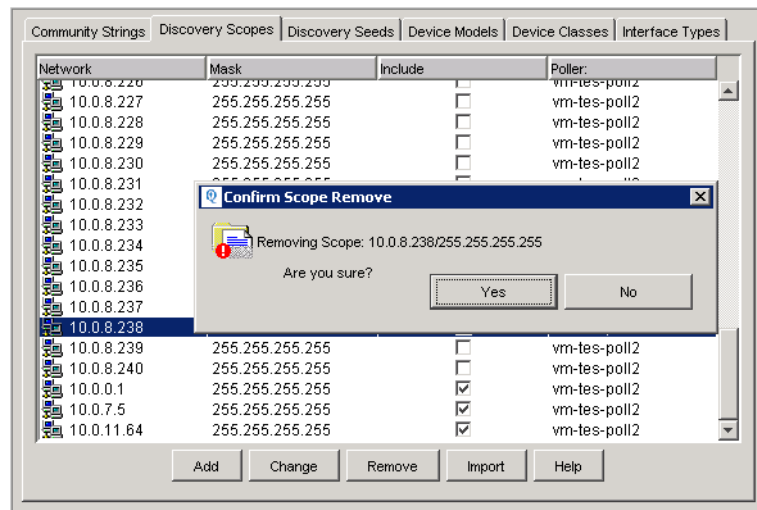


## Removing a Device from the Discovery Scope

If you have removed a device and do not want to discover that device again during the periodic full rediscovery, make sure to remove the device from the discovery scope.

### To remove a device from your discovery scope:

1. On the **Config** tab in the NetVoyant Console, expand the Master console
2. Expand **Discovery** and select **Discovery Scopes**.  
The currently configured discovery scopes appear in the context panel.
3. Select the device in the list.
4. Click **Remove**.



5. Click **Yes** to confirm.

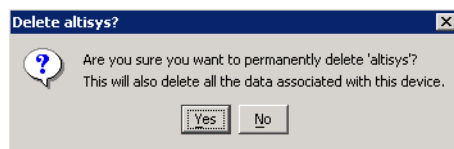
## Deleting a Device

If you want to omit a device from discovery, disable the device from discovery while keeping the device with its definitions and data in the NetVoyant system. If you want to completely remove a device, you can delete it.

**Warning:** Deleting a device deletes the device and all related data from the NetVoyant system.

### To delete a device:

1. On the **Group** tab in the NetVoyant Console, browse for and locate the device.
2. Right-click the device and select **Delete**.
3. Click **Yes** to confirm.



## Using the Find Utility to Locate Devices

The NetVoyant Console includes a Find utility that you can use to quickly locate a particular device name or IP address in the tree-tab panel. This utility displays a list of location path names. Double-click the found item to display the group/device.

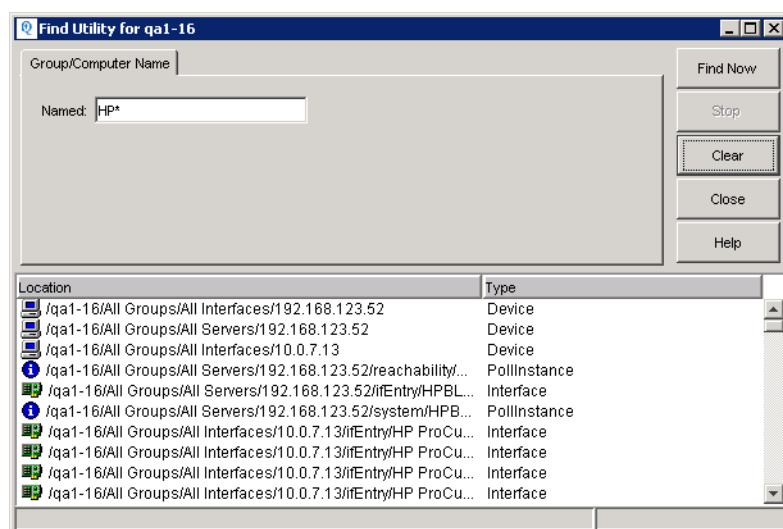
### To locate items by name or IP address:

1. From the **Tools** menu in the NetVoyant Console, choose **Find**.

The **Find Utility** opens.

2. In the **Named** text box, enter the search string.

This field supports wild card values using the \* symbol. For example, a search string HP\* would find a match for any device where the name begins with HP.



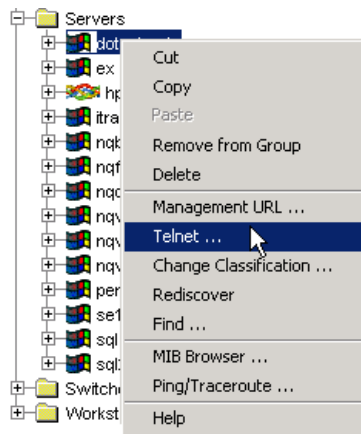
3. Click **Find Now** to search for devices.
4. Double-click an item to locate it and select it with the tree-tab panel in the NetVoyant Console.
5. Click **Clear** to clear the current search string and listed devices before you begin a new search or click **Close** to close the utility.

## Starting a Telnet Session with a Device

Telnet, which is a login and terminal emulation program for Transmission Control Protocol/Internet Protocol (TCP/IP) networks, is a common way to communicate with an individual device. You can start a Telnet session with a device from the NetVoyant Console.

### To start a Telnet session with a device:

1. In the NetVoyant Console in the **Group** tab, expand the tree structure to locate the device.
2. Right-click the device and select **Telnet**.



The NetVoyant product starts a Telnet session with the device.

## Performing a Ping or Traceroute

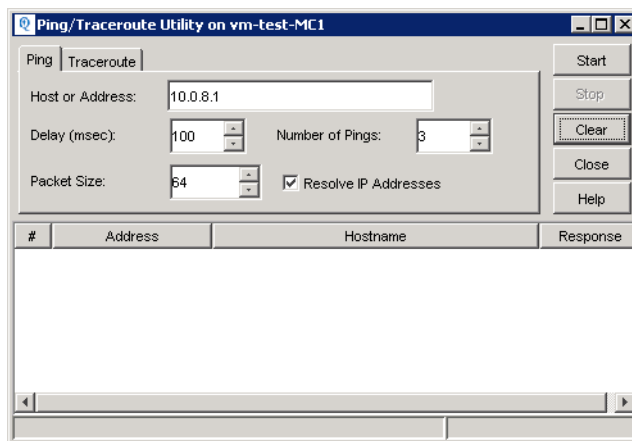
An ICMP (Internet Control Message Protocol) ping is an Internet utility used to determine whether a particular IP address is reachable online by sending out a packet and waiting for a response. An ICMP traceroute is an Internet utility that describes the path that a packet follows in real-time from the client computer to the remote host computer being contacted. A traceroute reports the IP addresses of all the routers in between the source and destination computers.

### To perform an ICMP ping or traceroute on a device:

1. On the **Group** tab in the NetVoyant Console, browse for and locate the device.
2. Right-click the device and select **Ping/Traceroute**.

The Ping/Traceroute Utility opens.

3. Perform one of the following actions:
  - To perform a ping, remain on the **Ping** tab.
  - To perform a traceroute, click the **Traceroute** tab.



4. Enter or edit the following parameters:

Parameter	Description
<b>Host or Address</b>	Enter the hostname or IP address to which you want to ping or perform a traceroute.
<b>Delay</b> ( <i>ping only</i> )	Enter the time between successive pings in milliseconds.
<b>Number of Pings</b> ( <i>ping only</i> )	Enter the number of pings that you want to send.
<b>Packet Size</b> ( <i>ping only</i> )	Enter the size of the ICMP data field that you want to send in the ping.
<b>Timeout</b> ( <i>traceroute only</i> )	Enter the time in milliseconds that you want to wait for a response from each host before considering the request to be failed.
<b>Maximum Hops</b> ( <i>traceroute only</i> )	Enter the maximum number of hops that you want to perform for a traceroute.
<b>Start From Hop</b> ( <i>traceroute only</i> )	Enter the hop number on which you want to begin displaying traceroute information in the response table. The NetVoyant product performs hops prior to the Start From Hop number, but does not display these hops in the response table.
<b>Resolve IP Addresses</b>	Select this check box to configure the NetVoyant product to perform a hostname lookup and enter values in the <b>Hostname</b> field.

5. Click **Start**.

At the bottom of the Ping/Traceroute Utility, the responses appear in the response table with the following fields:

Field	Description
<b>#</b>	The ping or traceroute hop number. This indicates the order in which the ping or traceroute request was sent. If a ping number is repeated, NetVoyant resent the ping because of a slow or timed-out response from the host.
<b>Address</b>	The IP address of the host.

Field	Description
<b>Hostname</b>	The hostname of the host as determined by a hostname lookup. NetVoyant does not enter a value for the Hostname if you do not select the <b>Resolve IP Addresses</b> check box.
<b>Response</b>	The response time for the ping or traceroute hop.

6. You can perform the following actions after performing a ping or traceroute:
  - To cancel the ping or traceroute after you have started it, click **Stop**.
  - To clear the responses in the response table, click **Clear**.
7. When you are finished, click **Close** to close the Ping/Traceroute Utility.

## CONFIGURING PROTOCOL DATA

If your network has an RMON2 probe and you include this device in discovery, the NetVoyant product gathers protocol data from the probe and displays it in Protocol views in the reporting interface. NetVoyant Protocol views also display data collected using Cisco's Network Based Application Recognition (NBAR). For more information about NetVoyant report views, see the *NetVoyant User Guide*.

### Adding an RMON2 Probe

To view Protocol Distribution views, like the ones included in the Protocol Summary (RMON2) report, you must have a Remote Monitoring (RMON2) probe in place in your network that the NetVoyant product can discover with SNMP.

You can add an RMON2 probe to your network by using one of the following methods:

- Add the probe to your discovery scope and initiate rediscovery. For more information, see [“Configuring the Discovery Scopes” on page 40](#).
- Manually add the probe by using the Device Wizard. For more information, see [“Manually Adding Networks and Devices” on page 116](#).





### Viewing Details for an RMON Protocol Distribution

Each poll instance in an RMON Protocol Distribution poll table represents an interface or channel that a Remote Monitoring (RMON2) probe is monitoring.

#### To view details for a protocol distribution:

1. On the **Group** tab in the NetVoyant Console, expand the RMON2 probe to view its poll tables.
2. Expand the **Protocol Distribution** poll table.
3. Select the poll instance.

Details for the poll instance appear in the context panel.

Details		Reports	Alarms	Show All Properties	Customize
 Poll instances represent SNMP rows in a MIB table					
Display Name:	nam2 - ALL SPAN				
Description:	Protocol Distribution on ALL SPAN (ifIndex.2)				
Polling rate:	Fast (5 Mins) 				
Poller:	vm-tes-poll2				
Poll event severity:	None 				
Threshold event severity:	Minor 				
ifSpeed:	2000000000				
PacketOverhead:	20				
<div>Set Help</div>					

4. On the **Details** tab you can view the following information for a poll instance:

Parameter	Description
<b>Display Name</b>	The name of the poll instance.
<b>Description</b>	A description of the poll instance, which is used to reference the poll instance in the NetVoyant Console.
<b>Polling rate</b>	<p>The polling group to which the poll instance belongs.</p> <p>The polling group determines how often the poll instance data is gathered and rolled up.</p> <p>For more information, see <a href="#">“Configuring Polling for Poll Instances and Interfaces” on page 166.</a></p>
<b>Poller</b>	<p>The NetVoyant server that gathers data for the poll instance.</p> <p>In a standalone configuration, the poller is always the Master server. In a distributed configuration, the poller is the NetVoyant server that polls the device to which the poll instance belongs.</p>
<b>Poll event severity</b>	<p>The severity of a missed poll event for the poll instance.</p> <p>You can configure the severity used for missed poll events for a poll instance. For more information, see <a href="#">“Setting the Event Severity for a Poll Instance or Interface” on page 167.</a></p>
<b>Threshold event severity</b>	<p>The severity of a threshold event for the poll instance.</p> <p>If the polled data exceeds the threshold exceeded value for an expression, it triggers a threshold event. You can configure the severity used for threshold events for a poll instance. For more information, see <a href="#">“Setting the Event Severity for a Poll Instance or Interface” on page 167.</a></p>

Parameter	Description
<b>ifSpeed</b>	<p>The speed of an interface as defined by the <code>ifSpeed</code> field in the <code>SNMP ifEntry</code> table.</p> <p>You can configure the speed of an interface by editing the <code>ifSpeed</code> field for the interface. For more information, see <a href="#">“Editing the Interface Speeds”</a> on page 170</p>
<b>PacketOverhead</b>	<p>A variable used to add precision to utilization calculations by capturing the mandatory “down time” in between packets in the physical layer.</p> <p>This is typically a 12 octet interframe gap, a 7 octet “preamble,” and a 1 octet “start frame,” equalling total default value of 20.</p>

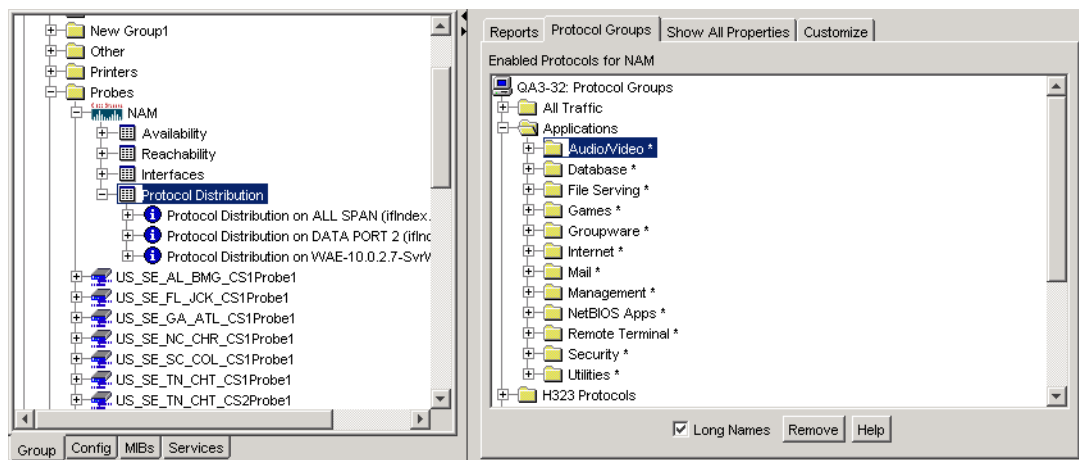
## Editing an Application Group or Protocol Group

In the NetVoyant Console, you can edit the RMON protocol groups used to generate Protocol Distribution views in NetVoyant reports. For example, you can edit what applications are considered IPX applications or even add another application type.

### To access protocol groups for an RMON probe:

1. On the **Group** tab in the NetVoyant Console, expand the RMON2 probe to view its poll tables.
2. Select the **Protocol Distribution** poll table.
3. In the context panel, select the **Protocol Groups** tab.

This tab displays the list of protocol reporting groups. The first level of the tree contains the protocol group types. The second level of the tree contains the protocol groups. The third level displays the protocols (from the Protocol Directory), which are enabled for the protocol group.



**Note:** If the **Protocol Groups** tab does not appear in the context panel, click the **Customize** tab to select the Protocol Groups tab for display.

**To change the name of an application type or protocol group:**

- Double-click the group's name and enter the new name.

**To add a new application type:**

1. Right-click the root directory and select **New Group**.
2. In the **Input** dialog box, enter a name for the application type.
3. Click **OK**.

**To add a new protocol group:**

1. Right-click the application type and select **New Group**.
2. In the **Input** dialog box, enter a name for the group.
3. Click **OK**.

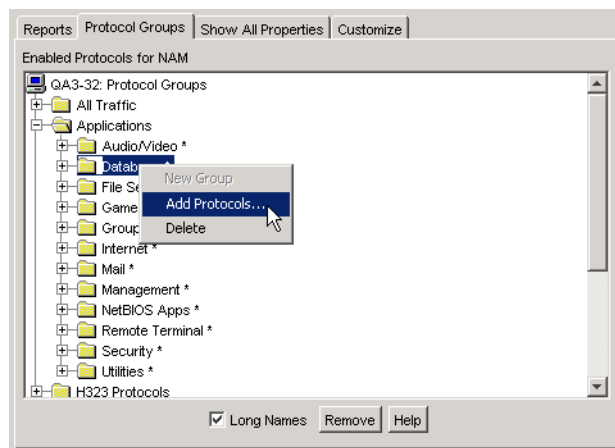
After you create a new protocol group you can add protocols or protocol groups to it.

## Adding or Removing a Protocol from a Protocol Group

In the NetVoyant Console, you can add or remove protocols from RMON protocol groups. For example, you can add a protocol to the Database protocol group in the IPX application group.

**To add or remove a protocol from a Protocol Group:**

1. On the **Group** tab in the NetVoyant Console, expand the RMON2 probe to view its poll tables.
2. Select the **Protocol Distribution** poll table.
3. In the context panel, select the **Protocol Groups** tab.
4. Expand the **Applications** group.
5. Select the protocol group where you want to add or remove a protocol.



6. To add a new protocol, right-click the protocol group and select **Add Protocols**.

The **Add Protocol** dialog box opens and displays all the supported protocols on the selected probe.

7. To remove a protocol, expand the application group structure, select a protocol, and click **Remove**.
8. Click **OK** to add the protocol to the protocol group.

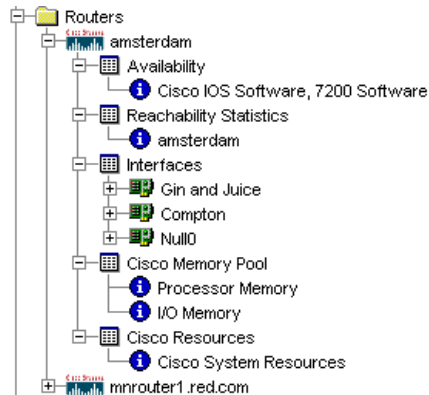


## WORKING WITH POLL INSTANCES AND INTERFACES

Each poll instance represents a row of SNMP data in a MIB table on a device. The NetVoyant product organizes poll instances into poll tables referenced and defined by dataset. If a device supports the MIB table upon which a dataset is based, it creates a poll table for the device in the dataset and places poll instances for that device in the correlated poll table.

**Note:** For more information about poll instances, see “Data Organization by Poll Instance” on page 68.

In the NetVoyant product, an interface is a specific type of poll instance that also represents a physical connection of a device to a network. When you expand a device or network in the **Group** tab of the NetVoyant Console, the poll instances and interfaces are listed under it in the tree.



### Polling Status and Expiration

During discovery, the NetVoyant product uses the discovery scope to poll all eligible devices and determine what poll instances and interfaces are available for data collection and reporting. At this time, it can change the status of a previously discovered poll instance or interface. A poll instance or interface can be in any of the following states:

Status	Description
Enabled	Indicates that the poll instance or interface is currently enabled for polling. For more information about changing the polling status for a poll instance or interface, see <a href="#">Configuring Polling for Poll Instances and Interfaces</a> .
Disabled	This is an initial state during discovery or when polling is disabled on the dataset or polling group. For more information about disabling polling at the dataset or polling group level, see “Editing Dataset Details” on page 71 and “Creating or Editing a Polling Group” on page 94.
Manually Disabled	Indicates that the poll instance or interface polling has been manually disabled. For more information about changing the polling status for a poll instance or interface, see “Configuring Polling for Poll Instances and Interfaces” on page 166.

Status	Description
Auto-Disabled	Indicates that the poll instance or interface or its parent has been disabled by an Auto-enable rule at the dataset level.  For more information about auto-enable rules, see <a href="#">“Using Auto-Enable Polling” on page 88</a> .
Expiring	Each dataset has a setting for poll instance expiration. If the NetVoyant product determines that a poll instance or interface is out-of-scope or unresponsive, its expiration clock will start and elapse according to the number of days indicated in the dataset. When it expires, the poll instance or interface no longer exists for that device.  For example, you might delete an IP SLA test. The poll instance and data for this test is maintained during the expiration (“time-to-live”) period, but deleted when the poll instance is expired.  For more information about setting the poll instance expiration in a dataset, see <a href="#">“Editing Dataset Details” on page 71</a> .
Off-line	Indicates that the poll instance or interface has been manually removed from the automatic expiration schedule, disabling its “time-to-live” removal.  For more information about changing the polling status for a poll instance or interface, see <a href="#">“Configuring Polling for Poll Instances and Interfaces” on page 166</a> .

## Viewing and Editing Poll Instance and Interface Details

When you select a poll instance or interface in the **Group** tab of the NetVoyant Console, the **Details** tab appears in the context panel. This tab provides detailed information about the selected poll instance or interface. Some of these settings can be changed in the **Details** tab.

### To access details for a poll instance or interface:

1. On the **Group** tab in the NetVoyant Console, expand the device or network to view its poll and interface tables.
2. Expand the table and select the poll instance or interface.  
The details appear in the context panel.

3. On the **Details** tab you can view the following details for a poll instance:

Parameter	Description
<b>Display Name/ Name</b>	<p>The name of the poll instance or interface, which is used to reference it in reports.</p> <p>You can dynamically name and apply descriptions to poll instances and interfaces by dataset upon discovery. For more information, see <a href="#">“Naming Poll Instances and Interfaces”</a> on page 78.</p>
<b>Description</b>	<p>A description of the poll instance or interface, which is used to reference it in the NetVoyant Console.</p> <p>You can dynamically name and apply descriptions to poll instances and interfaces by dataset upon discovery. For more information, see <a href="#">“Naming Poll Instances and Interfaces”</a> on page 78.</p>
<b>Polling Status</b>	<p>The polling status for the poll instance or interface.</p> <p>For more information about changing the polling status for a poll instance or interface, see <a href="#">“Configuring Polling for Poll Instances and Interfaces”</a> on page 166.</p>
<b>Polling rate</b>	<p>The polling group to which the poll instance or interface belongs. The polling group determines how often data is gathered and rolled up.</p> <p>For more information, see <a href="#">“Configuring Polling for Poll Instances and Interfaces”</a> on page 166.</p>
<b>Poller</b>	<p>The NetVoyant server that gathers data for the poll instance or interface.</p> <p>In a standalone configuration, this is always the Master server. In a distributed configuration, the Poller is the NetVoyant server that polls the device to which the poll instance or interface belongs.</p>
<b>ifIndex</b>	<p><i>(Interfaces and Frame Relay circuits only)</i> The index for the interface’s SNMP ifEntry table.</p>

Parameter	Description
<b>ifDescr</b>	<i>(Interfaces and Frame Relay circuits only)</i> The description of the interface as defined in the SNMP ifEntry table. You can use ifDescr to dynamically name and apply descriptions to new interfaces or circuits. For more information, see <a href="#">“Naming Poll Instances and Interfaces” on page 78.</a>
<b>ifType</b>	<i>(Interfaces and Frame Relay circuits only)</i> An interface’s type as defined by the ifType field in the SNMP ifEntry table; for example, frame-relay.
<b>ifPhysAddress</b>	<i>(Interfaces and Frame Relay circuits only)</i> The physical address of an interface according to the SNMP ifEntry table.
<b>Addresses</b>	<i>(Interfaces and Frame Relay circuits only)</i> The IP addresses assigned to the interface.
<b>Poll event severity</b>	The severity of a missed poll event for the poll instance or interface. You can configure the severity used for missed poll events for a specific poll instance or interface. For more information, see <a href="#">“Setting the Event Severity for a Poll Instance or Interface” on page 167.</a>
<b>Poll event category</b>	The assigned category for a missed poll event for the poll instance or interface. This information is used to categorize events in the Event Manager when the NetVoyant system is registered with the NetQoS Performance Center as a data source. You can also use the poll event category to filter events when creating notifications. For more information about creating event filters for notifications, see <a href="#">“Writing an Event Filter Expression” on page 241.</a>
<b>ifType</b>	<i>(Interfaces only)</i> An interface’s type as defined by the ifType field in the SNMP ifEntry table.
<b>ifSpeed_in</b>	<i>(Interfaces only)</i> An interface’s inbound speed as defined by the ifSpeed_in field in the SNMP ifEntry table. This setting can be used to calculate utilization for the inbound direction. For more information, see <a href="#">“Editing the Interface Speeds” on page 170.</a>
<b>ifSpeed_out</b>	<i>(Interfaces only)</i> An interface’s outbound speed as defined by the ifSpeed_out field in the SNMP ifEntry table. This setting can be used to calculate utilization for the outbound direction. For more information, see <a href="#">“Editing the Interface Speeds” on page 170.</a>
<b>IP SLA Parameters</b>	<i>(IP SLA only)</i> Provides details about poll instances that are part of IP SLA operations. For more information about poll instances, see <a href="#">“Data Organization by Poll Instance” on page 68.</a>
<b>CirOut</b>	<i>(Frame Relay circuits only)</i> This is a built-in property for Frame Relay circuit poll instances used for the Input Committed Information Rate for the DLCI.
<b>CirIn</b>	<i>(Frame Relay circuits only)</i> This is a built-in property for Frame Relay circuit poll instances used for the Output Committed Information Rate for the DLCI.

Parameter	Description
<b>EirIn</b>	<i>(Frame Relay circuits only)</i> This is a built-in property for Frame Relay circuit poll instances used for the Input Excess Information Rate for the DLCI.
<b>EirOut</b>	<i>(Frame Relay circuits only)</i> This is a built-in property for Frame Relay circuit poll instances used for the Output Excess Information Rate for the DLCI.

## Editing Names and Descriptions for Poll Instances or Interfaces

You can edit the name and description on the **Details** tab for each poll instance or interface. NetVoyant reports display names of poll instances and interfaces and the NetVoyant Console tree-tab panel displays the descriptions.

**Note:** The NetVoyant product enables you to dynamically name and apply descriptions to poll instances and interfaces by dataset upon discovery. For more information, see [“Naming Poll Instances and Interfaces”](#) on page 78.

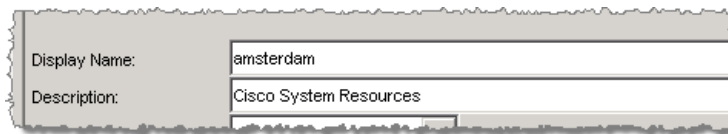
### To edit the name or description of a poll instance or interface:

1. On the **Group** tab in the NetVoyant Console, expand the device to view its poll and interface tables.
2. Expand the table that contains the poll instance or interface.
3. Select the poll instance or interface.

The details appear in the context panel.

4. Edit the following parameters in the **Details** tab:

Parameter	Description
<b>Display Name</b>	Enter the name for the poll instance or interface, which is used to reference it in NetVoyant Console.
<b>Description</b>	Edit the description for the poll instance or interface, which is used to reference it in the NetVoyant reports.



Display Name: amsterdam

Description: Cisco System Resources

5. Click **Set**.

## Configuring Polling for Poll Instances and Interfaces

To configure polling for a specific poll instance, you can apply a different polling group to that poll instance on its **Details** panel. The assigned polling group determines how often the NetVoyant product polls this device for the data in this poll instance.

For example, you can apply a polling group with a polling rate of five minutes to a poll instance for a Jitter IP SLA test on a router. It then polls this router for data relating to this IP SLA test every five minutes.

As another example, if you apply a polling group with a polling rate of five minutes to a Fast Ethernet interface on a router, it polls this router for statistics about this interface every five minutes.

You can also enable or disable polling for the poll instance or interface.

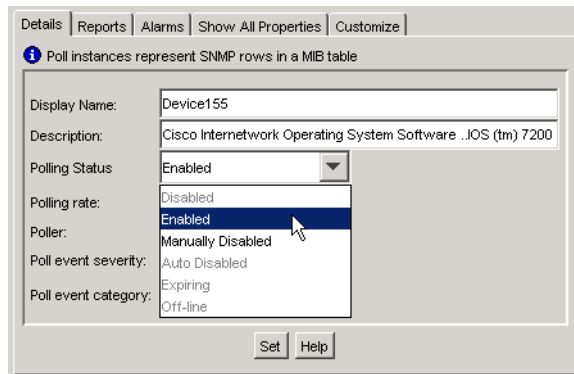
### To configure polling for a poll instance or interface:

1. On the **Group** tab in the NetVoyant Console, expand the device to view its poll and interface tables.
2. Expand the table and select the poll instance or interface.

The poll instance's details appear in the context panel.

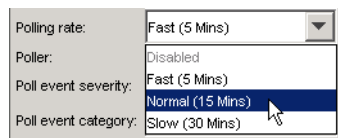
3. Change the **Polling Status** to disable or enable polling.

Select **Enabled** to enable polling, or **Manually Disabled** to disable polling. For information about polling status and expiration of poll instances and interfaces, see [“Polling Status and Expiration” on page 161](#).



4. Change the polling frequency by selecting a polling group from the **Polling rate** list.

This list is populated with the polling groups defined for the dataset.



5. Click **Set**.

**Note:** To hide devices, poll instances, and interfaces that are disabled for polling in the NetVoyant Console, clear the **Show Disabled from Polling** option in the **View** menu.

## Setting the Event Severity for a Poll Instance or Interface

You can configure the severity used for missed poll events and threshold events for poll instances and interfaces. A missed poll event occurs when the NetVoyant product cannot poll a device for a poll instance or on an interface. A threshold event occurs when an expression value for the polled data on a poll instance or interface meets the threshold trigger value within an alarm profile that is applied to the device.

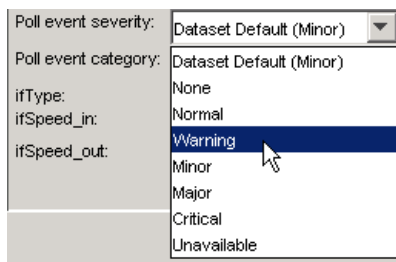
The event severity that you set for these event types determines what type of alarm event is triggered for exceptions on the poll instance or interface.

**Note:** Events can be one of the following event severities: normal, warning, minor, major, or critical. For more information about events and event severities, see [“Configuring Event Severities” on page 224](#).

### To set the event severity level for a poll event on a poll instance:

1. On the **Group** tab in the NetVoyant Console, expand the device to view its poll and interface tables.
2. Expand the table and select the poll instance or interface.  
The details appear in the context panel.
3. Select a severity level from the **Poll event severity** drop-down list.

This determines the severity level for a missed poll event for the poll instance or interface



Poll event severity:	Dataset Default (Minor)
Poll event category:	Dataset Default (Minor)
ifType:	None
ifSpeed_in:	Normal
ifSpeed_out:	Warning
	Minor
	Major
	Critical
	Unavailable

4. Click **Set**.

## Viewing and Acknowledging Alarms

You can view the alarms related to a poll instance or interface on the **Alarms** tab for the poll instance or interface. You can also acknowledge alarms remedied on this tab like you can in the alarm log panel.

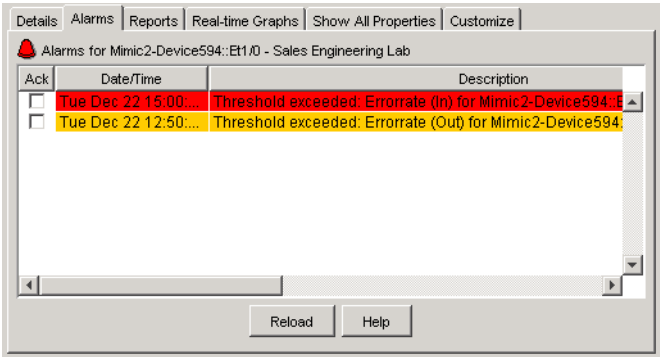
**Note:** For more information about alarms, see [“Using Events and Alarms” on page 190](#).

### To view and acknowledge alarms for a poll instance or interface:

1. On the **Group** tab in the NetVoyant Console, expand the device to view its poll tables.
2. Expand the poll instance or interface table and select the poll instance or interface.
3. Click the **Alarms** tab.

This tab displays a color-coded list of alarms for the selected poll instance or interface. You can configure the colors for alarms from the **Logs** menu.

**Note:** If the **Alarms** tab does not appear in the context panel, click the **Customize** tab to select the Alarms tab for display.



The **Alarms** tab provides the following details for each alarm:

Field	Description
<b>Ack</b>	This check box enables you to acknowledge an alarm that you have already addressed.
<b>Date/Time</b>	The server date and time at which the alarm occurred.
<b>Description</b>	A description of the alarm that occurred.
<b>Source</b>	The service or device that initiated the alarm.
<b>Severity</b>	The severity level of the alarm. Alarms can be one of the following severity levels: Warning, Minor, Major, or Critical. The NetVoyant product labels alarm logs by color according to their severity. It also labels the device and group that was the source of the alarm log in the Group tab of the tree-tab panel.
<b>Type</b>	The type of alarm. Possible alarm types include threshold, polling, and trap.
<b>Category</b>	The event category. Possible categories are Status, Threshold, Configuration, or Performance.
<b>Error code</b>	A code to assist technical support in diagnosing issues.
<b>Server</b>	The server on which the service that initiated the alarm resides. To acknowledge an alarm, select the <b>Ack</b> check box next to the alarm. This clears the alarm.



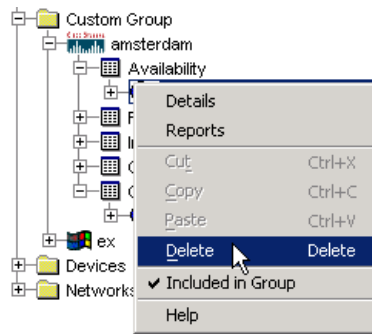
## Deleting All Data for a Poll Instance or Interface

Deleting a poll instance or interface removes all the historical data for it. When the NetVoyant product rediscovers the device, it recreates the poll instance or interface for the device with no existing data.

**Note:** If you do not want to continue to collect data for a poll instance or interface, do not delete it. Instead, disable polling for it. For more information, see [“Configuring Polling for Poll Instances and Interfaces” on page 166](#). If you do not want to include data for a poll instance or interface in a report, exclude it from the group. For more information, see [“Including and Excluding Poll Instance or Interface Data” on page 129](#).

### To delete all data for a poll instance or interface:

1. On the **Group** tab in the NetVoyant Console, right-click the poll instance or interface and select **Delete**.

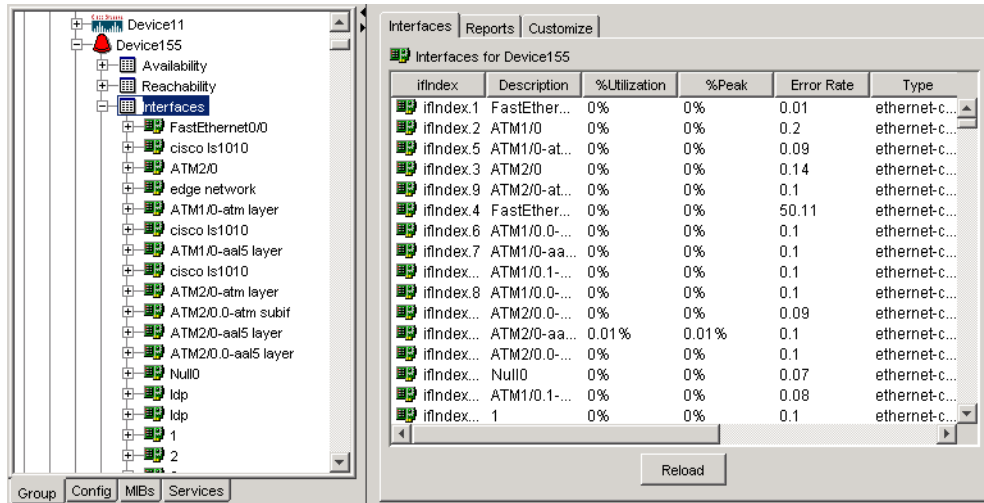


2. Click **Yes** to confirm.

This deletes the poll instance or interface and all related data. If the device is rediscovered, NetVoyant recreates the poll instance or interface for the device, with no existing data.

## Managing Device Interfaces

An interface is a specific type of poll instance that also represents a physical connection of a device to a network. When you expand a device in the **Group** tab, select the **Interfaces** poll table to view the interfaces discovered for the device and the parameters for each interface.



Because interfaces represent a physical connection, there are additional settings to use for managing data collection and alarming for interfaces.

### Editing the Interface Speeds

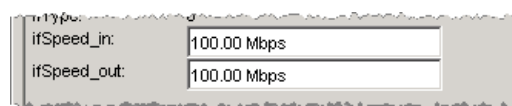
The NetVoyant product automatically discovers and sets the interface speed when it discovers an interface; however, you can edit the overall interface speed, as well as the inbound and outbound speeds, in the NetVoyant Console. These speed values are used in NetVoyant calculations and are included in many interface reports.

**Note:** The `ifSpeed` property is reported to the NetQoS Performance Center when the NetVoyant system is registered as a data source. The `ifSpeed_in` and `ifSpeed_out` values are used in the `ifstat` expressions for calculating utilization. Use different inbound and outbound values to support interfaces such as ADSL, which have different inbound and outbound speeds.

#### To edit the interface speed for an interface:

1. On the **Groups** tab in the NetVoyant Console, expand the device to view its poll tables.
2. Expand the **Interfaces** poll table and select the interface.  
The interface's details appear in the context panel.
3. Enter the updated **ifSpeed\_in** or **ifSpeed\_out**.

**Note:** If you want to use differing speeds for inbound and outbound traffic on the interface, set the **ifSpeed\_in** and **ifSpeed\_out** values accordingly.



If you do not enter a unit for the speed, the default unit of bps (bits per second) is used. The NetVoyant product recognizes the following units for interface speed:

Unit	Description
bps	Bits per second.
Kbps	Kilobits per second. Thousand bits per second.
Mbps	Megabits per second. Million bits per second.
Gbps	Gigabits per second. Billion bits per second.
Tbps	Trillion bits per second.
Pbps	Quadrillion bits per second.
Qbps	Quintillion bits per second.
Zbps	Sextillion bits per second.
Ybps	Septillion bits per second.

Although several of these units seem high, a device might have erroneously entered an exaggerated interface speed. If this is the case, these units can be used for interface speed.

4. Click **Set**.

The NetVoyant product uses the new value(s) in its calculations.

## Resetting an Interface Speed

After you edit an interface's speed, if you want to reset the interface speed according to the device's interface statistics table (`ifstats`), you must reset the property's system mode to Normal so that the property can be modified. For more information, see [“Adding, Viewing, or Setting Values for Properties”](#) on page 316.

**Note:** If you have not edited the interface speed property, you cannot and do not need to reset the system mode.

### To reset an interface's speed to normal system mode:

1. On the **Groups** tab in the NetVoyant Console, expand the device to view its poll tables.
2. Expand the **Interfaces** poll table and select the interface.

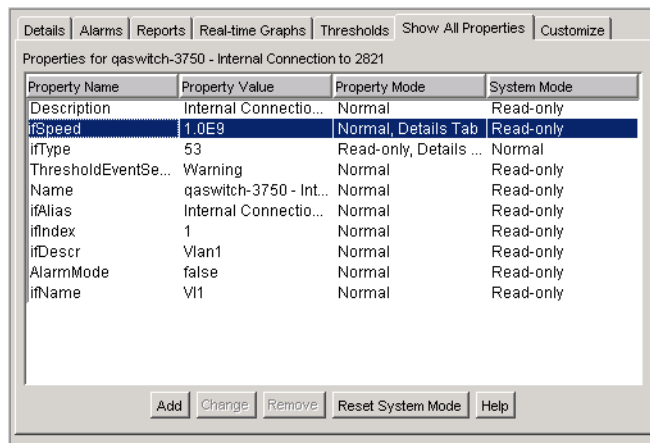
The interface's details appear in the context panel.

3. Click the **Show All Properties** tab.

This tab shows existing properties for the interface.

**Note:** If the **Show All Properties** tab does not appear in the context panel, click the **Customize** tab and select the Show All Properties tab for display.

4. Select the **ifSpeed** property.



5. Click **Reset System Mode** to set the property's system mode to Normal.

## Viewing a Real-Time Graph for an Interface

To troubleshoot an interface in the NetVoyant Console, display real-time graphs for selected expressions on the interface's **Real-time Graphs** tab.

**Note:** You can also view the following real-time graphs for MIB values. For more information, see “Viewing Real-Time Graphs for a Device” on page 143 and “Performing an SNMP Query on a Device” on page 145.

### To view a real-time graph for an interface:

1. On the **Group** tab in the NetVoyant Console, expand the device to view its poll tables.
2. Expand the **Interfaces** poll table, and select the interface.
3. Click the **Real-time Graphs** tab.

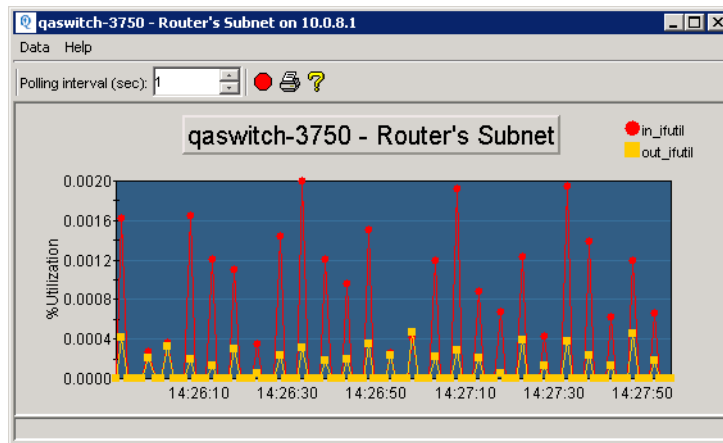
**Note:** If the Real-time Graphs tab does not appear in the context panel, click the **Customize** tab to display the Real-time Graphs tab.

4. Select one of the following real-time graphs:

Graph	Description
In vs Out Utilization	Plots the interface's incoming utilization ( <code>in_ifutil</code> ) and outgoing utilization ( <code>out_ifutil</code> ) as a percent of total bandwidth.
In vs Out Volume	Plots the interface's incoming and outgoing volume as octets per second.
Errors	Plots the interface's errors for incoming and outgoing traffic.
Discards	Plots the interface's discards for incoming and outgoing traffic.
Unknown Protocols	Plots packets that have been discarded on the interface because the packets are a protocol that is unknown to the device.

5. Click **Display**.

This displays the selected real-time graph for the interface.



**Note:** If no data appears in a real-time graph after a few seconds, see “[Troubleshooting a Real-time Graph](#)” on page 144 for possible solutions.

6. (Optional) To configure the frequency for adding plot points to the graph, edit the **Polling interval**. You can lower the polling interval to as low as one second for a real-time graph.
7. (Optional) To print the graph, click the printer icon.

**Note:** This requires that the NetVoyant server on which you are accessing the NetVoyant console has a printer installed.

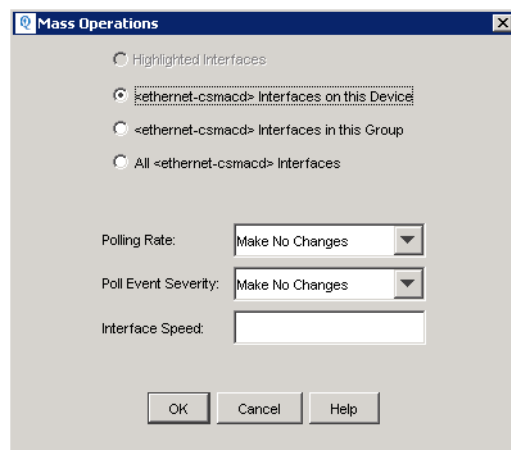
## Performing Mass Operations by Interface Type

To configure large groups of interfaces at one time, you can use the Mass Operation tool to configure interfaces by interface type (IFType). The tool enables you to make configuration changes to all interfaces of a selected type in your entire network, in a group, or on an individual device.

For example, if you apply a polling group with a polling rate of five minutes to all Gigabit Ethernet interfaces in the Routers group, the NetVoyant product polls Gigabit Ethernet interfaces on all routers in the Routers group for interface statistics every five minutes.

### To perform a mass operation by interface type:

1. On the **Groups** tab in the NetVoyant Console, expand the device to view its poll tables.
2. Expand the **Interfaces** poll table and select the interface.  
The interface’s details appear in the context panel.
3. Right-click the interface and select **Mass Configure (by IFType)**.  
The **Mass Operations** dialog box opens.



4. Select one of the following operation options:

Option	Description
<b>Interfaces on this Device</b>	Applies the configuration changes to interfaces of the selected type on the same device as the selected interface
<b>Interfaces in this Group</b>	Applies the configuration changes to interfaces of the selected type in the same group as the selected interface.
<b>All Interfaces</b>	In a distributed configuration, this applies the configuration changes to interfaces of the selected type on the same poller as the selected interface. In a standalone configuration, this applies the configuration changes to interfaces of the selected type.

5. Configure the interfaces using the following parameters:

Parameter	Description
<b>Polling Rate</b>	<ul style="list-style-type: none"> <li>To disable polling for the selected interfaces, select Disable.</li> <li>To set the polling rate for the selected interfaces, select a polling group from the list.</li> </ul> <p>This list is populated with the polling groups defined for the Interface Statistics dataset. For more information, see <a href="#">“Configuring Polling for Poll Instances and Interfaces”</a> on page 166.</p>

Parameter	Description
<b>Poll Event Severity</b>	<p>Select the severity of a missed poll event for the interfaces.</p> <p>A missed poll event occurs when the NetVoyant product cannot poll the interface.</p> <p>The severity level that you set determines what type of alarm events are triggered for missed polls on the selected interfaces.</p> <p>Events can be one of the following severity levels: normal, warning, minor, major, critical, or a custom severity level. For more information, see <a href="#">“Setting the Event Severity for a Poll Instance or Interface” on page 167</a>.</p>
<b>Interface Speed</b>	<p>Enter an interface speed including a unit.</p> <p>If you do not enter a unit for the speed, the default unit of bps (bits per second) is used.</p> <p>The NetVoyant product automatically discovers and sets the interface speed when it discovers an interface; however, you can edit the interface speed (<code>ifSpeed</code>) for your interfaces. This speed is used in NetVoyant calculations and is included in reports. For more information, see <a href="#">“Editing the Interface Speeds” on page 170</a>.</p>

6. Click **OK**.

The NetVoyant product applies the configuration changes to the selected interfaces.





# Working with Management Information Bases

---

A Management Information Base (MIB) is a file that describes types of data that SNMP pollers (like the NetVoyant product) can gather from a device using SNMP. A MIB contains *objects* (units of management information) divided into *scalars* and *tables*, which are identified by object identifiers (OIDs). The NetVoyant product recognizes many MIBs at installation.

**Note:** MIB management tasks take place in the NetVoyant Console on the **MIBs** tab and in the MIB Browser.

This chapter covers the following topics:

- “Using MIBs for Data Collection” on page 178
- “Using the MIB Browser” on page 182
- “Adding MIBs to the NetVoyant Product” on page 185

## USING MIBs FOR DATA COLLECTION

A Management Information Base (MIB) is an SNMP structure that describes a type of data that an SNMP agent can monitor using SNMP. The NetVoyant product uses MIBs to determine what type of data it can collect from your devices.

An SNMP-enabled device supports a selection of MIBs, and this selection is determined by how the device manufacturer has implemented SNMP support on the device. In the NetVoyant Console, you can view the MIBs that a selected device supports using the MIB browser. For more information, see [“Opening the MIB Browser” on page 182](#).

### MIB Structure

An SNMP MIB defines a tree structure, in which each node is assigned a unique name and object identifier. Managed objects or data variables occur at the leaf nodes of the tree. The following example is from RFC1213. The nodes represented in *italics* correspond to actual data items.

```
iso(1)
  org(3)
    dod(6)
      internet(1)
        directory(1)
          mgmt(2)
            |   mib-2(1)
            |     system(1)
            |       |   sysDescr(1)
            |       |   sysObjectID(2)
            |       |   sysUpTime(3)
            |       |   sysContact(4)
            |       |   sysName(5)
            |       |   sysLocation(6)
            |       |   sysServices(7)
            |       |   interfaces(2)
            |       |     |   ifNumber(1)
            |       |     |   ifTable(2)
            |       |     |     |   ifEntry(1)
            |       |     |     |     |   ifIndex(1)
            |       |     |     |     |   ifDescr(2)
            |       |     |     |     |   ifType(3)
            |       |     |     |     |   ifMtu(4)
            |       |     |     |     |   ...
            |       |     |     |     |   ...
            |       |     |     |     |   experimental(3)
            |       |     |     |     |   private(4)
```

...

The node `ifNumber` is an example of a scalar value. While it is not apparent from this representation, the nodes under `ifEntry` actually represent a table structure within the MIB. Each of the child nodes of `ifEntry` define a column of the table.

## MIB Object Identifiers

A MIB uses object identifiers (OIDs) to label each type of data that it describes. An OID is a permanent, unique name assigned to a type of data for storage (persistence). A MIB file defines:

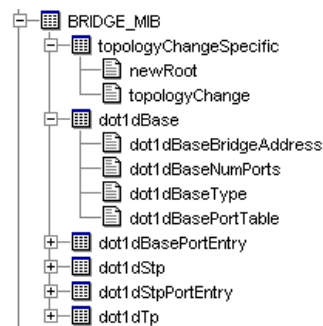
- The types of data and their OIDs.
- The tables where SNMP agents should store data.

When a device gathers data, it stores it in associated MIB tables as data labeled with the appropriate OIDs. SNMP pollers (like the NetVoyant product) use the OID to search for, gather, and sort data from many devices.

For example, the Host Resources MIB defines a type of data with the `hrStorageSize` OID, which stores the storage size of a host resource. If a server supports the Host Resources MIB, it stores the size of each of its resources labeled with the OID `hrStorageSize`. The NetVoyant product can poll this device for data labeled as `hrStorageSize` and compare this data with other devices that support this MIB.

## Viewing MIBs in the NetVoyant Console

You can view all MIBs currently added to the NetVoyant system on the **MIBs** tab in the NetVoyant Console. The tree structure that appears in the tab lists MIB modules, which are collections of managed objects and trap definitions that describe an SNMP-manageable entity. Each module contains one or more tables. On the **MIBs** tab, you can also view the details of a selected MIB table or an OID.



## Viewing the Details of a MIB Table

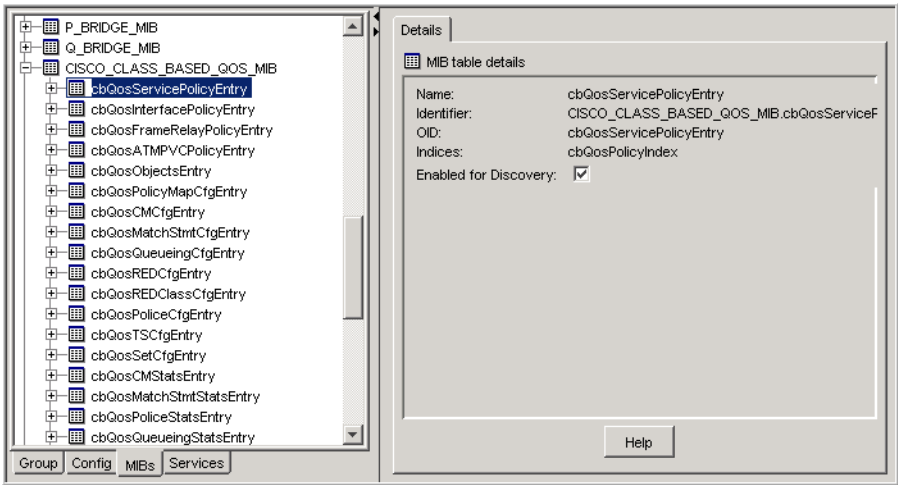
Each dataset in the NetVoyant product is based on a table defined in a MIB. By browsing the definitions in the MIB, you can view information about how each MIB table is defined. You can also view details about how a selected table is defined in a MIB on the **MIBs** tab in the NetVoyant Console.

SNMP agents residing on your devices store SNMP data in MIB tables. The NetVoyant product creates poll tables to store SNMP data from MIB tables.

To view the details of a MIB table:

- 1. In the NetVoyant Console (Master or standalone), select the **MIBs** tab.
- 2. Expand the Master server item.  
All recognized MIBs appear.
- 3. Browse for and expand the MIB module in which the table is defined.
- 4. Select the MIB table.

This displays the details for the MIB table in the context panel.



This panel displays the following details:

Parameter	Description
Name	The name of the MIB table.
Identifier	The text identifier for the table in the form: <code>MIB.TableName</code> where MIB is the name of the MIB and TableName is the name of the table.
OID	The object identifier for the table.
Indices	The OID that is used as an index to the table.
Enabled for Discovery	Indicates whether the NetVoyant system discovers the MIB table on those devices that support the MIB. If the table is tied to a dataset, this check box is selected. If the table is not tied to an existing dataset, this check box is not selected.

## Viewing the Details of an OID

A MIB uses OIDs to label each type of data that it describes. An OID is a permanent, unique name assigned to an object for storage (persistence).

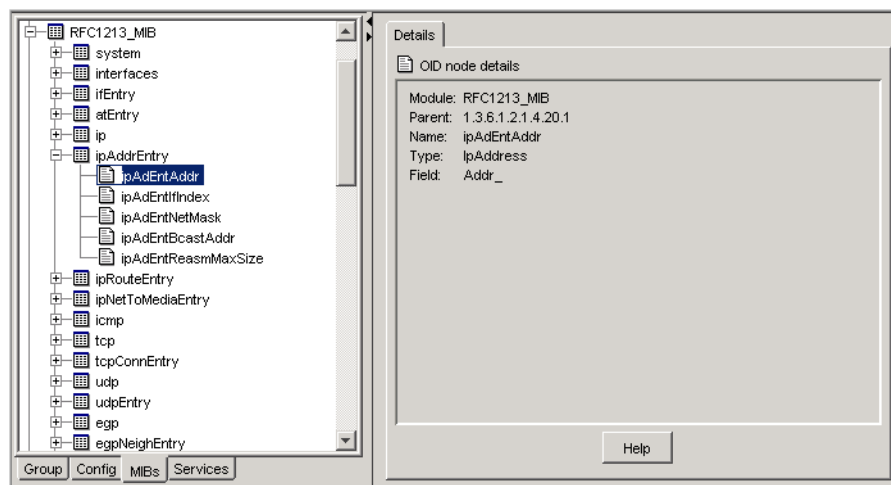
When a device gathers SNMP data, it stores its data in its associated MIBs using fields labeled with the appropriate OIDs. The NetVoyant product uses the OID to search for, gather, and sort data from many devices.

By browsing the definitions in a MIB, you can view information about how each OID is defined. You can also view details about how a selected OID is defined in a MIB on the **MIBs** tab in the NetVoyant Console.

### To view the details of an OID:

1. In the NetVoyant Console (Master or standalone), select the **MIBs** tab.
2. Expand the Master server.  
All recognized MIBs are listed.
3. Browse for and expand the MIB and table in which the OID is defined.  
The OIDs stored in the MIB table are listed.
4. Select the OID.

This displays the details of the OID in the context panel.



This tab displays the following details:

Parameter	Description
<b>Module</b>	The MIB in which the OID is defined.
<b>Parent</b>	The object identifier of the parent object, which is either the MIB or the MIB table.
<b>Name</b>	The name of the OID.
<b>Type</b>	The type of data that the field holds.
<b>Field</b>	The name that the NetVoyant product gives to the field in the objects table associated with the OID.

# USING THE MIB BROWSER

Use the MIB Browser to browse the SNMP MIBs currently recognized by your NetVoyant system. In this tool you can select MIB tables and OIDs to be queried or graphed.

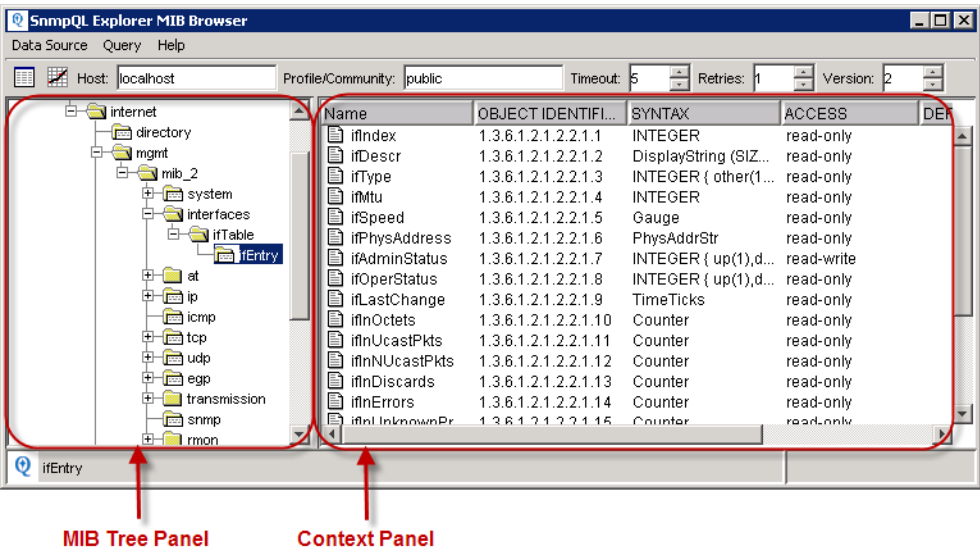
## Opening the MIB Browser

Perform one of the following to open the MIB Browser from the NetVoyant Console:

- On the **Groups** tab, right-click a device and select **MIB Browser**.  
The MIB Browser opens, displays only those recognized MIBs that are supported by the SNMP agent on the selected device.
- From the **Tools** menu, select **MIB Browser**.  
The MIB Browser displays all MIBs that are recognized by the NetVoyant product.

The main portion of the MIB Browser is organized into two panels:

Panel	Description
MIB tree panel	Displays a hierarchical view of all MIBs and MIB tables. Select a MIB to view the tables that it contains in the context panel. Select a MIB table to view the OIDs that it contains in the context panel.
Context panel	Displays information about the tables or OID in the MIB or MIB table selected in the MIB tree panel.



The following parameters are defined in the MIB Browser context panel:

Parameter	Description
Name	The name of the table or OID.
Object Identifier	The object identifier number for the table or OID.

Parameter	Description
<b>Syntax</b>	The type of data stored in an OID. For a table or identifier OID, this is OBJECT IDENTIFIER.
<b>Access</b>	How the field is configured by the MIB to be accessed.
<b>Defval</b>	The default value of the field if it exists. The SNMP agent populates a field with the default value when the device is restarted or when a new row is created in the MIB table and a value for the field is not specified.
<b>Description</b>	A textual description of the type of data that is stored in an OID.

## Configuring What the MIB Browser Displays

In the toolbar at the top of the MIB Browser are several options that customize how data appears in the MIB Browser.



The following options are available:

Option	Description
<b>Host</b>	<p>The device queried for SNMP information that appears in the MIB Browser. This information is automatically entered depending upon how you launch the MIB browser, or you can enter it manually:</p> <p>Enter a device name or IP address to query the device for its supported MIBs. If a table is not supported by the device, there will be no data displayed for the query.</p> <p>If the SNMP agent is running on a UDP port other than the SNMP default of 161, enter the host using the following syntax:</p> <p style="text-align: center;">&lt;host&gt;:&lt;port number&gt;</p> <p>For example:</p> <p style="text-align: center;">192.168.0.80:3000</p>
<b>Profile/Community</b>	<p>The SNMP profile used to query the host. For SNMPv1/v2, you can simply specify a community string instead of a defined profile.</p> <p>For more information about SNMP profiles and how the NetVoyant product uses them to access devices on your network, see <a href="#">“Defining SNMP Profiles” on page 35</a>.</p>
<b>Timeout</b>	The length of time in seconds to wait for a reply to an SNMP query from the host before considering the query to have failed.
<b>Retries</b>	The number of attempts made to a host for failed SNMP queries.
<b>Version</b>	The SNMP version used to query the host.

## Performing an SNMP Query in the MIB Browser

Perform an SNMP query for a MIB to determine the OIDs contained within the MIB and the type of data available. This is also a good way to test a custom MIB after you have loaded and compiled it into the NetVoyant product.

### To perform an SNMP query for the selected MIB table or OID:

- Click the query button (  ) on the toolbar.

For more information, see [“Performing an SNMP Query on a Device”](#) on page 145.

If no data appears in a query after a couple seconds, then one of the following might be true:

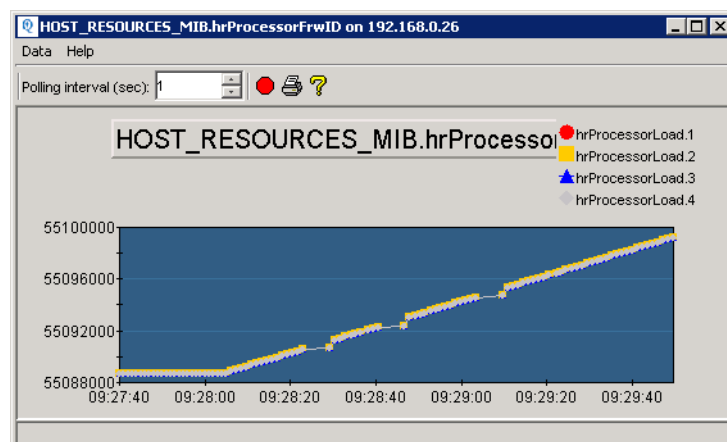
Problem	Solution
The device does not support the selected MIB.	Check your device vendor’s documentation for more information on which MIBs the device supports.
The device is not configured for SNMP or is not SNMP capable.	Check your device vendor’s documentation for more information on SNMP support.
The device is not available to the NetVoyant product.	Check network connectivity for the NetVoyant Master Console and the device.

## Viewing a Real-Time Graph

The real-time graphing feature available in the MIB Browser provides a graphical view of the data for the selected MIB or OID as it is processed for the device. Real-time graphs are useful troubleshooting tools that you can use to view poll processes on a specific device.

### To view a real-time graph of data in a selected MIB table or OID:

- Click the graph button (  ) on the toolbar.



For more information, see [“Viewing Real-Time Graphs for a Device”](#) on page 143.



## ADDING MIBs TO THE NETVOYANT PRODUCT

As manufacturers continue to produce new device models, new MIBs are created. In addition to the numerous standard MIBs that install with the NetVoyant product, administrators can compile new MIBs and build datasets to poll devices that support those MIBs. This allows it to poll any device that supports the compiled MIB.

For the NetVoyant system to poll and transform data from a MIB that is currently not configured, three main steps must be performed:

- The MIB must be compiled - this provides the definition of the MIB, where to find particular pieces of data, what data-type the data uses, and so on.
- At least one dataset must be created - the datasets actually tell NetVoyant what to poll, how to mathematically or logically transform the data, and also contain other configuration information about the polling of the MIB.
- At least one view must be created - the views are the graphs and tables that display the data in the web reporting tool. Without a view that uses a dataset based on the compiled MIB, NetVoyant will collect the data but there will be no way of displaying it. For more information about adding a custom NetVoyant view, see the *NetVoyant User Guide*.

Private MIBs can usually be obtained from the manufacturer, downloadable from their Website. To add a new MIB, you must have the MIB file stored in a location that makes it available from the NetVoyant Console.

**Note:** In a distributed NetVoyant system, you must add MIB files on the Master server and these changes are synched to the pollers.

### Determining MIB Dependencies

In order for the NetVoyant product to utilize an OID, every element to which it refers must be specifically called out and identified in that MIB or reside within another MIB that already resides in the NetVoyant system. When you compile a MIB file in the NetVoyant product, you must supply not only the OIDs defined by the device manufacturer, but also any OIDs for public entities (such as `iso`, `org`, `dod`, `internet`, and so on) that are required by OIDs within the MIB.

Before adding a new MIB to the NetVoyant product, you can preview the contents of the MIB to determine whether it has dependencies. MIBs upon which another MIB is dependent must be compiled into the NetVoyant product before compiling the dependent MIB.

#### To determine the MIBs upon which a MIB is dependent:

1. Open the MIB file using a text editor, such as Notepad.
2. Browse the beginning of the MIB for the `IMPORTS` section.

The `IMPORTS` section of a MIB lists the variables that the MIB imports from other MIBs. These other MIBs are the dependencies of the MIB.

```

CISCO-NETFLOW-MIB.my
--
-- CISCO-NETFLOW-MIB.my
--
-- January 2004, Nitish Kundu and Paul Aitken.
--
-- Copyright (c) 2004, 2005 by Cisco Systems, Inc.
-- All rights reserved.
--
--
CISCO-NETFLOW-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Counter32,
    Unsigned32,
    Integer32,
    Gauge32,
    Counter64
        FROM SNMPv2-SMI
    InetAddressType,
    InetAddress,
    InetAddressPrefixLength,
    InetPortNumber,
    InetAutonomousSystemNumber
        FROM INET-ADDRESS-MIB
    RowStatus,
    TruthValue,
    Timestamp,
    DisplayString,
    TEXTUAL-CONVENTION
        FROM SNMPv2-TC
    MODULE-COMPLIANCE,
    OBJECT-GROUP
        FROM SNMPv2-CONF

```

3. View each MIB dependency, which is listed after FROM.

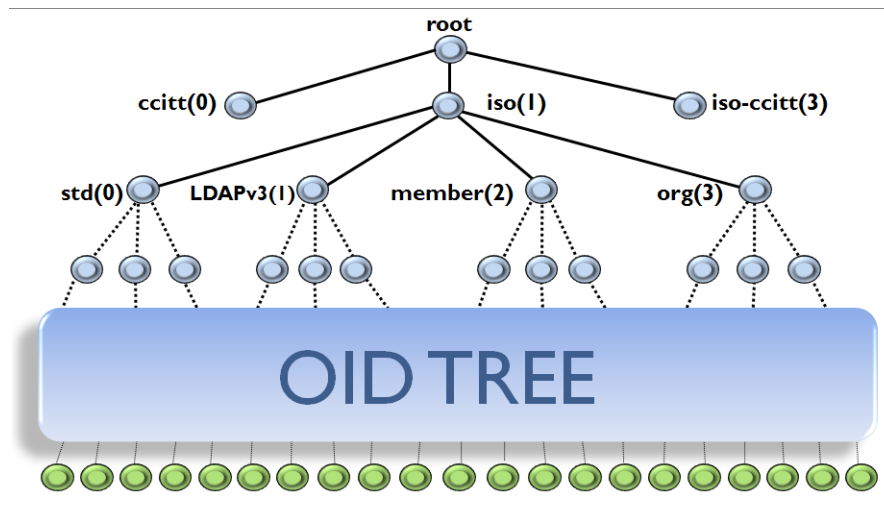
In the preceding figure, the `InetAddress` variable is imported from the SNMPv2-SMI MIB. The SNMPv2-SMI MIB is a dependency of this MIB.

### Inspecting the OIDs

At the beginning of the MIB file is an `IMPORTS` line, which calls out the terms used in the MIB and the RFC MIB that defines those terms.

The upper levels of the OID tree define the general OID structure using a series of standard reference MIB files called *RFCs* (Request for Comment).

An RFC MIB defines a basic dictionary of terms that manufacturers use to write their own equipment-specific MIBs. By utilizing these standard building blocks, a private MIB (created by the manufacturer) does not need to define the entire OID tree; it only has to define the unique OIDs that describe the manufacturer's device.



## Compiling New MIBs into the NetVoyant Product

Before adding a MIB to the NetVoyant product, preview the contents of the MIB to determine whether it has dependencies. MIBs upon which another MIB is dependent must be compiled into the NetVoyant product before compiling the MIB. For more information, see [“Determining MIB Dependencies”](#) on page 185.

**Note:** In a distributed NetVoyant system, you must add and compile MIB files on the Master server and these changes are automatically synched to the pollers.

### To compile a new MIB into NetVoyant:

1. From the **File** menu in the NetVoyant Console, select **New > MIB**.

The MIB Compiler opens.

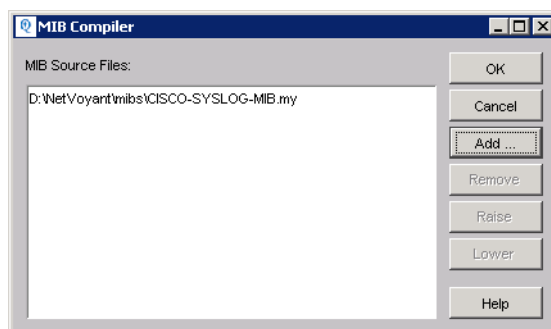
2. Click **Add** to add a new MIB.

The **Add MIB File** dialog box opens.

3. Browse for and select the MIB file.

4. Click **Add**.

This adds the MIB to the list of MIB Source Files.



5. Repeat steps 2 through 4 for each MIB that you want to add to the NetVoyant system.

6. Click **OK**.

The NetVoyant product compiles the MIB. You can verify the addition of the MIB by locating the MIB on the **MIBs** tab.

### Creating a Custom Dataset

To begin gathering data defined in a MIB after you add it, you must create a custom dataset based on a MIB table from which you want to gather data. You can create a new dataset using the Dataset Wizard. For more information, see [“Creating and Configuring Custom Datasets”](#) on page 80.

# Managing NetVoyant Events and Alarms

---

Events are actions, changes, or other occurrences that the NetVoyant product tracks using event logs. Each event has an event severity assigned to it, which is one of the following: normal, warning, minor, major, critical or a custom severity level.

Alarms are events that have an elevated event severity (not normal), which includes warning, minor, major, and critical, as well as unavailable, which indicates a polling failure.

You can use the NetVoyant Console to configure the triggering and automated clearing of threshold event alarms. All alarms can be viewed and managed directly in the NetVoyant Console using the Alarm Log or in the Event Manager when your NetVoyant system is registered as a data source in the NetQoS Performance Center.

This chapter covers the following topics:

- [“Using Events and Alarms” on page 190](#)
- [“Working with Event and Alarm Logs” on page 209](#)
- [“Configuring Event Severities” on page 224](#)

## USING EVENTS AND ALARMS

Events are actions, changes, or other occurrences that the NetVoyant product tracks using event logs. This includes the following types of events:

- **Log events** - Result from the actions that it performs or changes in your network that it detects. Log events track actions that NetVoyant services perform along with topology changes in your network or devices.  
You can configure the logging level of the NetVoyant services. For more information, see [“Configuring a Service’s Start Mode or Logging Level”](#) on page 283.
- **Polling events** - Result from the SNMP polls performed by the NetVoyant product. Polling events track the SNMP polls sent to your devices.
- **Trap events** - Result from incoming SNMP traps. Trap events track incoming SNMP traps.  
You can configure new trap events for the types of SNMP traps that you expect the NetVoyant product to receive. For more information, see [“Adding or Editing an SNMP Trap Event”](#) on page 325.
- **Threshold events** - Result from threshold violations. Threshold events track threshold violations on your devices. A threshold event occurs when a value for an expression goes beyond a threshold limitation value that you set for the alarm rule. You can configure threshold events by specifying threshold triggered and cleared values in an alarm rule. For more information, see [“Defining Thresholds for Alarm Rules”](#) on page 201.

### Event and Alarm Tasks

You can perform the following actions to configure how the NetVoyant product identifies and responds to events and alarms:

Task	More information
Manage event and alarm logs.	<a href="#">“Working with Event and Alarm Logs”</a> on page 209
Create alarm profiles	<a href="#">“Creating a New Alarm Profile”</a> on page 195
Specify alarm rules and threshold event severity.	<a href="#">“Defining an Alarm Rule”</a> on page 199
Set or edit the thresholds for alarm rules.	<a href="#">“Using Thresholds to Trigger Events”</a> on page 204
Configure the event severity applied to events for a selected poll instance.	<a href="#">“Setting the Event Severity for a Poll Instance or Interface”</a> on page 167
Configure the event severity applied to events for a selected interface.	<a href="#">“Setting the Event Severity for a Poll Instance or Interface”</a> on page 167
Configure event severities to facilitate notifications and reporting.	<a href="#">“Configuring Event Severities”</a> on page 224
Add or edit the SNMP trap events defined in the NetVoyant product.	<a href="#">“Adding or Editing an SNMP Trap Event”</a> on page 325

**Task****More information**

Create notifications to alert you and your team about selected events and alarms.

[“Creating a Notification” on page 227](#)

Configure the logging performed by NetVoyant services.

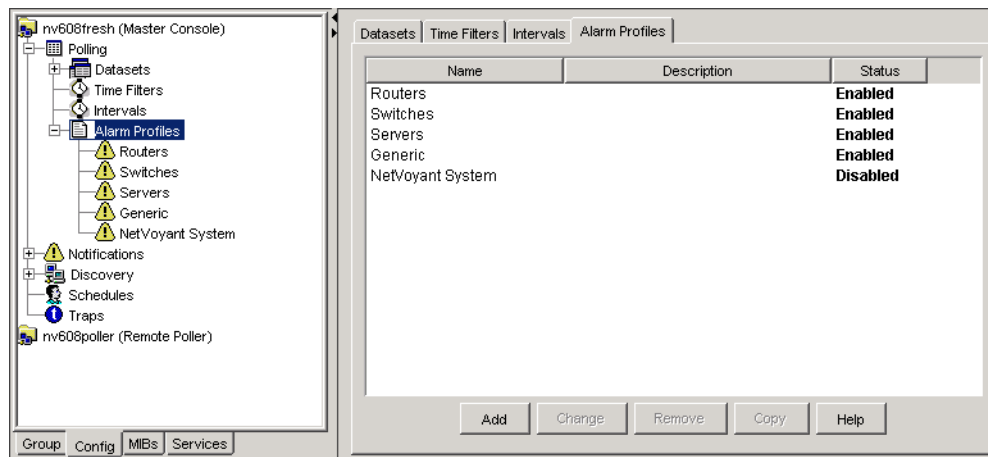
[“Configuring a Service’s Start Mode or Logging Level” on page 283](#)

## Using Alarm Profiles

An alarm profile is a set of rules that define when a polling event generates an alarm. A profile is assigned to a group of devices so that when polling events and their resulting data for any device within the group meets any of the conditions, an alarm is generated.

Using alarm profiles is a convenient way to group alarm rules into a functional set for a specific purpose. For example, an alarm profile named “Phoenix Servers” would consist of alarm rules for disk space, processor usage, and device availability with thresholds set specifically for an operational region within the wider network.

You can access the alarm profiles in the **Config** tab in the NetVoyant Console, in the **Polling** item of the tree.



**Note:** In a distributed system, alarm profiles are defined and applied only on the Master server. You cannot add alarm profiles or change the alarm rules for an alarm profile on a poller. However, in the event that the Master server is down, you can restart the services on the poller and then add or modify alarm profiles locally. This provides a backup in the case that the Master server is down for an extended period of time. But be aware that when the Master server returns to service, it overwrites the rules configured locally on the poller.

## Default Alarm Profiles

The NetVoyant Console includes five pre-configured alarm profiles by default. These profiles contain standard rules typically used for alarm generation by device class and are assigned to the default NetVoyant groups. These profiles can be modified or deleted; however, it is recommended that you remove or modify them only after careful consideration.

**Note:** In a distributed NetVoyant system, alarm profiles are defined and applied only on the Master server.

### Routers

The Routers alarm profile is a predefined profile designed to generate threshold events for routers. This profile is automatically assigned to the default Routers group and defines the following alarm rules and severities by default:

Alarm rules	Severity
Availability < 100%	Minor
Availability < 100% for 10 minutes	Critical
Interface Availability < 100%	Minor
Interface Availability < 100% for 10 minutes	Critical
Inbound Utilization >= 90% for 10 minutes	Minor
Inbound Utilization >= 95% for 10 minutes	Major
Outbound Utilization >= 90% for 10 minutes	Minor
Outbound Utilization >= 95% for 10 minutes	Major
Inbound Error rate > 2%	Minor
Inbound Error rate > 5%	Major
Outbound Error rate > 2%	Minor
Outbound Error rate > 5%	Major
CPU Utilization > 50% for 10 minutes	Minor

### Switches

The Switches alarm profile is a predefined profile designed to generate threshold events for switches. This profile is automatically assigned to the default Switches group and defines the following alarm rules and severities by default:

Alarm rules	Severity
Availability < 100%	Minor
Availability < 100% for 10 minutes	Critical
Interface Availability < 100% for 10 minutes	Critical
Inbound Utilization >= 50% for 10 minutes	Minor
Inbound Utilization >= 75% for 10 minutes	Major
Outbound Utilization >= 50% for 10 minutes	Minor



Alarm rules	Severity
Outbound Utilization >= 75% for 10 minutes	Major
Inbound Error rate >= 2%	Minor
Inbound Error rate >= 5%	Major
Outbound Error rate >= 2%	Minor
Outbound Error rate >= 5%	Major
CPU Utilization >= 50% for 10 minutes	Minor

### Servers

The Servers alarm profile is a predefined profile designed to generate threshold events for servers. This profile is automatically assigned to the default Servers group and defines the following alarm rules and severities by default:

Alarm rules	Severity
Availability < 100%	Minor
Availability < 100% for 10 minutes	Critical
Inbound Interface Utilization >= 90% for 10 minutes	Minor
Inbound Interface Utilization >= 95% for 10 minutes	Major
Outbound Interface Utilization >= 90% for 10 minutes	Minor
Outbound Interface Utilization >= 95% for 10 minutes	Major
Inbound Error Rate >= 2%	Minor
Inbound Error Rate >= 5%	Major
CPU Utilization >= 20% for 10 minutes	Minor
CPU Utilization >= 50% for 15 minutes	Major
Disk Storage Used >= 95% for 1 hour	Minor
Disk Storage Used >= 99% for 1 hour	Major

### Generic

The Generic alarm profile is a predefined profile designed to generate threshold events for a wide range of devices that are not routers, switches, or servers. This profile is automatically assigned to the default Firewalls, Hubs, Network Termination, Printers, Probes, and Workstations groups. It defines the following alarm rules and severities by default:

Alarm rules	Severity
Availability < 100%	Minor
Availability < 100% for 10 minutes	Critical
Interface Availability < 100% for 10 minutes	Critical
Inbound Interface Utilization >= 90% for 10 minutes	Minor
Inbound Interface Utilization >= 95% for 10 minutes	Major

Alarm rules	Severity
Outbound Interface Utilization >= 90% for 10 minutes	Minor
Outbound Interface Utilization >= 95% for 10 minutes	Major
Inbound Error Rate >= 2%	Minor
Inbound Error Rate >= 5%	Major
Outbound Error Rate >= 2%	Minor
Outbound Error Rate >= 5%	Major

### NetVoyant System

The NetVoyant System alarm profile is a predefined profile designed to generate standard threshold events for devices. It is not assigned to any group by default, but contains a number of standard threshold definitions used in device management. Rather than creating a new, empty alarm profile and defining alarm rules from scratch, you can copy this profile to quickly create new custom alarm profiles and modify the alarm rules according to your needs.

For more information about copying an alarm profile, see [“Duplicating an Alarm Profile” on page 196](#).

The NetVoyant System alarm profile defines the following alarm rules and severities by default:

Alarm rules	Severity
Availability < 100%	Minor
Availability < 100% for 10 minutes	Critical
Interface Availability < 100% for 10 minutes	Critical
Outbound Interface Utilization >= 90% for 10 minutes	Minor
Outbound Interface Utilization >= 95% for 10 minutes	Major
Inbound Error Rate >= 2%	Minor
Inbound Error Rate >= 5%	Major
Outbound Error rate >= 2%	Minor
Outbound Error rate >= 5%	Major
CPU Utilization >= 20% for 10 minutes	Minor
CPU Utilization >= 50% for 15 minutes	Major
Disk Storage Used >= 95% for 1 hour	Minor
Disk Storage Used >= 99% for 1 hour	Major

## Creating a New Alarm Profile

The NetVoyant product installs with some pre-defined alarm profiles; however, you can create your own custom alarm profiles to use instead of the default profiles or in addition to them. When you create a new profile, you add the alarm rules that you want to include in the profile. Each alarm rule defines one or more thresholds for triggering and clearing a threshold event.

**Note:** In a distributed NetVoyant system, alarm profiles are defined and applied only on the Master server.

### To add a new alarm profile:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Select **Alarm Profiles**.

A list of the existing alarm profiles appears in the context panel.

3. In the **Alarm Profiles** tab of the context panel, click **Add**.

The NetVoyant Console automatically creates a new, empty alarm profile using a “New Profile #” naming scheme.

The screenshot shows a 'Profile Settings' dialog box with two tabs: 'Profile Settings' and 'Assigned Groups'. The 'Profile Settings' tab is active. It contains a 'Profile' section with a 'Name' field (containing 'New Profile 1'), an 'Enabled' checkbox, and a 'Description' field. A 'Save' button is located at the bottom right of the 'Profile' section. Below this is an 'Alarm Rules' section containing a table with four columns: 'Name', 'Severity', 'Window (Minutes)', and 'Status'. The table is currently empty. At the bottom of the 'Alarm Rules' section are three buttons: 'Add', 'Change', and 'Remove'.

4. Enter a name for the alarm profile in the **Name** field.
5. Enter descriptive text in the **Description** field.
6. Add a rule to the **Alarm Rules** list by clicking **Add** at the bottom of the panel.

This opens the **Alarm Rule Definition** dialog box. Click **OK** when you are finished defining the alarm rule. For more information about using this dialog box to define alarm rules, see [“Defining an Alarm Rule” on page 199](#).

Repeat this step for as many rules as you need to add to the profile.

7. To enable the alarm profile so that alarms are generated according to the rules for all assigned groups, select the **Enabled** check box.

For more information about assigning an alarm profile to a group, see [“Assigning an Alarm Profile to One or More Groups” on page 197](#).

8. Click **Save**.

## Duplicating an Alarm Profile

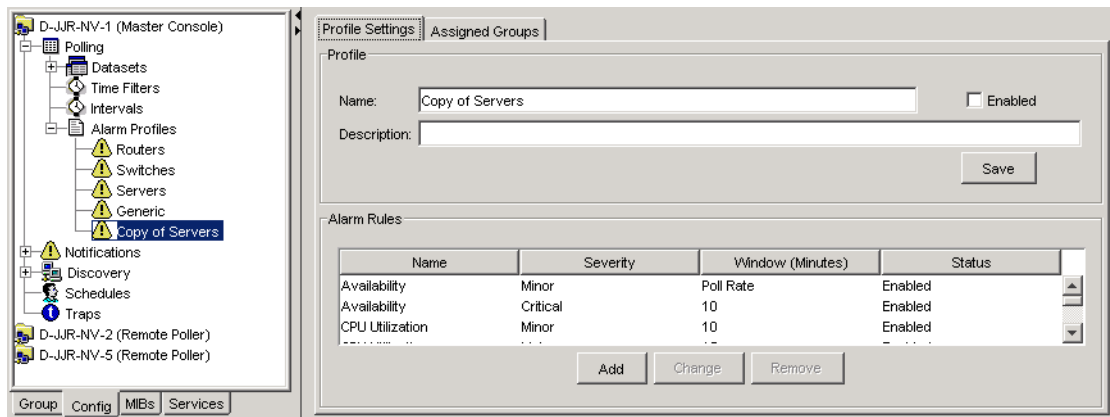
If you have existing alarm profiles and alarm rules with defined thresholds, duplicating a profile and then modifying it can be a quicker and easier way to create specific alarm profiles to assign to the various groups of devices. This is especially time-saving if you are using the same expressions for defining thresholds, but you want to use different severity settings or specify different threshold trigger or clear values.

**Note:** In a distributed NetVoyant system, alarm profiles are defined and applied only on the Master server.

### To duplicate an existing alarm profile:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Select **Alarm Profiles**.  
A list of the existing alarm profiles appears in the context panel.
3. Select the alarm profile in the list that you want to duplicate.
4. Click **Copy**.

The NetVoyant Console automatically generates a duplicate of the selected profile, including its alarm rules, and names it using a “Copy of Profile Name” naming scheme. This new profile is automatically selected and its profile settings appear in the context panel.



5. Change the name for the alarm profile in the **Name** field.
6. Make the additional modifications to the profile settings and alarm rules to customize the profile according to your needs and click **Save**.

**Note:** When you copy an alarm profile, it does not automatically include the assigned group settings. After you save the new profile version, click the **Assigned Groups** tab to assign the profile. For more information about assigning the profile to groups, see [“Assigning an Alarm Profile to One or More Groups” on page 197](#).

For more information about editing the alarm profile settings see the following section. For more information about setting the alarm rules, see [“Defining an Alarm Rule” on page 199](#).

## Editing an Alarm Profile

You can easily change the settings for an existing alarm profile. This includes disabling/enabling the profile, as well as adding, editing, and removing alarm rules for the profile.

**Note:** In a distributed NetVoyant system, alarm profiles are defined and applied only on the Master server.

### To edit an alarm profile:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Select **Alarm Profiles**.  
A list of the existing alarm profiles appears in the context panel.  
You can also select the alarm profile from the tree in the **Config** tab.
3. Select the alarm profile from the list in the context panel and click **Change**.
4. Make any required changes to the **Profile Settings**:
  - Change the text in the **Name** or **Description** fields.
  - Click the **Enabled** check box to enable or disable the profile.
  - Add or change the **Alarm Rules**. For more information about using alarm rules, see [“Defining an Alarm Rule”](#) on page 199.
5. Click **Save** to save your changes
6. Click the **Assigned Groups** tab and select or clear groups for the profile as needed.
7. Click **Save** to save your changes.

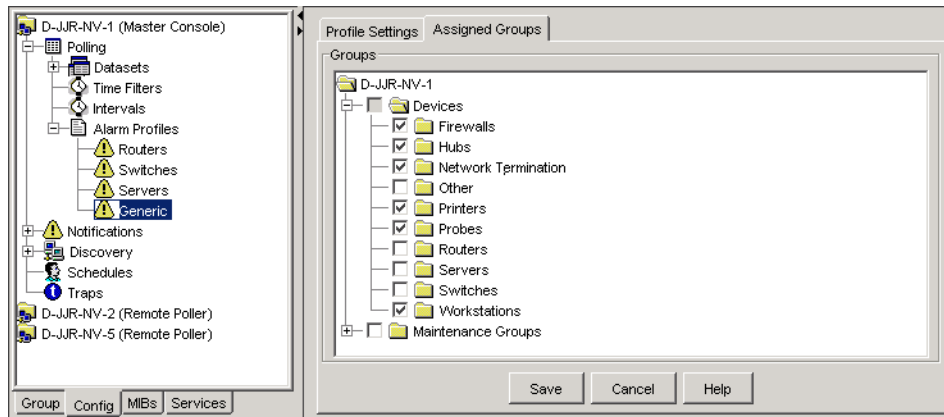
## Assigning an Alarm Profile to One or More Groups

When you assign an alarm profile to a NetVoyant group, the alarm rules and threshold values are used to generate alarm events for the devices within the group. You can assign a profile to more than one group and a group can have more than one alarm profile assigned to it.

**Note:** In a distributed NetVoyant system, alarm profiles are defined and applied only on the Master server.

### To assign a profile to one or more groups:

1. In the **Config** tab of the NetVoyant Console (Master or standalone), expand the Master server.
2. Expand **Alarm Profiles** and navigate to the alarm profile you want to assign.  
The **Profile Settings** for the selected alarm profile appear in the context panel.
3. Click the **Assigned Groups** tab.



4. In the context panel, expand folders so that groups and sub-groups are visible.

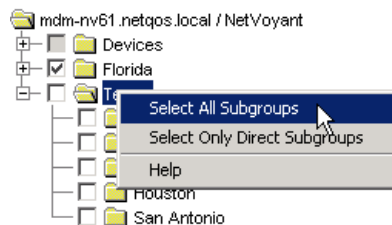
- All checked items are groups to which the alarm profile is assigned.
- A gray box next to an item indicates that there is one or more subgroups assigned, but not all subgroups.

**Note:** If your NetVoyant system is registered with the NetQoS Performance Center as a data source, only groups created in the NetVoyant Console are available for assigning alarm profiles. Groups populated from NPC synchronization do not appear in the **Assigned Groups** tab.

5. Select and clear the check boxes so that the alarm profile is assigned to the groups that you want.

When you select a group check box, all child objects in the group are selected, but not subgroups.

To make selections for groups containing many subgroups and child objects, you can right-click a group and choose **Select All Subgroups** (to make a recursive selection) or **Select Only Direct Subgroups**.



You can also clear selections by choosing **Deselect All Subgroups** (to recursively clear the selections) or **Deselect Only Direct Subgroups**.

6. Click **Save** to save your changes.

## Working with Alarm Rules

The alarm rules that you add to an alarm profile define how an alarm and the threshold values are generated. A rule is a set of conditions for a single dataset that, when they evaluate to true, will trigger an alarm. All of the conditions (thresholds) in the rule must be met in order for the rule to generate an alarm. A profile can contain multiple rules. Each rule designates the severity of the alarm condition, which expressions are tested, and the exceeded and cleared values.

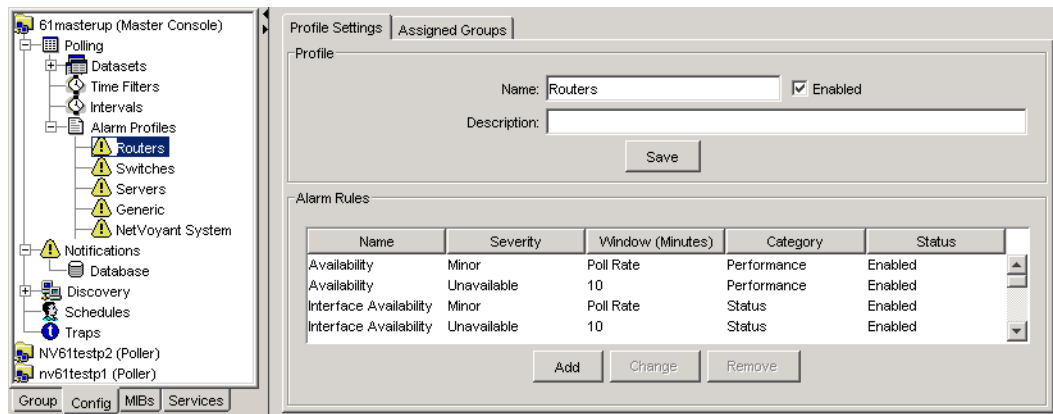
### Defining an Alarm Rule

You must have at least one alarm rule in an alarm profile. Most alarm profiles contain multiple rules and might have duplicate rule types that use different severity levels and threshold values so that notifications can be sent based on the severity level of the threshold violation. For more information about generating notifications from threshold events, see [“Triggering Notifications for a Threshold Event”](#) on page 243.

**Note:** In a distributed NetVoyant system, alarm profiles are defined and applied only on the Master server.

#### To define a new alarm rule:

1. Navigate to the profile settings for an alarm profile by expanding **Master server > Polling > Alarm Profiles** in the **Config** tab and selecting the alarm profile where you want to add a rule.



2. In the **Profile Settings**, click **Add** at the bottom of the panel.

The **Alarm Rule Definition** dialog box opens.

3. Enter a name for the rule in the **Name** field.
4. Use the **Dataset** drop-down list to select a dataset for the rule.

This is the dataset used for defining any thresholds for the rule. A threshold is specified by the value for an expression in the dataset. After a threshold has been defined for the rule, you cannot change the dataset.

For more information about dataset expressions, see [“Creating or Editing a Dataset Expression”](#) on page 105.

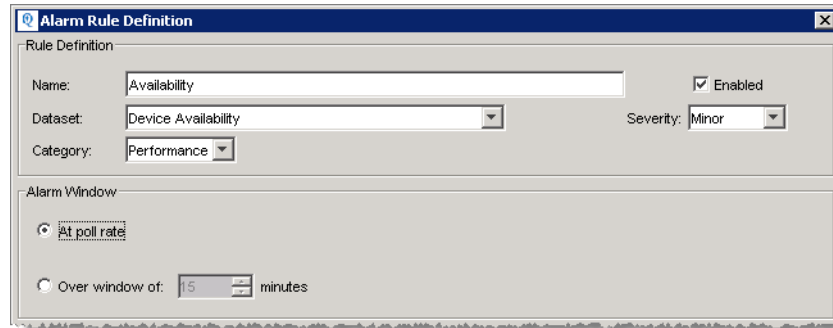
5. Use the **Category** drop-down list to assign an event category for the alarm rule.

An event can be one of the following categories: Status, Threshold, Configuration, Performance, or Unknown.

**Note:** If your NetVoyant system is registered with the NetQoS Performance Center as a data source, this category is used to filter events in the Map and Map Event List.

6. Use the **Severity** drop-down list to designate the severity level of the alarm that is generated when the rule's threshold condition is met, or if multiple conditions are all met.

For more information about event severities, see [“Configuring Event Severities” on page 224](#).



7. In the **Alarm Window** section of the dialog box, choose the alarm window type for the rule:
  - **At poll rate** - Use this option to test the rule at every polling interval. The newest value is compared with the threshold definitions and will trigger immediately if the value meets all threshold definitions.
  - **Over window of \_\_ minutes** - Use this option to specify an interval for testing the expression values (rate values) taken over that interval. These values are compared with the threshold definitions and will trigger immediately if the values meet all threshold definitions.

**Note:** When using the `availability` expression in the Device Availability dataset to create an alarm rule, availability is determined by a successful or unsuccessful poll. For more information about using alarm windows to calculate thresholds using `availability`, see [“Availability Threshold Events” on page 205](#).

8. In the **Thresholds** section of the dialog box, click **Add** to add a threshold (condition) for the rule. This opens the **Threshold Definition** dialog box. The defined threshold is a limit on the values for the specified expressions that you see as acceptable. A threshold is composed of a threshold exceeded and a threshold cleared limit. For more information, see [“Defining Thresholds for Alarm Rules” on page 201](#).



Alarm Condition	Interval
availability < 100.0	Poll Rate

You can click **OK** to add the threshold to the list and repeat this step for as many threshold definitions (conditions) that you want for the rule.

- Click **OK** when you have finished defining the alarm rule.

You can repeat this process for as many rules as you need to add to the profile.

## Defining Thresholds for Alarm Rules

The NetVoyant product generates alarms and sends notifications based upon the thresholds that you set for the rules within the assigned alarm profile. These thresholds are the limits on the values for these expressions that you see as acceptable. Each threshold is composed of a threshold exceeded and a threshold cleared limit. For more information, see [“Using Thresholds to Trigger Events”](#) on page 204.

**Note:** You can create thresholds that change according to the baseline value for an expression or according to property values set at the poll instance level. For more information, see [“Creating Dynamic Thresholds and Expressions”](#) on page 208.

### To set a threshold for an alarm rule:

- Navigate to the profile settings for an alarm profile by expanding **Master server > Polling > Alarm Profiles** in the **Config** tab and selecting the alarm profile where you want to add or modify a rule.
- In the Profile Settings, click **Add** at the bottom of the panel to create a new rule or select a rule and click **Change**.

This opens the **Alarm Rule Definition** dialog box. For information about changing the **Rule Definition** or **Alarm Window** settings, see [“Defining an Alarm Rule”](#) on page 199.

- In the **Thresholds** section of the dialog box, click **Add** to add a threshold to the rule.

This opens the **Threshold Definition** dialog box.

The image shows a 'Threshold Definition' dialog box. It has two main sections: 'Event Detection' and 'Expression'. In the 'Event Detection' section, 'Alarm detection window is: 10 minutes' is shown. There are two radio buttons: 'Alarm when condition exists for the entire window.' (which is selected) and 'Alarm when condition occurs for: 1 total minute(s) during the window'. The 'Expression' section has three tabs: 'Constant', 'Percent of Baseline', and 'Baseline +/- Std Dev'. The 'Constant' tab is active. It shows 'Expression: availability'. Below this, 'Alarm when: Below' is selected in a dropdown, 'Value of: 100.0' is in a text box, and 'Clear when: [Above or Equal] 100.0' is also in a text box. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

4. If the alarm detection window is a specified number of minutes in the **Alarm Rule Definition** dialog box, choose an **Event Detection** option:

- **Alarm when condition exists for entire interval** - Select this option to trigger an alarm when the condition has been met for the entire interval.
- **Alarm when condition occurs for \_\_ total minute(s) during total minute(s) during the window** - Select this option to trigger an alarm when the condition has been met for a specified number of minutes within the alarm detection window. These values should be set in increments of the poll rate if possible (5, 10, 15, 20 minutes, and so on).

**Note:** If the alarm detection window is set to the poll rate for the alarm rule, this option is not available.

5. Define an **Expression** for the threshold by type:

- **Constant** - Use this threshold expression type to generate an alarm event based on the raw value of a dataset expression.

The **Alarm when** setting specifies the point at which an alarm event is triggered— when that value is above, above or equal, below, below or equal, not equal, or equal to the specified threshold value.

Set the **Clear when** value to specify the point at which the alarm event is marked as over or “cleared.” This enables the expression to remain in the threshold event state until it returns to an acceptable value.

The image shows a close-up of the 'Expression' section of the dialog box. It has three tabs: 'Constant', 'Percent of Baseline', and 'Baseline +/- Std Dev'. The 'Constant' tab is active. It shows 'Expression: availability'. Below this, 'Alarm when: Below' is selected in a dropdown, 'Value of: 100.0' is in a text box, and 'Clear when: [Above or Equal] 100.0' is also in a text box.

- **Percent of Baseline** - Use this threshold expression type to specify a calculated percentage over or under the baseline value for the dataset expression to trigger an alarm event.

For each poll instance, the NetVoyant product evaluates the function as the current baseline calculation of the expression for a given poll instance. It typically calculates baselines on an hourly basis.

**Note:** To use this function, the value must be defined in the **Baselines** tab of the dataset so that a baseline is calculated. If the baseline is not in this list, it uses the actual value of the expression for the baseline value. For more information about baselines, see [“Using Baselines” on page 108](#)

The **Alarm when** setting specifies the point at which an alarm event is triggered— when the dataset expression value is above, above or equal, below, below or equal, not equal, or equal to the specified baseline percentage value.

The **Clear when** setting specifies the point at which an alarm event is marked as over or “cleared”— when the dataset expression value is above, above or equal, below, below or equal, not equal, or equal to the specified baseline percentage value. This enables the expression to remain in the threshold event state until it returns to an acceptable value.

- **Baseline +/- Std Dev** - Use this expression type to trigger the threshold when the value exceeds the baseline plus  $x$  number of standard deviations. For example, if the interface utilization baseline is 25% with a standard deviation of 5%, configuring the threshold to trigger when the interface utilization exceeds 3 standard deviations above the baseline would result in a trigger when the utilization exceeds 40%.

The **Alarm when** setting specifies the point at which an alarm event is triggered— when the dataset expression value is the specified number of standard deviations above, above or equal to, below, below or equal to, not equal to, or equal to the baseline value.

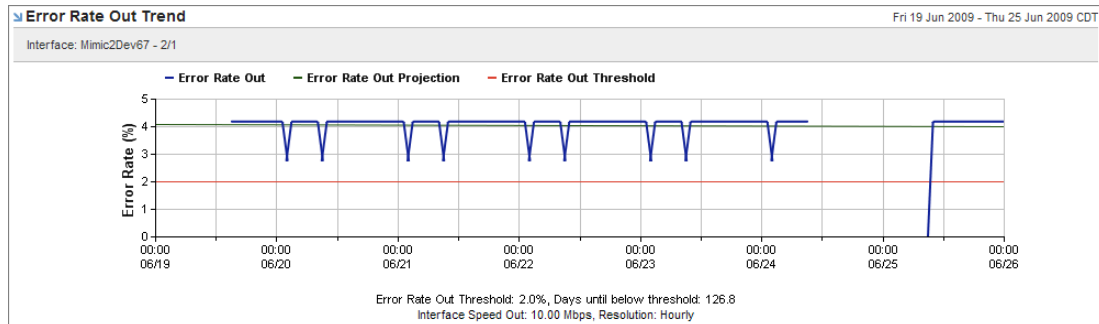
The **Clear when** setting specifies the point at which an alarm event is marked as over or “cleared”— when the dataset expression value is above, above or equal to, below, below or equal to, not equal to, or equal to the specified number of standard deviations away from the baseline value. This enables the expression to remain in the threshold event state until it returns to an acceptable value.

**Note:** Ensure that the tab for expression type you want to use is the active tab before you save your changes.

6. Click **OK**.

## Using Thresholds in Reporting

By default, some of the NetVoyant trend plot views display the threshold for a metric. Many of these views include the threshold information in the footer, and some of these calculate the projected number of days until the threshold is reached.



If there is more than one threshold defined for the dataset expression (reporting metric) in any alarm profiles assigned to the selected group containing the device, the NetVoyant reporting tool uses the strictest threshold definition (higher severity/lower threshold) to generate a threshold value for the view.

## Using Thresholds to Trigger Events

A threshold is the limit on the values you see as acceptable for an expression. Each threshold is composed of a threshold triggered and a threshold cleared limit.

You can create thresholds that change according to the baseline value for an expression or property values set at the poll instance level. For more information, see [“Defining Thresholds for Alarm Rules”](#) on page 201.

**Threshold Triggered.** If the NetVoyant product polls data that exceeds the threshold exceeded value, it triggers a threshold event.

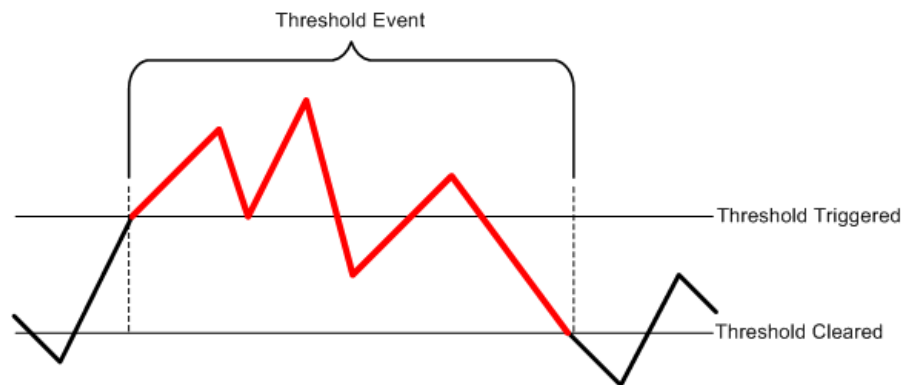
For example, you can set a threshold exceeded value of 50.0 for the interface utilization (`ifutil`) expression. If it polls utilization data from an interface that is greater than 50.0, it triggers a threshold event.

**Threshold Cleared.** After a threshold event has been triggered for a poll instance, when it polls data from the poll instance that is below the threshold cleared value, the NetVoyant product marks the threshold event as over or “cleared.”

For example, you can set a threshold cleared value of 30.0 for the interface utilization (`ifutil`) expression. After a threshold event has been triggered for a poll instance, if the NetVoyant product polls utilization data from an interface that is less than 30.0, it clears the threshold event.

**Note:** When the alarm occurs because of a value exceeding the threshold trigger value (threshold exceeded), the threshold cleared values are often lower than threshold trigger value to require expressions to return to a level that is closer to normal before it considers the threshold event to be cleared.

*A threshold event starts where the threshold is triggered and ends when it crosses the threshold cleared value.*



**Using Event Severities.** You can set the event severity for each alarm rule as shown in the following figure. This is the severity assigned to the threshold event when a threshold is triggered. You can create multiple versions of the same rule using different levels of severity in order to create escalated alarms and notifications.

*The alarm rule severity for the rules in an alarm profile*

Alarm Rules			
Name	Severity	Window (Minutes)	Status
CPU Utilization	Minor	10	Enabled
Errorrate (In)	Minor	Poll Rate	Enabled
Errorrate (In)	Major	Poll Rate	Enabled
Errorrate (Out)	Minor	Poll Rate	Enabled
Errorrate (Out)	Minor	Poll Rate	Enabled
Utilization (In)	Minor	10	Enabled
Utilization (In)	Major	10	Enabled
Utilization (Out)	Minor	10	Enabled

**Notifications.** When an alarm rule is set, a threshold event occurs when an expression meets the threshold trigger value. Threshold events (except those where the alarm rule severity is set to None) create alarm log entries in the NetVoyant database, but, by default, notifications are not sent. If you want to receive notifications, such as emails, SNMP traps, or others in response to alarm events, you must configure a notification for the threshold event.

For more information on creating notifications, see [“Creating a Notification” on page 227](#).

**Availability Threshold Events.** If you create an alarm rule for the Device Availability dataset that sets an alarm condition when the availability expression falls below a specified level (threshold) over an entire window, the alarm might not be triggered. The reason for this is that the default availability expression is calculated using the sysUpTime OID, and this information is available only when there is a successful poll.

```
if ((sysUpTime/100.0) < duration) then (sysUpTime/duration) else 100.0
```

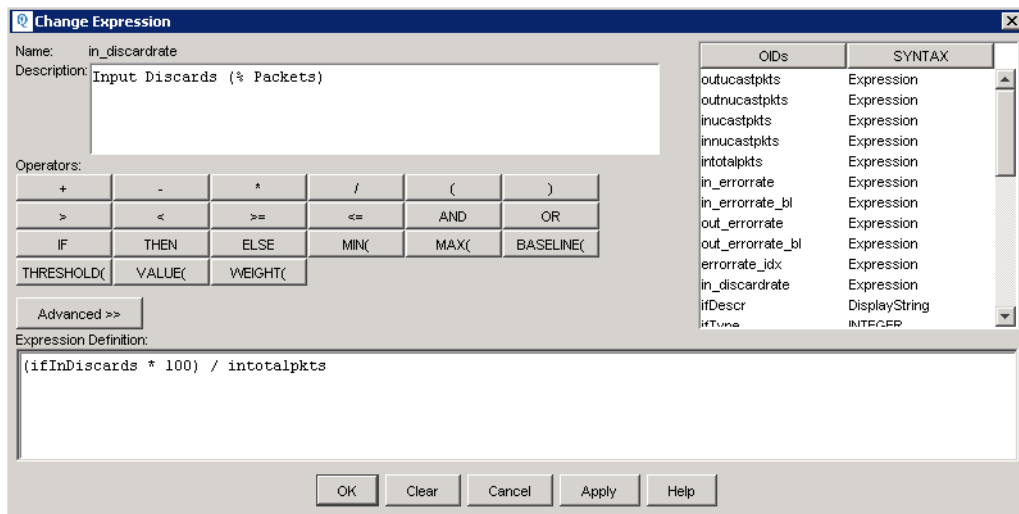
When there is a successful poll, NetVoyant looks at the sysUpTime information in the current poll and any previous polls over the event duration window and uses this to calculate the value for the expression.

The default alarm profiles include an Availability alarm rule over a 10 minute window using a 100 threshold value. You can lower this value to make the condition less sensitive, but the lower the threshold value, the more likely it is that NetVoyant does not trigger an event when an unsuccessful poll occurs during the event duration window.

## Using Dataset Expressions in Thresholds

Many of the default datasets in the NetVoyant Console have existing expressions designed to capture and calculate useful metrics. To create a threshold expression that generates and clears an alarm, you must specify an expression that is associated with the dataset specified in the alarm rule.

For example, the Interface Statistics dataset has an expression named `in_discardrate`. This expression (shown in the following figure) calculates the input discard rate by multiplying the value of the inbound interface discards (`ifInDiscards`) by 100 and dividing it by the value of the total number of interface's inbound packets (`intotalpkts`):



This expression is used to create thresholds for the Utilization (in) alarm rules within the default Routers alarm profile.

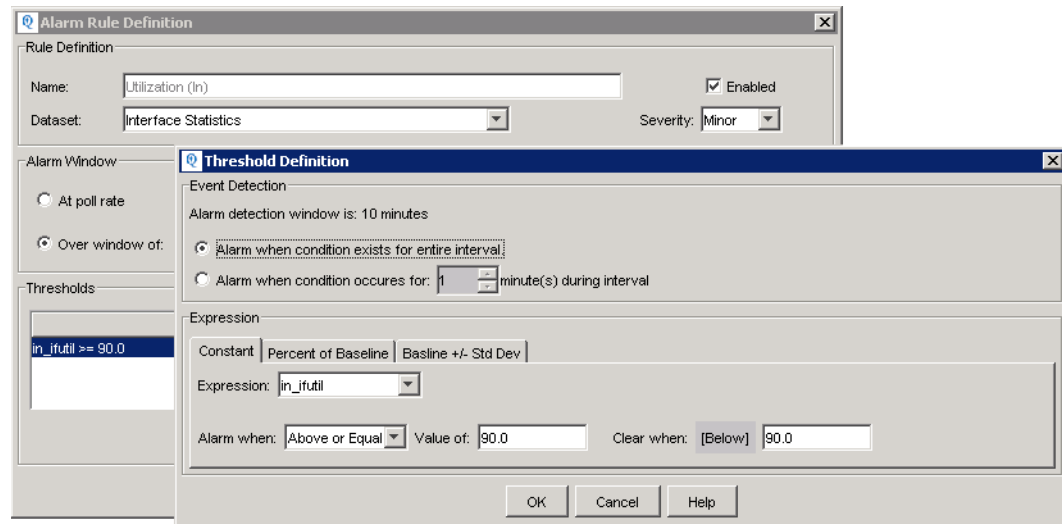
For more information about working with dataset expressions, see [“Creating or Editing a Dataset Expression” on page 105](#).

**Important:** When you add, delete, or modify a dataset expression, the system will modify the rollup tables. This can affect historical data.

**About Threshold Levels and Escalated Notifications.** You can configure the NetVoyant product to send escalated notifications for an expression based on increasing thresholds. To configure an escalated notification, you must create multiple alarm rules for the same expression and then assign each rule a different event severity. When you create notifications for each level, you can trigger the notification based on the threshold level expression name.

For example, the default Routers alarm profile contains two alarm rules named Utilization (in) that are associated with the Interface Statistics dataset. One rule has a severity setting of Minor and the other has an event severity of Major. These two rules are designed so that the same metric is used to trigger alarm events of differing severity.

The first Utilization (in) rule contains a single threshold expression that triggers the alarm event when the value of `in_ifutil` is above or equal to 90.0 for the entire polling interval. It clears the alarm event when this value is below 90.0 for an entire polling interval. In the alarm rule, this is assigned a Minor event severity.



The second Utilization (in) rule contains a single threshold expression that triggers the alarm event when the value of `in_ifutil` is above or equal to 95.0 for the entire polling interval. It clears the alarm event when this value is below 95.0 for an entire polling interval. In the alarm rule, this is assigned a Major event severity.

These two rules function to generate the same type of threshold event, but with different severities. The event with the Minor severity will appear in the alarm log. A NetVoyant administrator might set up a notification for the event with the Major event severity because it is a more serious violation.

## Creating Dynamic Thresholds and Expressions

The following are some examples for how to threshold expressions to create dynamic thresholds for which the NetVoyant product can generate alarms or send notifications.

**Example 1: Constant Value Threshold.** The following is an example of a fixed-value (Constant) threshold definition using the availability (`availability`) expression in the Device Availability dataset.

### *A fixed value threshold for availability*

The screenshot shows the 'Expression' configuration window. It has three tabs: 'Constant', 'Percent of Baseline', and 'Baseline +/- Std Dev'. The 'Constant' tab is selected. The 'Expression:' dropdown is set to 'availability'. The 'Alarm when:' dropdown is set to 'Below', and the 'Value of:' text box contains '100.0'. The 'Clear when:' dropdown is set to '[Above or Equal]', and the text box contains '100.0'.

This threshold uses a fixed value of 100 as the threshold trigger for the `availability` expression. Any value below 100 triggers an alarm event. A value equal or above 100 clears the event.

**Example 2: Setting Thresholds as a Percent of Baseline.** The following is an example of a threshold definition based on the inbound interface utilization (`in_ifutil`) by a percentage of the 30-day moving baseline for the expression.

### *A percent of baseline threshold for interface utilization*

The screenshot shows the 'Expression' configuration window. It has three tabs: 'Constant', 'Percent of Baseline', and 'Baseline +/- Std Dev'. The 'Percent of Baseline' tab is selected. The 'Expression:' dropdown is set to 'in\_ifutil'. The 'Alarm when:' dropdown is set to 'Above', and the text box contains '2'. The text 'times the baseline' follows the text box. The 'Clear when:' dropdown is set to '[Below or Equal]', and the text box contains '1.25'. The text 'times the baseline' follows the text box.

This threshold is crossed when `in_ifutil` exceeds a value that is two times (200%) the current 30-day moving baseline.

**Example 3: Removing False Positives with a Combination Threshold.** The following is an example of using two threshold definitions that use a constant and a baseline to create a less erroneously sensitive threshold trigger for interfaces that generally have a low utilization baseline (for example, GigE or LAN switch ports).

### *Use two threshold definitions to create a more sensitive alarm trigger*

The screenshot shows the 'Thresholds' configuration window. It has a table with two columns: 'Alarm Condition' and 'Interval'. The table contains two rows:

Alarm Condition	Interval
<code>ifutil &gt; 50.0</code>	Entire window
<code>ifutil Above 200% of baseline</code>	Entire window

At the bottom of the window are three buttons: 'Add', 'Change', and 'Remove'.

The threshold is triggered only when `ifutil` exceeds a value that is above either 50% **and** is at least two times the current 30-day moving baseline for `ifutil` as described in Example 3.



## WORKING WITH EVENT AND ALARM LOGS

The NetVoyant Console includes logs for event and alarms. You can display these as log panels in the main Console window or you can view the contents of a log in a separate log window.

Events can be one of the following types:

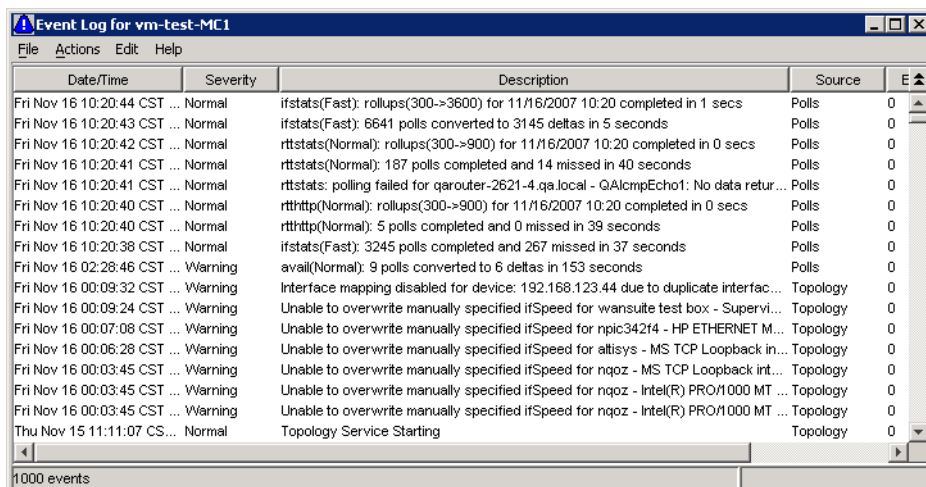
- **Log** - These events track actions that NetVoyant services perform along with topology changes in your network or devices. You can configure the logging level of the NetVoyant services. For more information, see [“Configuring a Service’s Start Mode or Logging Level” on page 283](#).
- **Polling** - These events track the SNMP polls sent to your devices. A polling event occurs when a device does not respond to an SNMP request from the NetVoyant product during a scheduled polling cycle.
- **Trap** - These events track incoming SNMP traps. You can configure new trap events for the types of SNMP traps that you expect the NetVoyant product to receive. For more information, see [“Adding or Editing an SNMP Trap Event” on page 325](#).
- **Threshold** - These events track threshold violations on your devices. A threshold event occurs when a polled value for an expression goes beyond the threshold exceeded value that you set for the expression in an alarm profile. For more information about defining thresholds in an alarm profile, see [“Defining Thresholds for Alarm Rules” on page 201](#).

### Viewing the Log Panels

You can choose to display the event and alarm log panels at the bottom of the NetVoyant Console or in separate windows. These panels display current event logs as triggered by service logging, polling events, SNMP traps, and database notifications for threshold events.

To view the event log panel, perform one of the following actions:

- To view the log panel within the NetVoyant Console main window, select **Show Event Log** from the **View** menu.
- To view the log panel in a separate window, select **Event Log** from the **Tools** menu.



The event log panel provides the following information:

Field	Description
<b>Date/Time</b>	The server date and time at which the event occurred.
<b>Severity</b>	The severity of the event. Logs in the event log panel can be one of the following severities: normal, warning, minor, major, critical, or a custom event severity.
<b>Description</b>	A description of the event that occurred.
<b>Source</b>	The service or device that initiated the event.
<b>Error code</b>	A code to assist technical support in diagnosing issues.
<b>Server</b>	The Master Console or remote poller on which the service that initiated the event resides. For standalone configurations, the server is always the Master Console.

**Note:** You can double-click an event to see all information recorded in the event log in an **Event Details** window. For more information, see “[Viewing Details for an Event or Alarm](#)” on page 211.

## Viewing the Alarm Log Panel

The alarm log panel displays event logs for threshold events, missed polls, and incoming SNMP traps.

To view the Alarm Log Panel, perform one of the following:

- To view the log panel within the NetVoyant Console main window, select **Show Alarm Log** from the **View** menu.
- To view the log panel in a separate window, select **Alarm Log** from the **Tools** menu.

Ack	Date/Time	Type	Source	Severity	Description	Category	Error code
<input type="checkbox"/>	Thu Nov 15 11:00:16 CST 2007	Polling	np127e04b	Major	avail: polling failed for np127e04b...	Status	108
<input type="checkbox"/>	Thu Nov 15 11:00:16 CST 2007	Polling	np18cfc7f	Major	avail: polling failed for np18cfc7f...	Status	108
<input type="checkbox"/>	Thu Nov 15 11:00:16 CST 2007	Polling	np122b9dd	Major	avail: polling failed for np122b9dd...	Status	108
<input type="checkbox"/>	Thu Nov 15 10:55:00 CST 2007	Threshold	qarouter-2621-4.qa.local - DHC...	Minor	Threshold exceeded for qarouter...	Threshold	0
<input type="checkbox"/>	Thu Nov 15 10:50:11 CST 2007	Polling	np127e04b	Major	avail: polling failed for np127e04b...	Status	108
<input type="checkbox"/>	Thu Nov 15 10:50:11 CST 2007	Polling	np122b9dd	Major	avail: polling failed for np122b9dd...	Status	108
<input type="checkbox"/>	Thu Nov 15 10:30:00 CST 2007	Threshold	qarouter-2621-4.qa.local - DHC...	Minor	Threshold exceeded for qarouter...	Threshold	0
<input type="checkbox"/>	Thu Nov 15 10:25:00 CST 2007	Threshold	qarouter-2621-4.qa.local - DHC...	Minor	Threshold exceeded for qarouter...	Threshold	0
<input type="checkbox"/>	Thu Nov 15 10:20:10 CST 2007	Polling	np122b9dd	Major	avail: polling failed for np122b9dd...	Status	108
<input type="checkbox"/>	Thu Nov 15 10:10:00 CST 2007	Threshold	qarouter-2621-4.qa.local - DHC...	Minor	Threshold exceeded for qarouter...	Threshold	0
<input type="checkbox"/>	Thu Nov 15 10:10:11 CST 2007	Polling	np127e04b	Major	avail: polling failed for np127e04b...	Status	108
<input type="checkbox"/>	Thu Nov 15 10:10:11 CST 2007	Polling	np18cfc7f	Major	avail: polling failed for np18cfc7f...	Status	108
<input type="checkbox"/>	Thu Nov 15 10:10:11 CST 2007	Polling	np122b9dd	Major	avail: polling failed for np122b9dd...	Status	108
<input type="checkbox"/>	Thu Nov 15 10:00:00 CST 2007	Threshold	qarouter-2621-4.qa.local - DHC...	Minor	Threshold exceeded for qarouter...	Threshold	0
<input type="checkbox"/>	Thu Nov 15 09:45:13 CST 2007	Polling	np127e04b	Major	avail: polling failed for np127e04b...	Status	108

The alarm log panel displays the following information:

Field	Description
<b>Ack</b>	This check box enables you to acknowledge an alarm that you already addressed.
<b>Date/Time</b>	The server date and time at which the alarm occurred.
<b>Type</b>	The type of alarm. Possible alarm types include threshold, polling, and trap.
<b>Source</b>	The service or device that initiated the alarm.

Field	Description
<b>Severity</b>	The severity level of the alarm. Alarms can be one of the following severity levels: Warning, Minor, Major, or Critical.  The NetVoyant product labels alarm logs by color according to their severity. It also labels the device and group that was the source of the alarm log in the Group tab of the tree-tab panel.
<b>Description</b>	A description of the alarm that occurred.
<b>Category</b>	The category of the event, which can be one the following: <ul style="list-style-type: none"> <li>• <b>Status</b> - Indicates that the a status change occurred. Polling events are in the status category.</li> <li>• <b>Threshold</b> - Indicates that a threshold event occurred.</li> <li>• <b>Configuration</b> - Indicates that a configuration change occurred.</li> <li>• <b>Performance</b> - Indicates an issue with utilization or availability.</li> </ul>
<b>Error code</b>	A code to assist technical support in diagnosing issues.
<b>Server</b>	The server on which the service that initiated the alarm resides.

**Note:** You can double-click an event to view all information recorded in the event log in an **Event Details** window. For more information, see [“Viewing Details for an Event or Alarm”](#) on page 211.

## Viewing Details for an Event or Alarm

As you review the event or alarm logs, you will see items that you want to investigate so that you can determine if further action is needed. You can access details for an individual event or alarm from the log and alarm windows or panels.

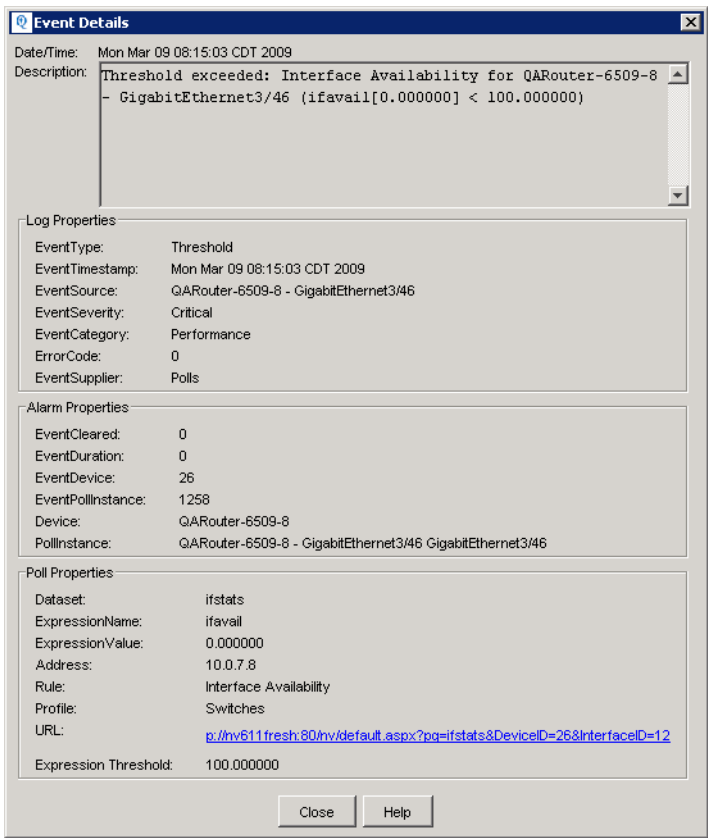
### To view the details of an event or alarm:

1. Double-click the event in the log panel or the alarm in the alarm panel on the NetVoyant Console.

The **Event Details** dialog box opens.

This dialog box displays the following details for the event or alarm:

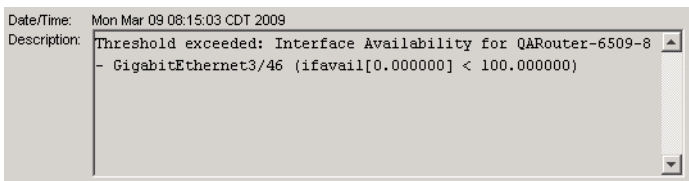
- [Standard Event Properties](#)
- [Log Properties](#)
- [Alarm Properties](#)
- [Poll Properties](#)
- [Trap Bindings](#)



- 2. Click **Close** to close the dialog box.

Standard Event Properties

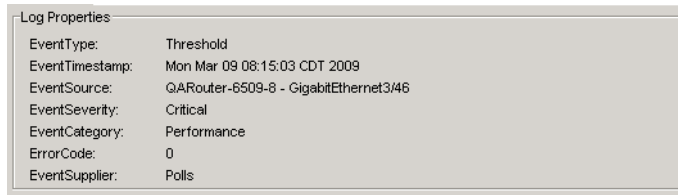
The **Event Details** dialog box displays the Standard Event properties for all events and alarms.



Field	Description
Date/Time	The server date and time at which the event occurred.
Description	A description of the event that occurred.

## Log Properties

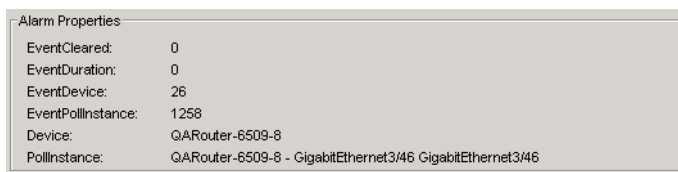
The **Event Details** dialog box displays the Log Properties for all logged events.



Field	Description
<b>Date/Time</b>	The server date and time at which the event occurred.
<b>Description</b>	A description of the event that occurred.
<b>EventType</b>	The type of event that occurred.
<b>EventTimestamp</b>	The date and time at which the event occurred.
<b>EventSource</b>	The service or device that initiated the event.
<b>EventSeverity</b>	The severity of the event. Events can be one of the following severities: normal, warning, minor, major, critical, or a custom event severity.
<b>EventCategory</b>	The category of the event. An event can be one the following categories: <ul style="list-style-type: none"> <li>• <b>Status</b> - Indicates that a status change has occurred. Polling events are in the status category.</li> <li>• <b>Threshold</b> - Indicates that a threshold event occurred.</li> <li>• <b>Configuration</b> - Indicates that a configuration change occurred.</li> <li>• <b>Performance</b> - Indicates an issue with utilization or availability.</li> </ul>
<b>ErrorCode</b>	A code to assist Technical Support in diagnosing issues.
<b>EventSupplier</b>	The NetVoyant service that supplied the event.

## Alarm Properties

The **Event Details** dialog box displays the Alarm Properties for alarms, which are triggered by threshold and polling events.



Field	Description
<b>EventCleared</b>	Indicates whether the alarm has been cleared.
<b>EventDuration</b>	The duration of the event in seconds.
<b>EventDevice</b>	The numeric identifier for the device that initiated the event.
<b>EventPollInstance</b>	The numeric identifier for the poll instance that initiated the event.

Field	Description
<b>Device</b>	The device that initiated the event.
<b>PollInstance</b>	The poll instance that initiated the event.

## Poll Properties

The **Event Details** dialog box displays the Poll Properties for all polling and threshold events. Some of the information is available only for threshold events.

Poll Properties	
Dataset:	ifstats
ExpressionName:	ifavail
ExpressionValue:	0.000000
Address:	192.168.123.2
Rule:	Interface Availability
Profile:	Routers
URL:	<a href="http://nv6111fresh:80/nv/default.aspx?pg=ifstats&amp;DeviceID=3&amp;InterfaceID=59">http://nv6111fresh:80/nv/default.aspx?pg=ifstats&amp;DeviceID=3&amp;InterfaceID=59</a>
Expression Threshold:	100.000000

Field	Description
<b>Dataset</b>	The dataset for the poll instance that generated the polling or threshold event.
<b>ExpressionName</b>	The name of the expression used to evaluate the alarm rule.
<b>ExpressionValue</b>	The value for the expression that triggered the alarm.
<b>Address</b>	The IP address of the device or interface that generated the alarm.
<b>Rule</b>	The name of the alarm rule that generated the threshold event.
<b>Profile</b>	The name of the alarm profile that contains the alarm rule.
<b>URL</b>	Use this URL to open the NetVoyant reporting tool and view a summary report for the device or interface that generated the event.
<b>Expression Threshold</b>	The threshold trigger value for the alarm rule that generated the alarm.

## Trap Bindings

The **Event Details** dialog box displays the Trap Bindings for trap events (incoming SNMP traps) only.

Trap Bindings	
CISCO_SYSLOG_MIB.clogHistSeverity.26449	5
TrapCommunity	redpoint
CISCO_SYSLOG_MIB.clogHistTimestamp.26449	386198370
CISCO_SYSLOG_MIB.clogHistMsgText.26449	Process exceeds 200ms threshold (200ms IOS ...
TrapName	
SNMPv2_MIB.snmpTrapOID.0	CISCO_SYSLOG_MIB.clogMessageGenerated
TrapType	CISCO_SYSLOG_MIB.clogMessageGenerated
TrapUpTime	386198371
RFC1213_MIB.sysUpTime.0	386198371
CISCO_SYSLOG_MIB.clogHistFacility.26449	SNMP
TrapVersion	1
EventSource	mnrouter1.redpt.com
CISCO_SYSLOG_MIB.clogHistMsgName.26449	HIGHCPU

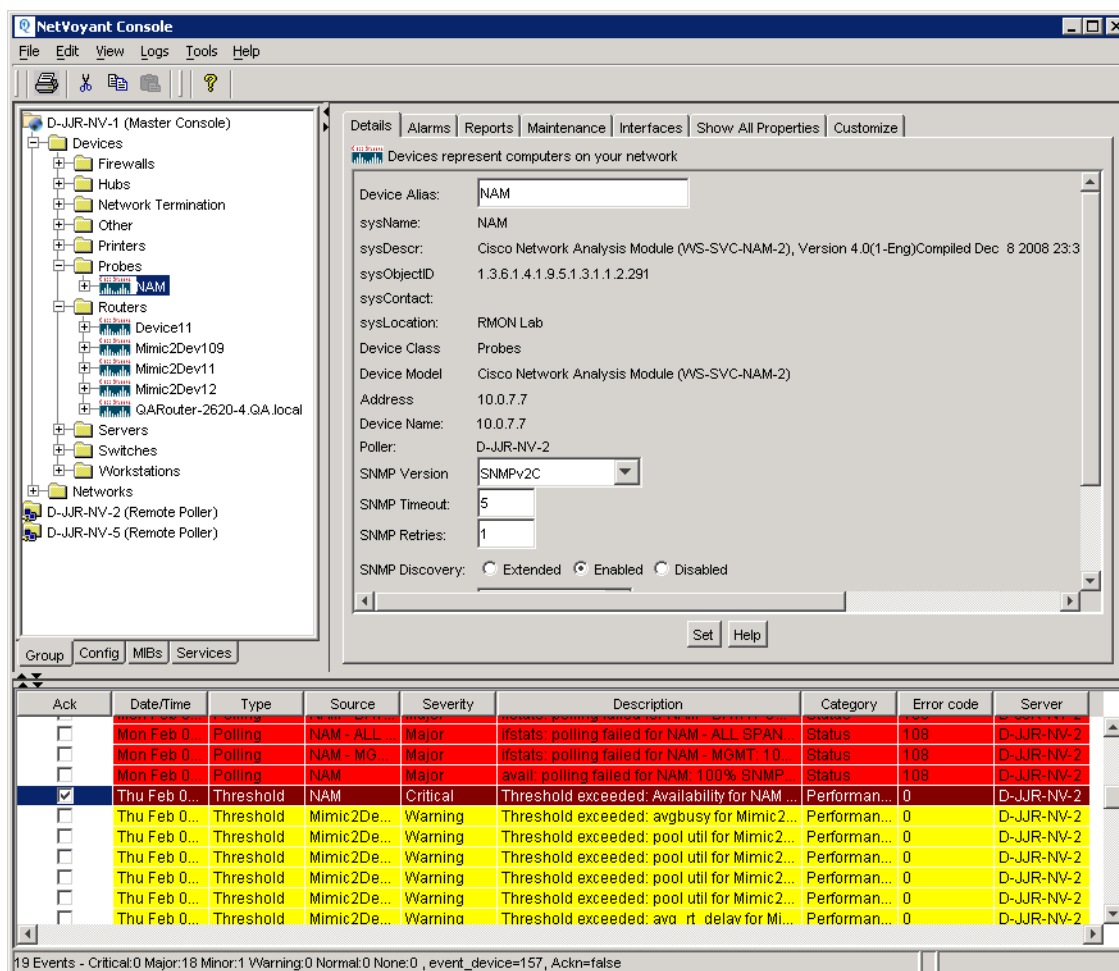
Field	Description
<b>Variable bindings</b>	Fields supplied by the SNMP agent that initiated the trap that are unique to the SNMP trap or SNMP agent type. For more information, see <a href="#">“Using Variable Bindings”</a> on page 330.
<b>TrapCommunity</b>	The SNMP profile that NetVoyant used to authenticate the trap sender.
<b>TrapName</b>	The name of the trap event, if it has been configured.
<b>TrapType</b>	The type of SNMP trap as indicated by the SNMP agent’s MIB definition. The TrapType defines what variables are sent as variable bindings in the MIB-specific bindings and the purpose of the trap.
<b>TrapUpTime</b>	The time at which the SNMP agent sent the trap.
<b>SNMPEnterpriseID</b>	SNMP Enterprise ID of the SNMP agent that sent the trap.
<b>TrapVersion</b>	The version number of the trap.

## Viewing the Source of an Event or Alarm

The source of an event or alarm is the poll instance or interface that the NetVoyant product identifies as the cause of the event or alarm.

### To view the source of an event or alarm in the tree-tab panel:

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels”](#) on page 209.
2. Select the event or alarm in the log panel.
3. Select one of the following from the **Logs** menu:
  - For an event, select **Event Log > Actions > Highlight Source in Tree**.
  - For an alarm, select **Alarm Log > Actions > Highlight Source in Tree**.



The NetVoyant Console highlights the source of the event or alarm in the tree-tab panel on the **Group** tab.

**Note:** You can also view the name of the source of an event or alarm by double-clicking the log in the log panel to view the details of the event or alarm.

## Saving Log Files to a CSV File

You can save the event or alarm logs that appear in the log panels to a comma-separated values (CSV) file. When you save logs to a CSV file, each event or alarm occupies a separate line with event properties separated by commas.

For example:

```
Fri May 11 13:27:02 CDT 2007,Major,PING: Could not resolve device
slab03,Ping,0,TLAB51
```

```
Fri May 11 13:26:50 CDT 2007,Normal,Notification Service Starting,Notify,0,TLAB51
```

### To save an individual event or alarm to a CSV file:

1. View the alarm or event log panel in the NetVoyant Console.

For more information, see “Viewing the Log Panels” on page 209.



2. Select the event or alarm in the log panel.
3. Select one of the following from the **Logs** menu:
  - To save an event, select **Event Log > Save > Selected**.
  - To save an alarm, select **Alarm Log > Save > Selected**.
4. Select a location to which to save the file.
5. Enter a file name.
6. Click **Save**.

### To save all events or alarms from the log panels to a CSV file:

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels” on page 209](#).
2. Select one of the following from the **Logs** menu:
  - To save all events, select **Event Log > Save > All Events**.
  - To save all alarms, select **Alarm Log > Save > All Alarms**.
3. Select a location to which to save the file.
4. Enter a file name.
5. Click **Save**.

### To save all filtered events or alarms to a CSV file:

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels” on page 209](#).
2. Apply an event log filter to limit the events or alarms that appear in the log panels.  
For more information, see [“Filtering the Events and Alarms in the Log Panels” on page 221](#).
3. Select one of the following from the **Logs** menu:
  - To save the filtered events, select **Event Log > Save > Filtered**.
  - To save the filtered alarms, select **Alarm Log > Save > Filtered**.
4. Select a location to which to save the file.
5. Enter a file name.
6. Click **Save**.

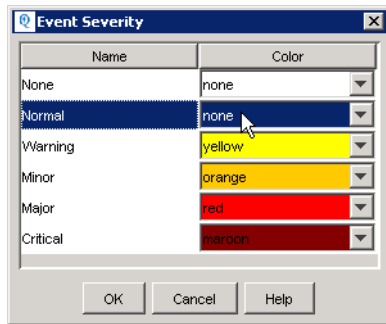
## Editing the Alarm Log Colors

The NetVoyant product color codes alarm logs and source devices in the NetVoyant Console according to each event’s severity. You can adjust the alarm log colors that it uses for each event severity to help you quickly identify the severity and source of events.

**Note:** Changing the color for an event severity affects only the alarm logs in the NetVoyant Console. Events displayed in the NetVoyant web reporting tool and the NetQoS Performance Center always use the default color indicators associated with the event severity.

**To edit the color of an event severity:**

1. On the **Logs** menu in the NetVoyant Console, select **Event Severity**.
2. Select the **Color** from the list next to the event severity that you want to adjust.



3. Click **OK**.

**Note:** If you do not see the colors change immediately in the alarm log panel, close and reopen the panel from the **View** menu.

## Acknowledging an Alarm

You can manually mark an alarm as over after you remedy the underlying fault by acknowledging the alarm. When you acknowledge an alarm, the NetVoyant product removes the alarm from the alarm log on the next polling cycle and immediately removes alarm log colors from the source device and poll instances in the tree-tab panel on the **Group** tab.

**Important:** Acknowledging an alarm does not delete the alarm from the database.

**Automatic Acknowledgement.** NetVoyant automatically acknowledges and clears threshold, polling, and SNMP trap alarms according to the following rules:

- A threshold alarm is cleared when the expression value drops below the threshold-cleared value.
- A polling alarm is cleared on the next successful polling cycle.
- An SNMP trap alarm is cleared when the clear filter for the trap event is met.

**To acknowledge an alarm:**

1. View the alarm or event log panel in the NetVoyant Console.

For more information, see [“Viewing the Log Panels” on page 209](#).

2. Select the **Ack** check box next to the alarm that you want to acknowledge.

The NetVoyant product clears the alarm log colors for the alarm and clears the alarm from the alarm log panel on the next polling cycle. You can also manually clear all acknowledged alarms from the alarm log panel.

**Note:** In a distributed NetVoyant system, you can acknowledge an alarm on either the Master or the poller. However, if you acknowledge an alarm on the Master server when the poller is down, the change is not synched when communication with the poller is restored. In this situation, you must also acknowledge the alarm on the poller.

## Clearing an Event or Alarm from the Log Panel

You can manually clear an event to remove the event from the event or alarm log and to mark the event as over. When you clear an event, the NetVoyant product removes the item from the event or alarm log, but does not delete the event from the database.

**Note:** Clearing an alarm does not remove the color designation from the source device and poll instances on the **Groups** tab. To remove the alarm color indicators, you must acknowledge the alarms.

**Automatic Clearing.** The NetVoyant product automatically acknowledges and clears threshold, polling, and SNMP trap events according to the following rules:

- A threshold event is cleared when the expression value drops below the threshold-cleared value.
- A polling event is cleared on the next successful polling cycle.
- An SNMP trap event is cleared when the clear filter for the trap event is met.

### To clear an individual event or alarm from the log panels:

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels” on page 209](#).
2. Select the event or alarm in the log panel.
3. Select one of the following from the **Logs** menu:
  - To clear an event, select **Event Log > Actions > Clear > Selected**.
  - To clear an alarm, select **Alarm Log > Actions > Clear > Selected**.

### To clear all events or alarms from the log panels:

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels” on page 209](#).
2. Select one of the following from the **Logs** menu:
  - To clear all events, select **Event Log > Actions > Clear > All Events**.
  - To clear all alarms, select **Alarm Log > Actions > Clear > All Alarms**.

### To clear all acknowledged alarms from the log panels:

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels” on page 209](#).
2. Acknowledge the alarms.
3. From the **Logs** menu, select **Alarm Log > Actions > Clear > Acknowledged**.

## Viewing Cleared Events or Alarms

After you clear events or alarms from the log panels, you can update their display in the log panels.

### To return events or alarms that you have cleared from the log panels:

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels” on page 209](#).
2. Select one of the following from the **Logs** menu:
  - To refresh the event log panel, select **Event Log > Actions > Refresh**.
  - To refresh the alarm log panel, select **Alarm Log > Actions > Refresh**.

## Deleting Events or Alarms from the Database

If you delete an event or alarm from the database, you can recover the event or alarm only from a database backup. Instead of deleting an event or alarm, you can clear the events or alarms from the log panels to no longer view them in the NetVoyant Console. For more information, see [“Clearing an Event or Alarm from the Log Panel” on page 219](#).

You can also acknowledge alarms to clear the alarm log colors on the **Groups** tab in the NetVoyant Console. For more information, see [“Acknowledging an Alarm” on page 218](#).

### To delete an individual event or alarm:

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels” on page 209](#).
2. Select the event or alarm in the log panel.
3. Select one of the following from the **Logs** menu:
  - To delete an event, select **Event Log > Actions > Delete > Selected**.
  - To delete an alarm, select **Alarm Log > Actions > Delete > Selected**.
4. Click **Yes** to confirm.

This removes the event or alarm from the database.

### To delete all events or alarms:

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels” on page 209](#).
2. Select one of the following from the **Logs** menu:
  - To delete all events, select **Event Log > Actions > Delete > All Events**.
  - To delete all alarms, select **Alarm Log > Actions > Delete > All Alarms**.
3. Click **Yes** to confirm.

This removes the events or alarms from the database.

**To delete all filtered events or alarms:**

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels” on page 209](#).
2. Apply an event log filter to limit the events or alarms that appear in the log panels.
3. Select one of the following from the **Logs** menu:
  - To delete the filtered events, select **Event Log > Actions > Delete > Filtered**.
  - To delete the filtered alarms, select **Alarm Log > Actions > Delete > Filtered**.
4. Click **Yes** to confirm.  
This removes the events or alarms from the database.

## Displaying Fewer Logs in the Log Panels

In order to make the number of displayed items more manageable, you can limit the number of event and alarm logs that appear in the log panels of the NetVoyant Console.

**Note:** You can also limit the event or alarm logs that appear by applying an event log filter to the event or alarm log panel.

**To limit the number of logs that appear in both log panels:**

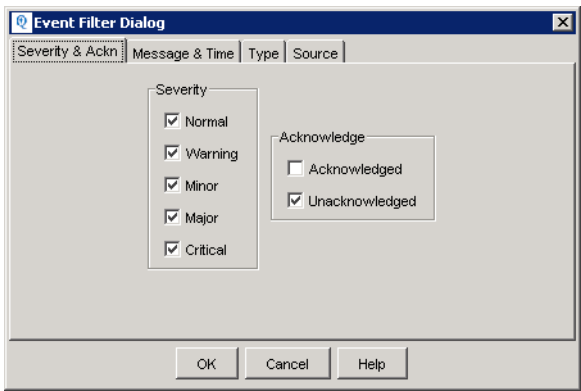
1. From the **Logs** menu, select **Event Log > Edit > Set Max Logs**.  
The **Max Log** dialog box opens.
2. Enter the number of logs that you want to display in the log panel.
3. Click **OK**.
4. Select one of the following from the **Logs** menu:
  - For the Events panel, select **Event Log > Actions > Refresh**.
  - For the Alarms panel, select **Alarm Log > Actions > Refresh**.

## Filtering the Events and Alarms in the Log Panels

You can limit the events or alarms that are visible in the log panels to those that meet the criteria in an event filter. This makes it easier to scan for the events and alarms that you want to see.

**To filter the events and alarms:**

1. View the alarm or event log panel in the NetVoyant Console.  
For more information, see [“Viewing the Log Panels” on page 209](#).
2. Select one of the following from the **Logs** menu:
  - To filter events in the event log panel, select **Event Log > Edit > Set Filters**.
  - To filter alarms in the alarm log panel, select **Alarm Log > Edit > Set Filters**.The **Event Filter** dialog box opens.



3. In the dialog box, apply an event log filter to the log panel by editing the settings on the following tabs:

Tab	Description
Severity & Ackn	<p>You can perform the following actions:</p> <ul style="list-style-type: none"><li>• Select an <b>Event Severity</b> check box to include events with the selected event severity on the log panel.</li><li>• Select the <b>Acknowledged</b> check box to include acknowledged alarms on the log panel. Clear this check box to remove them. (<i>Alarms only</i>)</li><li>• Select the <b>Unacknowledged</b> check box to include unacknowledged alarms on the log panel. Clear this check box to remove them. (<i>Alarms only</i>)</li></ul>
Message & Time	<p>Use this tab to restrict the displayed event logs to only those that have a selected message in the Description field or only those that occurred during a selected time period.</p> <ul style="list-style-type: none"><li>• Select the <b>Match message</b> check box and enter a message to view all events that have event descriptions that contain the entered text.</li><li>• Select the <b>Start date</b> check box to restrict the event logs shown to only those occurring after the entered date. Click the part of the date that you want to edit. Click the up or down arrows to edit that section of the date.</li><li>• Select the <b>End Date</b> check box to restrict the event logs shown to only those occurring before the entered date. Click the part of the date that you want to edit. Click the up or down arrows to edit that section of the date.</li></ul>

Tab	Description
<b>Type</b>	<p>Select or clear a <b>Type</b> check box to include or clear events of that event type on the log panel:</p> <ul style="list-style-type: none"> <li>• <b>Polling:</b> Polling events track the SNMP polls that are sent to your devices. A polling alarm occurs when a device does not respond to an SNMP request during a scheduled polling cycle.</li> <li>• <b>Trap:</b> Trap events track incoming SNMP traps. You can configure new trap events for the types of SNMP traps that you expect the NetVoyant product to receive. For more information, see <a href="#">“Adding or Editing an SNMP Trap Event” on page 325</a>.</li> <li>• <b>Threshold:</b> Threshold events track threshold violations on your devices. A threshold event occurs when a value for an expression goes above the threshold-exceeded value that you set for the expression.</li> </ul>
<b>Source</b>	<p>Select a <b>Source</b> check box to include events generated by that NetVoyant service on the log panel. Clear the check box to remove them.</p> <p>For more information, see <a href="#">“About the NetVoyant Services” on page 280</a>.</p>

4. Click **OK**.

This restricts the displayed event or alarm logs in the log panel to only those that match the event log filter that you defined.

## CONFIGURING EVENT SEVERITIES

The NetVoyant product assigns each event a severity that indicates the degree of seriousness of the underlying fault or action. The following are possible event severities:

Severity	Description
None	Events that are not recorded in the event or alarm logs.
Normal	Normal NetVoyant actions, including: services starting normally, successful SNMP polls, threshold events that you have assigned a normal event severity, and others.
Warning	Events with a slightly elevated severity above normal.
Minor	Events with a slightly elevated severity above warning.
Major	Events with a an elevated severity above minor.
Critical	Events with the highest severity.
Unavailable	Events resulting from polling failure due to unavailability. This is the default severity for polling events, which are triggered when a device is unavailable for polling.

Alarms are events that have an event severity that is not normal, which includes warning, minor, major, critical, and custom event severities. You can configure event severities to manage how you manage your NetVoyant events and alarms.

### Configuring Severities for Threshold Events

You can configure the event severity that is assigned to a threshold event and generate notifications based on the event severity by performing the following tasks:

Task	More information
Configure the event severity for an alarm rule.	<a href="#">“Defining an Alarm Rule” on page 199</a>
Create notifications based on event severity.	<a href="#">“Triggering Notifications by Event Severity” on page 247</a>

You can create notifications that are triggered based on the severity of an event. For example, you can send an email notification for a minor threshold event and send a numeric page for a major threshold event. For more information on creating notifications, see [“Creating a Notification” on page 227](#).



# Managing Notifications

---

Notifications enable you to notify yourself or team members of events that occur in your network. The NetVoyant product delivers notifications according to the event filters you configure in the NetVoyant Console, so that the NetVoyant product sends a selected notification only when events that meet your criteria occur. For example, you can create an event filter for an email notification where it sends you an email if utilization for an interface is over threshold for more than four hours.

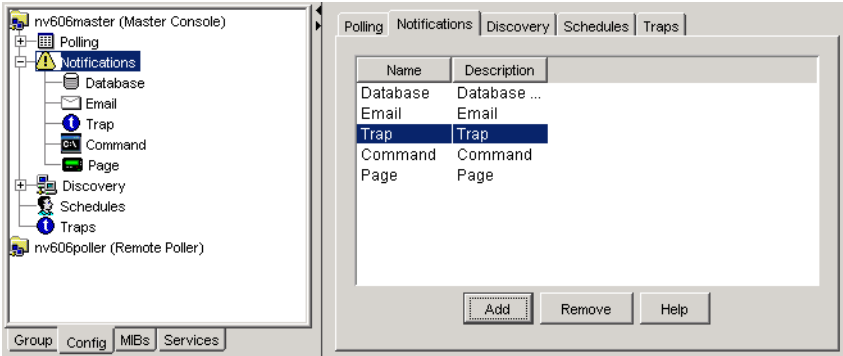
Notification configuration and management tasks take place in the NetVoyant Console on the **Config** tab.

This chapter covers the following topics:

- [“Using NetVoyant Notifications” on page 226](#)
- [“Selecting the Events that Trigger a Notification” on page 240](#)
- [“Triggering Notifications for Sustained Events” on page 248](#)

# USING NETVOYANT NOTIFICATIONS

To configure and manage notifications, go to the **Config** tab in the NetVoyant Console. Expand Notifications to view the notification items added, configure or remove existing notifications, or add new ones.



## Notification Types

The NetVoyant product can deliver the following types of notifications:

Type	Description	More information
Database logging	Database notifications are configured by default. The default database notification logs all non-normal events to the database enabling you to view them in the event and alarm logs and in service exception reports.	<a href="#">“Database Notifications” on page 227</a>
Email	When an event occurs that matches your filtering criteria, an email is sent according to your specifications.	<a href="#">“Configuring Email Notifications” on page 231</a>
Numeric pages	When an event occurs that matches your filtering criteria, a numeric page is sent according to your specifications.	<a href="#">“Configuring Numeric Page Notifications” on page 232</a>
SNMP traps	When an event occurs that matches your filtering criteria, an SNMP trap is sent according to your specifications.	<a href="#">“Configuring SNMP Trap Notifications” on page 233</a>
Command line commands	When an event occurs that matches your filtering criteria, the command is executed according to your specifications.	<a href="#">“Configuring Command Line Notifications” on page 236</a>

## Database Notifications

The default database notification logs all non-normal events to the database enabling you to view them in the event and alarm logs and in exception reports.

**Warning:** We recommend that you do not remove, edit, or add database notifications.

By default, the database notification is configured with the following event filter expression:

```
$EventSeverity != 'Normal'
```

This event filter logs all non-normal events to the database.

## Creating a Notification

Creating a new notification involves specifying the notification type and using an expression to further define the event that triggers the notification.

### To create a notification:

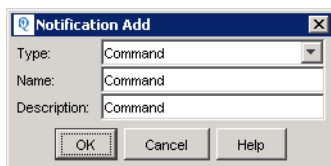
1. On the **Config** tab in the NetVoyant Console, expand the Master server or poller.

2. Click **Notifications**.

The list of existing notifications appears in the context panel.

3. Click **Add** in the context panel.

The **Notification Add** dialog box opens.



4. Enter the following parameters:

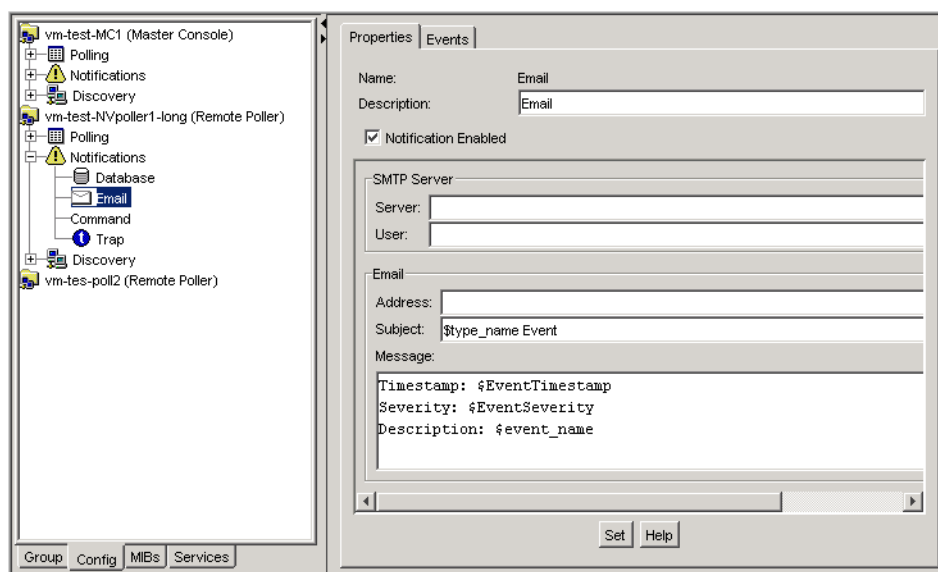
Parameter	Description
<b>Type</b>	Select one of the following types: <ul style="list-style-type: none"> <li>• Command</li> <li>• Email</li> <li>• Page</li> <li>• Trap</li> </ul> For more information, see <a href="#">“Using NetVoyant Notifications”</a> on page 226.
<b>Name</b>	Enter a name to help you identify the notification.
<b>Description</b>	Enter a description to help you identify the purpose of the notification.

5. Click **OK**.

This adds the notification to the list of existing notifications.

6. In the tree tab panel, expand **Notifications** and select the new notification.

The properties for the notification appear in the context panel.

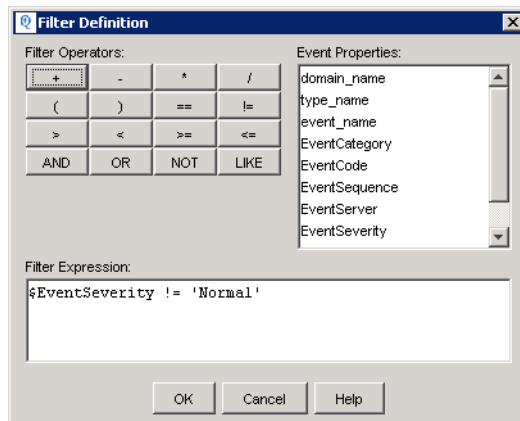


7. On the **Properties** tab of the context panel, edit the configuration parameters for the notification.  
For more information, see “[Notification Configuration Parameters](#)” on page 230.
8. Click **Set**.
9. Click the **Events** tab in the context panel.  
The event filters display. For a new notification, no event filters are defined.
10. Select **Subscribed** next to the type of events for which you want to be able to trigger a notification.  
You can select one or more of the following event types for an event filter:

Event type	Description
<b>Log</b>	Log events track actions that NetVoyant services perform along with topology changes in your network or devices. Configure an event filter for the Log event type to trigger a notification when the NetVoyant product experiences any event of a selected event severity.
<b>Trap</b>	Trap events track incoming SNMP traps. Configure an event filter for the Trap event type to trigger a notification when an SNMP trap of a selected type is received.
<b>Threshold</b>	Threshold events track threshold violations on your devices. A threshold event occurs when a value for an expression goes beyond a limit defined in an alarm rule associated with the device. Configure an event filter for the Threshold event type to trigger a notification when an expression value triggers a defined threshold in an alarm profile assigned to the device. For example, you can trigger a notification when interface utilization ( <code>ifutil</code> ) goes above a 75% threshold.
<b>Polling</b>	Polling events track the SNMP polls sent to your devices. Polling alarms indicate that a device did not respond to an SNMP request during a scheduled polling cycle. Configure an event filter for the Polling event type to trigger a notification when the NetVoyant product fails to poll a device because it is unavailable.

11. Select a subscribed event type and click **Change** to edit the event filter expression.

The **Filter Definition** dialog box opens.



12. Enter the **Filter Expression**.

You can use any expression names, NetVoyant operators, or notification or event properties in your event filters.

For more information on how to write an event filter, see [“Writing an Event Filter Expression”](#) on page 241. For a list of example event filters, see [“Examples for Using Notifications”](#) on page 237.

13. Click **OK**.

14. Enable the notification by selecting **Notification Enabled** on the **Properties** tab for the notification.

15. Click **Set**.

The NetVoyant product sends the notification according to your configuration whenever a subscribed event occurs and the event meets the filter requirements.

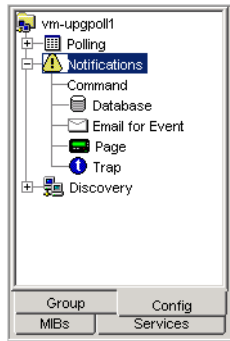
## Enabling or Disabling a Notification

You can have different notifications of different types defined in the NetVoyant product. Defined notifications can be enabled or disabled, depending on your current needs. By default, a new notification is not enabled until you enable it in the **Properties** tab.

### To enable or disable a notification:

1. On the **Config** tab in the NetVoyant Console, expand the NetVoyant poller.
2. Expand **Notifications**.

The list of existing notifications appears below **Notifications**.



3. Select the notification in the list under **Notifications**.

The notification's properties appear in the context panel.

4. Perform one of the following actions on the notification's **Properties** tab in the context panel:

- To enable a notification, select the **Notification Enabled** check box.

The NetVoyant product begins sending the notification according to its configuration.



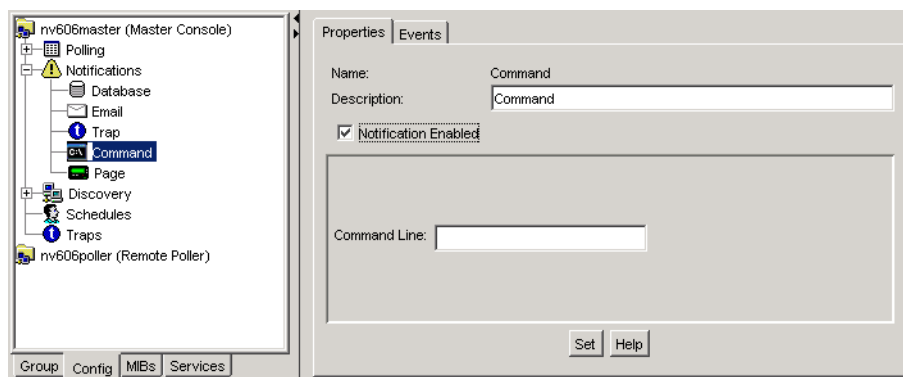
- To disable a notification, clear the **Notification Enabled** check box.

The NetVoyant product stops sending the notification.

5. Click **Set**.

## Notification Configuration Parameters

Use the **Properties** tab to configure the parameters for a notification. After you create a notification, it appears in the **Config** tab under Notifications. Select the notification to see its details in the context panel and make changes to the notification properties. The parameters that you set depend on the notification type.



Use the **Notification Enabled** check box to enable or disable the configured notification type.

The following sections describe the parameters you must configure for each type.

## Configuring Email Notifications

An email notification instructs the NetVoyant product to send an email when an event occurs that matches your filtering criteria. Configuring this notification type involves designating an SMTP server for sending the email, the email destination addresses, and the contents of the message.

**Note:** We recommend that you create at least one email notification to alert an administrator if NetVoyant data collection is interrupted.

Parameter	Description
<b>Server</b>	Enter the name or IP address of the SMTP server that routes email notifications.
<b>User</b>	Enter the email address that you want to use as the From address for emails sent as part of this notification.
<b>Address</b>	Enter the email addresses of the people that you want to receive the notification. Separate multiple addresses using commas. For example, you might specify the following list of recipients:  me@company.com, myboss@company.com, hisboss@company.com
<b>Subject</b>	Enter the text that you want to use as the Subject line in the emails sent as part of this notification. The default value is <code>\$type_name Event</code> .  <code>\$type_name</code> is a property that is resolved to the type of event that triggers the notification when it sends the notification email.  As an example, the subject line for an email triggered by a threshold event would be "Threshold Event." Add or remove words or properties from the subject line.  Notification properties are resolved when the notification email is sent.

Parameter	Description
<b>Message</b>	<p>Enter the text that you want to include as the body of the emails that the NetVoyant product sends as part of this notification.</p> <p>The default value is:</p> <pre>Timestamp: \$EventTimestamp Severity: \$EventSeverity Description: \$event_name</pre> <ul style="list-style-type: none"> <li>• <code>\$EventTimestamp</code> is a property that is resolved to the time that the event occurred when it sends the notification email.</li> <li>• <code>\$EventSeverity</code> is a property that is resolved to the event severity level of the event when it sends the notification email.</li> <li>• <code>\$event_name</code> is a property that is resolved to the description of the event when it sends the notification email.</li> </ul> <p>As an example, the message for an email triggered by a threshold event could be:</p> <pre>Timestamp: Tue May 08 04:25:07 CDT 2007 Severity: Minor Description: Threshold exceeded for 10.0.7.10:1 (in_discardrate = 45.312500)</pre>

**Troubleshooting Email Notifications with Verbose Logging.** If you have difficulty delivering email notifications from the NetVoyant product, you can use logs from the Notify service to help you troubleshoot the problem. For more information, see [“Configuring a Service’s Start Mode or Logging Level” on page 283](#).

## Configuring Numeric Page Notifications

A numeric page notification instructs the NetVoyant product to send a numeric page when an event that matches the filtering criteria occurs. Configuring this notification type involves specifying a modem port for sending the page, the pager number, and transmission details.

The screenshot shows a configuration window with the following details:

- Properties** | **Events** (selected)
- Name:** Page
- Description:** Page
- ☐ Notification Enabled
- Modem Port:** COM2
- Pager Number:** (empty field)
- Pause (secs):** 4
- Callback Number:** (empty field)
- Quiet Period (secs):** 300
- Buttons:** Set, Help



Parameter	Description
<b>Modem Port</b>	The port on which your modem is configured.
<b>Pager Number</b>	The phone number to which you want to send numeric pages as part of this notification. Enter one phone number per numeric page notification. If you need to page more than one number, you must create a new numeric page notification for each phone number.
<b>Pause</b>	The amount of time in seconds to wait after the pager answers before it transmits the Callback Number.
<b>Callback Number</b>	The transmitted code that is sent to the pager when the notification is triggered. For example, you could enter 911 to indicate that a mission-critical server is not operational.
<b>Quiet Period</b>	The length of time in seconds to wait after transmitting a page as part of this notification before sending an additional page as part of this notification. The NetVoyant product sends another page only if another event matches the event filter to trigger the notification. It does not repeat pages for the same event.

## Configuring SNMP Trap Notifications

An SNMP trap notification instructs the NetVoyant product to send an SNMP trap when an event occurs that matches the filtering criteria. Configuring this notification type involves designating SNMP v1, v2, or v3 encoding and variable bindings to include in the trap.


The screenshot shows the 'Events' tab of the 'Properties' dialog box. The 'Name' field is set to 'Trap' and the 'Description' field is also 'Trap'. The 'Notification Enabled' checkbox is unchecked. The 'Trap' section contains the following fields:

- Destination:** 10.6.7.34
- Profile:** public (dropdown menu)
- Encoding:** Radio buttons for SNMPv1, **SNMPv2C** (selected), and SNMPv3.
- Type:** NETVOYANT\_MIB.netvoyant (dropdown menu with an ellipsis button)

The 'Variable Bindings' section displays a table with two columns: 'OID' and 'Value'.

OID	Value
NETVOYANT_MIB.eventCategory	\$EventCategory
NETVOYANT_MIB.eventCleared	\$EventCleared
NETVOYANT_MIB.eventDataset	\$Dataset
NETVOYANT_MIB.eventDescription	\$event_name
NETVOYANT_MIB.eventDevice	\$Device
NETVOYANT_MIB.eventDuration	\$EventDuration
NETVOYANT_MIB.eventExpressionName	\$ExpressionName
NETVOYANT_MIB.eventExpressionValue	\$ExpressionValue

Below the table are buttons for 'Add', 'Remove', 'Raise', and 'Lower'. At the bottom of the dialog are 'Set' and 'Help' buttons.

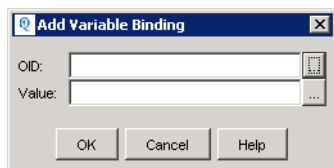
Parameters	Description
<b>Trap</b>	<p>You can edit the following parameters for the trap:</p> <ul style="list-style-type: none"> <li>• <b>Destination</b> - Enter the Destination network address or name. Use commas to separate multiple destinations.</li> <li>• <b>Profile</b> - Enter the SNMP profile for the destination of the trap.</li> <li>• <b>Encoding</b> - Select the SNMP Version for the trap. This is the version of SNMP used to generate the trap.</li> <li>• <b>Type</b> - Indicates the type of trap being sent to the receiving SNMP agent. For a NetVoyant trap, it sets this to <code>\$type_name</code> by default. To locate and select an SNMP object identifier (OID) to identify the enterprise or network management entity that you want to generate the trap., click  to open the <b>SNMP Identifiers</b> dialog box.</li> </ul> <p><b>Note:</b> The NetVoyant product sets type to an appropriate value for you. Typically, you do not need to configure this field.</p>
<b>Variable Bindings</b>	<p>Add or remove Variable Bindings that you want to include in the trap. The OID represents the name of the field and the value is the value that NetVoyant sends for each field.</p> <p>The order that the OIDs are listed is the order in which they are saved. Use the <b>Raise</b> and <b>Lower</b> buttons to specify the order for event management systems.</p> <p>For more information about variable bindings, see <a href="#">“Using Variable Bindings” on page 330</a>.</p>


### Including Device Names and Properties in SNMP Trap Messages

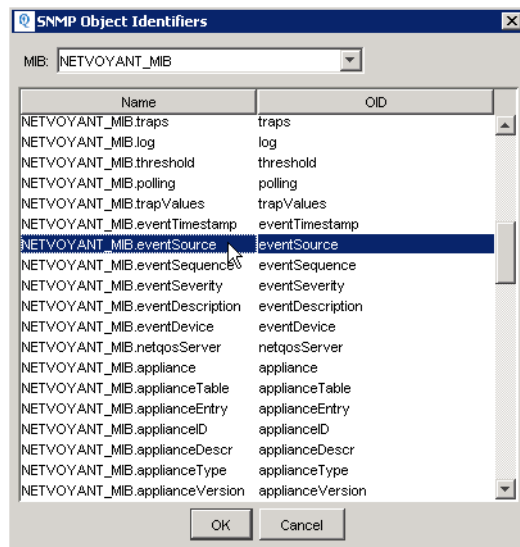
You can pass the name or IP address of a device, as well as other device information, in an SNMP trap message sent by the NetVoyant product. This can be useful when generating dynamic URLs so that your SNMP trap management agent can directly contact a device that is experiencing difficulty.

### To include device property information in an SNMP Trap Message:

1. Under **Variable Bindings**, click **Add**.



2. Next to the OID field in the **Add Variable Binding** dialog box, click . The **SNMP Object Identifiers** dialog box opens.
3. From **MIB** drop-down list, select **NETVOYANT\_MIB**.
4. From the list of OIDs in the **NETVOYANT\_MIB**, select **NETVOYANT\_MIB.eventSource**.



5. Click **OK**.
6. In the **Add Variable Binding** dialog box, enter a device or poll instance property with or without an attribute for the **Value** according to the following syntax types:

`$DeviceAttribute/<attr>`

`$PollInstanceAttribute/<attr>`

`$PollInstanceProperty/<property-name>`

These value definitions are very case sensitive except for the `<attr>`, which simply names a database field in either devices or pollinst. The `<property-name>` must be the exact property name, but property names with spaces are not currently supported. The following are some examples:

`$DeviceAttribute/dev_alias`

`$DeviceAttribute/sys_descr`

`$PollInstanceAttribute/pollinst_descr`

`$PollInstanceAttribute/pollinst_ior`

`$PollInstanceProperty/Description`

**Note:** Values are not mapped to anything, such as `dev_class` to a device class name or `pollinst_enabled` to a meaningful string; only a number is returned.

7. Click **OK**.
8. Continue configuring the SNMP trap notification.

If the NetVoyant product sends an SNMP trap notification of this type, it sends the device name or IP address of the device that initiated the event as the value for the eventSource OID.

## Configuring Command Line Notifications

A command line notification instructs the NetVoyant product to run a specified command when an event occurs that matches the filtering criteria. You can use this feature to run a script or an application that performs a corrective action whenever a selected type of event occurs. Configuring this notification type involves specifying the command to execute.

The screenshot shows a 'Properties' dialog box with an 'Events' tab. The 'Name' field is set to 'Command'. The 'Description' field contains the text 'Execute command to Telnet'. There is an unchecked checkbox labeled 'Notification Enabled'. Below this is a large text area for the 'Command Line' which is currently empty. At the bottom right are 'Set' and 'Help' buttons.

Parameter	Description
<b>Command Line</b>	Enter the command you want to execute when the notification is triggered. For example, you could enter the following command: <code>Telnet_script_a.bat \$PollInstance \$ExpressionName</code> This command runs a script called <code>Telnet_script_a.bat</code> that a user created to access Telnet and input two NetVoyant property values from the event.

## Configuring Database Logging Notifications

If you are troubleshooting events and notifications, it can be helpful to change the event logging to log all event notifications in the database. This produces another copy of the default logging channel to the database.

The screenshot shows a 'Properties' dialog box with an 'Events' tab. The 'Name' field is set to 'Database'. The 'Description' field contains the text 'Database Logging'. There is a checked checkbox labeled 'Notification Enabled'. Below this is a large empty text area. At the bottom right are 'Set' and 'Help' buttons.

There are no specific parameters to set for database logging notifications. Use the **Events** tab to specify the event filters that determine the event log items that generate a notification. For more information about using event filters, see [“Writing an Event Filter Expression”](#) on page 241.

## Examples for Using Notifications

The NetVoyant product delivers notifications according to the event filters you configure. You create expressions called event filters to specify events or alarms on which you want it to notify.

For example, you could create an event filter for an email notification where the NetVoyant product sends you an email if utilization for an interface is over threshold for more than four hours. For more information about event filters, see [“Selecting the Events that Trigger a Notification”](#) on page 240.

**Note:** Many of these examples use the interface utilization (`ifutil`) expression for threshold violation notifications. You can easily replace the `$ExpressionName` property value with another expression name to notify on other threshold violations.

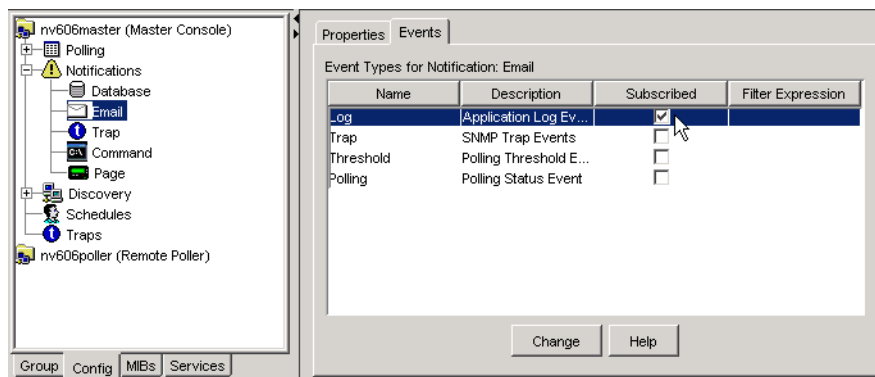
### Creating an Administrative Email Notification

The example administrative email notification described in this topic sends an email whenever the NetVoyant product experiences an event that has an event severity of Critical from any source or an event severity of Major from any source except the NetVoyant Topology service.

We recommend that you do not notify on major Topology events because these events do not usually affect NetVoyant data collection; however, major Poll and Threshold events could indicate that the NetVoyant product is not able to gather data and should be investigated.

#### To send an email for a major non-topology event or any critical event:

1. Create an email notification.  
For more assistance with this step, see [“Creating a Notification”](#) on page 227.
2. While configuring the email notification, enter an email address that a NetVoyant administrator checks regularly.
3. On the **Events** tab for the email notification, select the **Subscribed** check box for the Log event type.



4. Click **Change** or double-click the **Filter Expression** for the Log event type.  
The **Filter Definition** dialog box opens.
5. Enter the following filter expression:  

```
($EventSeverity == Major
AND $EventSupplier != Topology)
```

```
OR $EventSeverity == Critical
```

For more assistance with creating an event filter, see [“Writing an Event Filter Expression” on page 241](#).

**6. Click OK.**

The NetVoyant product sends an email notification to the NetVoyant administrator when it experiences a major non-Topology event or any critical event.

### Other Notification Examples

The following examples show how you can use notifications, as well as the event filters you must use to configure each notification.

**Example One.** Interface utilization, error rate, or discard rates are beyond the threshold limitation for an interface and have not yet cleared (returned below the threshold-cleared value).

Enter the following event filter for the Threshold event type:

```
$ExpressionName == ifutil
OR $ExpressionName == errorrate
OR $ExpressionName == discardrate
AND $EventCleared == 0
```

For more information, see [“Triggering Notifications for a Threshold Event” on page 243](#).

**Example Two.** A selected device has become unavailable.

Enter the following event filter for the Polling event type:

```
$Device == '10.0.7.7'
AND $Dataset == 'avail'
```

For more information, see [“Triggering Notifications by Device Availability” on page 242](#).

**Example Three.** A device’s interface utilization has gone beyond the threshold limitation during working business hours (8:00 a.m. to 5:00 p.m.) and has not yet cleared.

Enter the following event filter for the Threshold event type:

```
$ExpressionName == ifutil
AND HOURS($EventTimestamp) >= 8
AND HOURS($EventTimestamp) <= 17
AND $EventCleared == 0
```

For more information, see [“Triggering Notifications by Event Timestamp” on page 246](#).

**Example Four.** A device’s interface utilization has been over the threshold for over an hour and has not yet cleared.

Enter the following event filter for the Threshold event type:

```
$ExpressionName == ifutil
AND $EventDuration > 3600 - 50
AND $EventDuration < 3600 + 50
```

```
AND $EventCleared == 0
```

For more information, see [“Triggering Notifications for Sustained Events”](#) on page 248.

**Example Five.** Utilization for an interface that was over a threshold has cleared (gone back below the threshold cleared value).

Enter the following event filter for the Threshold event type:

```
$ExpressionName == 'ifutil'
AND $EventCleared > 0
```

For more information, see [“Triggering Notifications for Sustained Events”](#) on page 248.

**Example Six.** NetVoyant receives an SNMP Trap from a PBX source.

PBX SNMP trap suppliers have a device in the following range of IP addresses: 207.200.0.0 to 207.201.0.0.

Enter the following event filter for the Trap event type:

```
$Device > 207.200
AND $Device < 207.201
```

For more information, see [“Triggering Notifications by Device Name or Address”](#) on page 244.

**Example Seven.** NetVoyant receives an SNMP Trap from a non-PBX source.

PBX SNMP trap suppliers have an event supplier value that is in the following range of IP addresses: 207.200.0.0 to 207.201.0.0.

Enter the following event filter for the Trap event type:

```
$EventSupplier < 207.200
OR $EventSupplier > 207.201
```

For more information, see [“Triggering Notifications by Device Name or Address”](#) on page 244.

**Example Eight.** A threshold event occurs on a device in the following range of IP addresses: 192.168.0.0 to 192.168.1.0.

Enter the following event filter for the Threshold event type:

```
$Device > 192.168.0
AND $Device < 192.168.1
```

For more information, see [“Triggering Notifications by Device Name or Address”](#) on page 244.

**Example Nine.** A threshold event occurs on a WAN interface.

The dsx1near and dsx3near datasets collect interface statistics for T1 and T3 interfaces, respectively.

Enter the following event filter for the Threshold event type:

```
$Dataset == dsx1near
OR $Dataset == dsx3near
```

For more information, see [“Triggering Notifications for a Threshold Event”](#) on page 243.

**Example Ten.** An interface has changed operational status and you want to be notified immediately.

Enter the following event filter for the Threshold event type:

```
$ExpressionName == opstatus
AND $EventDuration == 0
```

For more information, see [“Triggering Notifications by Operational Status”](#) on page 243.

## SELECTING THE EVENTS THAT TRIGGER A NOTIFICATION

The NetVoyant product delivers notifications according to the event filters you configure in the NetVoyant Console. An event filter is an expression that specifies the events or alarms on which you want the NetVoyant product to notify.

For example, you could create an event filter for an email notification where the NetVoyant product sends you an email if utilization for an interface is over threshold for more than four hours.

The following are ways you can use event filters to trigger notifications for a selected circumstance:

Example	More information
A selected device has become unavailable.	<a href="#">“Triggering Notifications by Device Availability”</a> on page 242
An interface has changed operational status and you want immediate notification.	<a href="#">“Triggering Notifications by Operational Status”</a> on page 243
Interface utilization, error rate, or discard rates are over threshold for an interface and have not yet cleared (returned below the threshold-cleared value).	<a href="#">“Triggering Notifications for a Threshold Event”</a> on page 243
A threshold event occurs on a selected device.	<a href="#">“Triggering Notifications by Device Name or Address”</a> on page 244
NetVoyant receives an SNMP Trap from a selected IP address	<a href="#">“Triggering Notifications for Incoming SNMP Traps”</a> on page 246
A device’s interface utilization has gone over threshold during working business hours (8:00 a.m. to 5:00 p.m.) and has not yet cleared.	<a href="#">“Triggering Notifications by Event Timestamp”</a> on page 246
A device’s interface utilization has been over threshold for over an hour and has not yet cleared.	<a href="#">“Triggering Notifications for Sustained Events”</a> on page 248
An alarm occurs with a ‘Critical’ event severity.	<a href="#">“Triggering Notifications by Event Severity”</a> on page 247
An escalated threshold event occurs for which you want to send an escalated notification.	<a href="#">“Triggering Escalated Notifications by Event Severity”</a> on page 247



## Writing an Event Filter Expression

The NetVoyant product delivers notifications according to the event filters you configure in the NetVoyant Console. An event filter is an expression that specifies events or alarms on which you want the NetVoyant product to notify.

Event filters enable you to configure the NetVoyant product to send a selected notification only when events that meet your criteria occur. For example, you can create an event filter for an email notification where it sends you an email if utilization for an interface is over threshold for more than four hours.

**Note:** For examples of commonly used event filters, see [“Examples for Using Notifications” on page 237](#).

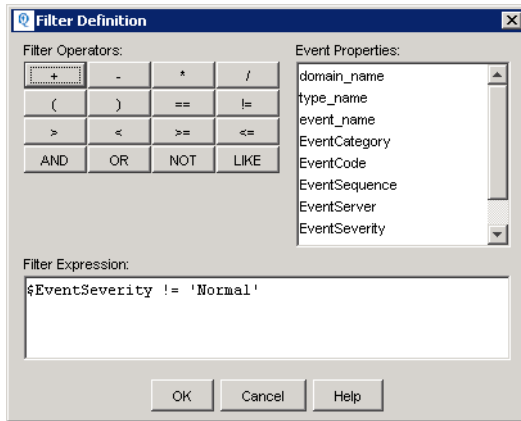
Event filters consist of two parts: the event type and the event filter expression.

**Event type.** The type of event to which you want to subscribe for the notification. You can select one or more of the following event types:

- **Log** - These events track actions that NetVoyant services perform along with topology changes in your network or devices. Configure an event filter for the Log event type to trigger a notification when any event of a selected event severity occurs.
- **Trap** - These events track incoming SNMP traps. Configure an event filter for the Trap event type to trigger a notification when the NetVoyant product receives an SNMP trap of a particular type.
- **Threshold** - These events track threshold violations on your devices. A threshold event occurs when a value for an expression goes beyond a threshold limitation value that you set for the alarm rule. Configure an event filter for the Threshold event type to trigger a notification when an expression value crosses a threshold. For example, you can trigger a notification when interface utilization (`ifutil`) goes above a 75%.
- **Polling** - These events track the SNMP polls that NetVoyant sends to your devices. Polling alarms indicate that a device did not respond to an SNMP request during a scheduled polling cycle. Configure an event filter for the Polling event type to trigger a notification when the NetVoyant product fails to poll a device because it is unavailable.

**Event filter expression.** An expression that can be evaluated as true or false for a given event.

When an event occurs, the Notify service evaluates whether the existing notifications' event filter expressions are true for the event. If an event filter expression is true for an event, it sends the selected notification according to how it was configured.



Event filter expressions can include the following:

- Notification properties. For example, `$ExpressionName` or `$EventSeverity`.
- Notification property values. For example, `ifutil`, which is an expression name, or `Critical`, which is an event severity.
- NetVoyant operators. For example, `AND` or `>=`

For more information see [“Using Properties in Notifications”](#) on page 309 and [“Using NetVoyant Operators in Expressions”](#) on page 319.

## Triggering Notifications by Device Availability

Use the Device Availability dataset to configure the NetVoyant product to notify you when any device becomes unavailable.

### To create a notification for device availability:

1. Create a notification of the appropriate type.  
For more assistance with this step, see [“Creating a Notification”](#) on page 227.
2. On the **Events** tab for the notification, select the **Subscribed** check box for the Polling event type.
3. Click **Change** or double-click the **Filter Expression** for the event type.

The **Filter Definition** dialog box opens.

4. Enter the following Filter Expression:

```
$Dataset == 'avail'
```

For more assistance with creating an event filter, see [“Writing an Event Filter Expression”](#) on page 241.

5. Click **OK**.

The NetVoyant product sends notifications according to your configuration when any device becomes unavailable.

## Triggering Notifications by Operational Status

You can configure the NetVoyant product to notify you immediately when any interface changes operational status.

### To create a notification for operational status:

1. Create a notification of the appropriate type.  
For more assistance with this step, see [“Creating a Notification” on page 227](#).
2. On the **Events** tab for the notification, select the **Subscribed** check box for the Threshold event type.
3. Click **Change** or double-click the **Filter Expression** for the event type.

The **Filter Definition** dialog box opens.

4. Enter the following Filter Expression:

```
$ExpressionName == opstatus  
AND $EventDuration == 0
```

For more assistance with creating an event filter, see [“Writing an Event Filter Expression” on page 241](#).

5. Click **OK**.

The NetVoyant product sends notifications according to your configuration when any interface changes its operational status.

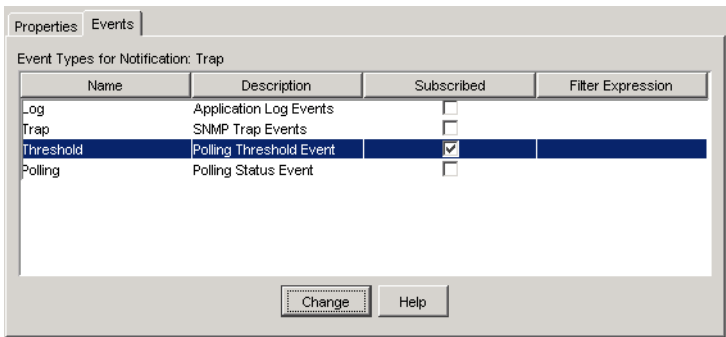
## Triggering Notifications for a Threshold Event

You can configure the NetVoyant product to notify you when it polls data that triggers a threshold in an alarm profile assigned to the device.

**Note:** You can delay notifications for a threshold event until the expression has been over threshold for a selected length of time. For example, you can create a notification that is triggered only after interface utilization has been above threshold for more than two hours. For more information, see [“Triggering Notifications for Sustained Events” on page 248](#).

### To create a notification for a threshold event:

1. Create a notification of the appropriate type.  
For more assistance with this step, see [“Creating a Notification” on page 227](#).
2. On the **Events** tab for the notification, select the **Subscribed** check box for the Threshold event type.



- 3. Click **Change** or double-click the **Filter Expression** for the event type.  
The **Filter Definition** dialog box opens.
- 4. Enter the following Filter Expression:  
`$ExpressionName == 'ExpressionName'`  
where `ExpressionName` is the name of the expression on which you want to notify. For example, `ifutil` to notify on interface utilization.  
**Note:** You can also filter based on alarm profile and alarm rule.  
For more assistance with creating an event filter, see [“Writing an Event Filter Expression” on page 241](#).
- 5. Click **OK**.  
The NetVoyant product sends notifications according to your configuration when a threshold event is triggered.

## Triggering Notifications by Device Name or Address

By editing the event filter for a notification to filter based on the device that initiated an event, you can configure the NetVoyant product to notify you about events that occur on selected devices.

You can configure notifications for an event occurrence on one of the following:

Event occurs on...	Event filter
A selected device.	<p>To configure an event filter to be triggered only for a selected device, add the following to the event filter:</p> <pre>AND \$Device == 'DeviceName'</pre> <p>where <code>DeviceName</code> is the name of the device.</p> <p>For example, the following event filter expression is triggered when the 10.0.7.7 device becomes unavailable.</p> <pre>\$Dataset == 'avail'</pre> <pre>AND \$Device == '10.0.7.7'</pre>

Event occurs on...	Event filter
A range of IP addresses.	<p>To configure an event filter to be triggered only for devices in a selected IP address range, add the following to the event filter:</p> <pre>AND \$Device &gt; 'IPrangeStart' AND \$Device &lt; 'IPrangeEnd'</pre> <p>where:</p> <ul style="list-style-type: none"> <li>• <code>IPrangeStart</code> is just less than the first address in the range of IP addresses.</li> <li>• <code>IPrangeEnd</code> is just greater than the last address in the range of IP addresses.</li> </ul> <p>For example, the following event filter expression is triggered when any device in the 10.0.0.0 to 10.0.1.0 IP address range becomes unavailable.</p> <pre>\$Dataset == 'avail' \$Device &gt; 10.0.0 AND \$Device &lt; 10.0.1</pre>
An alphabetical range of device names.	<p>To configure an event filter to be triggered only for devices with a name within a selected alphabetical range, add the following to the event filter:</p> <pre>AND \$Device &gt; 'NameRangeStart' AND \$Device &lt; 'NameRangeEnd'</pre> <p>where:</p> <ul style="list-style-type: none"> <li>• <code>NameRangeStart</code> starts with letters that are earlier alphabetically than the first device name in the range of device names.</li> <li>• <code>NameRangeEnd</code> starts with letters that are later alphabetically than the last device name in the range of device names.</li> </ul> <p>For example, the following event filter expression is triggered when any device that begins with QA becomes unavailable.</p> <pre>\$Dataset == 'avail' \$Device &gt; QA AND \$Device &lt; QB</pre> <p>The devices QA-switch and QA-101 would both trigger this notification. The device QB-101 would not trigger this notification.</p>

**Note:** For more assistance with creating an event filter, see [“Writing an Event Filter Expression”](#) on page 241.

## Triggering Notifications for Incoming SNMP Traps

You can configure the NetVoyant product to notify you when it receives incoming SNMP traps. You can configure these notifications to notify differently according to different trap types or sources or according to other event properties.

**Note:** Although there are trap events defined by default for standard SNMP traps, we recommend that you add and define trap events in the NetVoyant Console for the SNMP traps that you expect your devices to send. This enables you to configure the NetVoyant product to send notifications when it receives a selected type of SNMP trap. For more information, see [“Adding or Editing an SNMP Trap Event” on page 325](#).

### To create a notification for incoming SNMP traps:

1. Create a notification of the appropriate type.  
For more assistance with this step, see [“Creating a Notification” on page 227](#).
2. On the **Events** tab for the notification, select the **Subscribed** check box for the Trap event type.
3. Click **Change** or double-click the **Filter Expression** for the Trap event type.

The **Filter Definition** dialog box opens.

4. Create a Filter Expression to define what type of trap events trigger the notification.

For example, to create a notification that is triggered when the event severity for a trap event is critical, enter the following:

```
$EventSeverity == 'Critical'
```

For more assistance with creating an event filter, see [“Writing an Event Filter Expression” on page 241](#).

5. Click **OK**.

The NetVoyant product sends notifications according to your configuration when trap events meet your filter expression.

## Triggering Notifications by Event Timestamp

Configure the NetVoyant product to notify you about those events that occur during a given time period by editing a notification's event filter so that filtering is based on the event time stamp.

### To configure an event filter using the event timestamp:

- Add the following to the event filter:

```
AND HOURS($EventTimestamp) >= Begin
```

```
AND HOURS($EventTimestamp) <= End
```

where:

- **Begin** is the beginning hour of the time for which you want to notify. For example, to notify for events occurring after 8:00 a.m., enter 8.
- **End** is the ending hour of the time for which you want to notify. For example, to notify for events occurring before 5:00 p.m., enter 17.

**Note:** `EventTimestamp` is a property that equals the time at which the event occurred. The `HOURS` function evaluates the timestamp to an hourly numeric value between 0 and 24.

**Example.** You can enter the following event filter for the Threshold event type to trigger a notification when an interface utilization (`ifutil`) threshold event occurs between 8:00 a.m. and 5:00 p.m.:

```
$ExpressionName == ifutil
AND HOURS($EventTimestamp) >= 8
AND HOURS($EventTimestamp) <= 17
```

**Note:** For more assistance with creating an event filter, see [“Writing an Event Filter Expression”](#) on page 241.

## Triggering Notifications by Event Severity

Configure the NetVoyant product to notify you about events of a specific severity by editing a notification’s event filter so that filtering is based on the event severity.

### To configure an event filter to be triggered for a specified event severity:

- Add the following to the event filter:

```
AND $EventSeverity == 'SeverityName'
```

where `SeverityName` is the name of the event severity.

**Note:** You do not need to use a Boolean `AND` if you are filtering using only event severity.

**Example.** You can enter the following event filter for the Threshold event type to trigger a notification when a Critical threshold event occurs:

```
$EventSeverity == 'Critical'
```

**Note:** For more assistance with creating an event filter, see [“Writing an Event Filter Expression”](#) on page 241.

## Triggering Escalated Notifications by Event Severity

Configure the NetVoyant product to notify you differently according to the severity level of the event by editing a notification’s event filter so that filtering is based on the severity of an event. This enables you to escalate an event appropriately by sending a notification to a different team or in a different format.

### To create escalated notifications based on custom event severities:

1. Configure the expression to have multiple thresholds.  
For more information, see [“Using Thresholds to Trigger Events”](#) on page 204.
2. Configure a notification to be triggered for each escalated event severity triggered by the expression name and event severity.

For example, enter the following event filter for the Threshold event type to trigger a notification when a Critical interface utilization (ifutil) threshold event occurs:

```
$ExpressionName=='ifutil'
AND $EventSeverity=='Critical'
```

For more information, see [“Triggering Notifications by Event Severity” on page 247](#).

## TRIGGERING NOTIFICATIONS FOR SUSTAINED EVENTS

You will set up some notifications to be sent as soon as an event occurs. Others will be events that do not require notification until the event has occurred over a period of time.

When you set up the alarm profiles in the NetVoyant Console, you can define the alarm rules so that an alarm is triggered only when an event occurs over a specified duration, or period of time. Using this alarm rule to generate a notification, you can ensure that you or your team only receive a notification for a sustained event. For more information about event duration, see [“Using the Event Duration Property” on page 252](#).

**Note:** To trigger notifications for sustained events, you must raise the Threshold Notification Limit or Polling Notification Limit for the dataset. For more information, see [“Using Polling Notification Limits” on page 249](#).

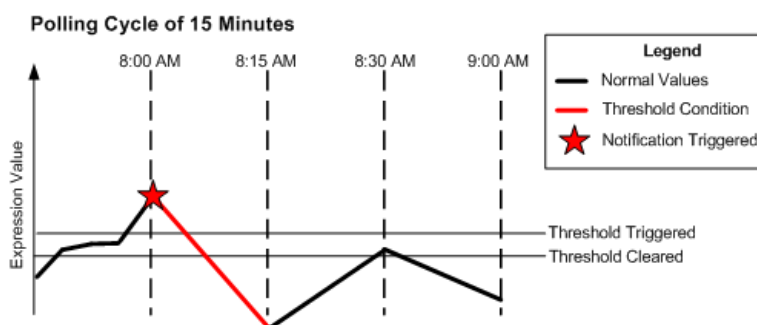
## Calculating Sustained and Spike Events

In the NetVoyant product, you can create notifications that are triggered for both of the following:

- Spike events - Events that occur when an expression goes over threshold.
- Sustained events - Events that continue for a continuous length of time.

**Spike Events.** If you create notifications that trigger by an alarm configured for poll intervals only, you are creating a notification that notifies for any spike in the expression’s value. This method of notification can create excessive notifications to your team. For example, you can create an email notification that sends a network engineer an email when utilization goes over a 70% threshold.

*NetVoyant sends a notification immediately when utilization spikes*





This notification enables your network engineer to know immediately when utilization spikes; however, in the example shown in the figure, utilization goes above threshold and immediately drops below threshold before the next 15 minute polling cycle. If the utilization again spikes after 15 minutes, the network engineer receives an additional email and so on for every utilization spike.

To reduce the number of notifications, you might want to configure the NetVoyant product to send notifications only for sustained events by using setting an event duration for the alarm.

**Sustained Events.** To limit notifications for events that clear quickly, you can create alarm rules for sustained events and or delay notifications for a selected length of time after an event first occurs.

For example, you can create an alarm that gets triggered when interface utilization is above the threshold for more than two hours or an event duration of 7200 seconds. If you configured such an alarm and created a notification using this alarm, the network engineer does not receive a notification for the example shown in the preceding figure because the threshold event does not last for more than two hours.

### Considerations When Configuring Notifications for Sustained Events

If you decide to create notifications for sustained events, you must perform the following actions:

- Decide upon an occurrence window, which is the maximum length of time that can be identified as one occurrence. Based on your occurrence window, you must configure the Threshold or Polling Notification Limit settings for the dataset and consider differences in polling rates on the dataset. For more information, see [“Using Polling Notification Limits” on page 249](#).
- Add an event duration window to the event filters for notifications that you want to delay, which delays the notification and limits the number of notifications sent for one event. For more information, see [“Using the Event Duration Property” on page 252](#).

## Using Polling Notification Limits

When you configure a dataset, you can edit the number of polling cycles over which the NetVoyant product can send notifications for polling events on the dataset by editing the **Polling Notification Limit** setting.

The default setting of 1 for the Polling Notification Limit setting enables you to set email notifications for availability spikes without having to use event-duration filters to restrict notifications to one per event.

To configure notifications for sustained events, you can raise the Polling Notification Limit setting to enable the NetVoyant product to correlate multiple polling exceptions over a continuous length of time with one distinct occurrence.

**Triggering Notifications for Sustained Events.** You can create notifications that are triggered only for sustained events or events that continue for a continuous length of time.

If you configure notifications for sustained polling events, or polling events that last for a sustained length of time, you must determine and set an appropriate Polling Notification Limit setting for each dataset that contains expressions on which you are notifying.

**Configuring the Occurrence Window.** When you configure the Polling Notification Limit, you are configuring an occurrence window, which is the maximum length of time that can be set for the event duration for a single event.

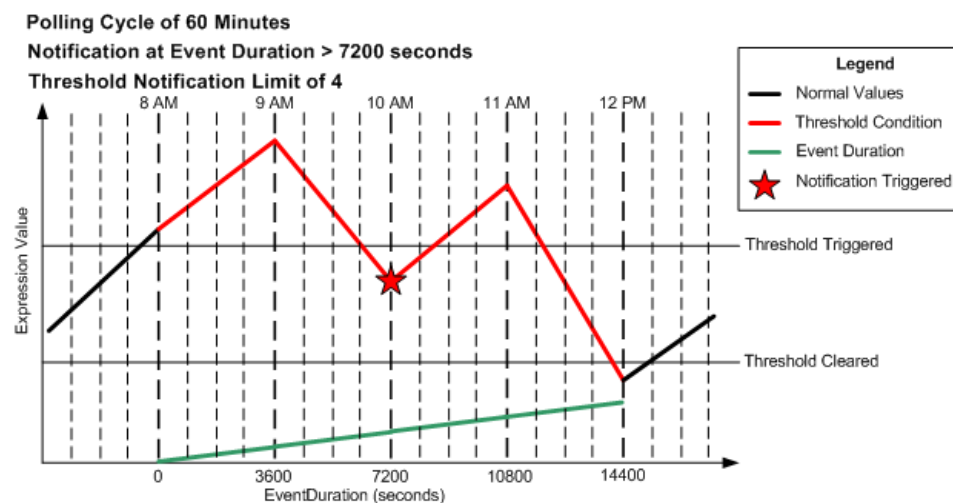
For example, you can set a Polling Notification Limit of 4 for a dataset that has two defined polling groups, one with a 60 minute polling rate and one with a 15 minute polling rate. In this example, the occurrence window for the 60 minute polling group is set to four hours or four polling cycles. The occurrence window for the 15 minute polling group is set to only 1 hour and four polling cycles.

In the 60 minute polling group, the NetVoyant product can identify a single polling event that lasts up to four hours as one event. In the 15-minute polling group, it can identify a single polling event that lasts up to one hour as one event.

To configure a large enough occurrence window, you must set a large enough Polling Notification Limit setting.

For example, to configure sending a notification after utilization has been over threshold for two hours, if the polling rate is 60 minutes for all interfaces, you must raise the Polling Notification Limit setting to at least 2 to allow for a two-hour occurrence window. To delay for four hours, you must raise the setting to 4 to allow for a four-hour occurrence window.

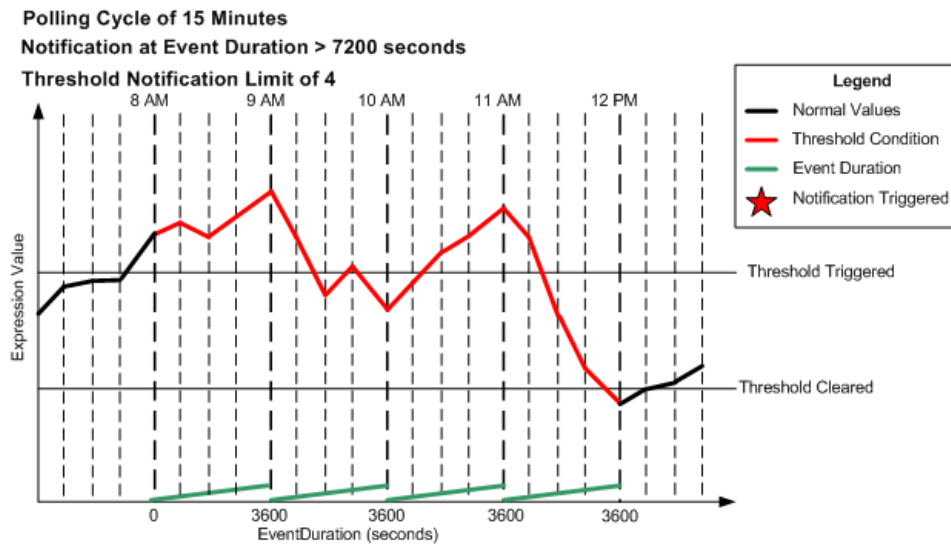
*A notification is triggered after two polling cycles (two hours)*



In many situations, you might configure different polling rates for your interfaces. If so, you must consider all polling rates in the dataset when determining a Notification Setting.

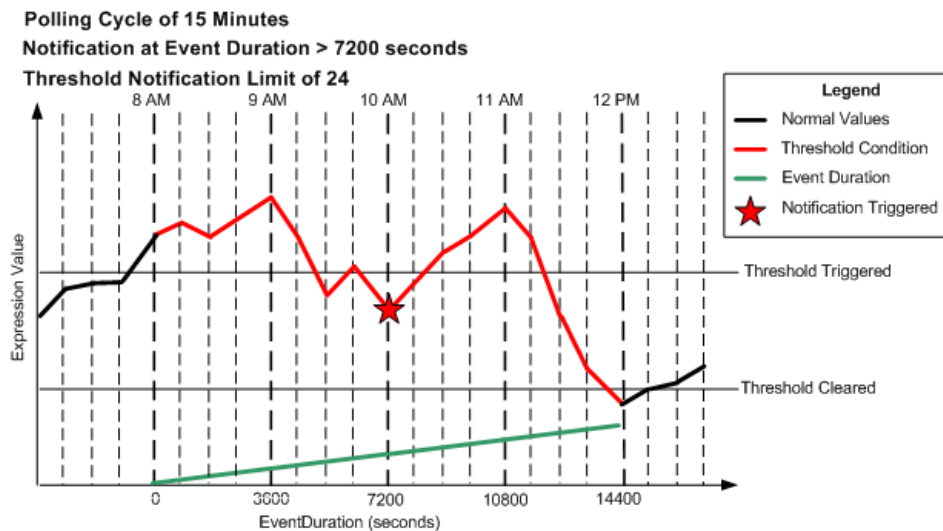
For example, consider if the dataset depicted in the following figure has two polling groups, one with a 60-minute polling rate and one with a polling rate of 15 minutes. If you set a Polling Notification Limit of 4 and configure a notification to be triggered after two hours, the notification is never triggered for those interfaces that have a polling rate of 15 minutes, even for sustained events of longer than two hours because the occurrence window for the 15-minute polling rate is set to only one hour (3600 seconds).

*A notification is never triggered for the threshold event*



To configure an occurrence window large enough to accommodate the two-hour delay you want for your notifications, change the Polling Notification Limit for the dataset to some number greater than 8.

*A notification is triggered after eight polling cycles (two hours).*



In the preceding figure, the Polling Notification Limit setting is set to 24 and the Notification is sent after eight polling cycles or two hours.

**Determining a Notification Limit Setting.** The relationship between occurrence window and notification limit setting can be expressed using the following formula:

$$\text{Notification Limit Setting} = \text{Occurrence Window} / \text{Polling Rate}$$

To determine the Notification Limit setting that you should use, calculate the largest occurrence window that you need to enable your delayed notifications. For example, to be able to delay notifications for events by up to two hours, you need an occurrence window of at least two hours.

Next, divide the length of the occurrence window by the smallest polling rate defined in the dataset. This provides you with a large enough Notification Limit setting to accommodate this occurrence window or larger on polling groups defined in the dataset.

For example, to be able to delay notifications by up to two hours (7200 seconds) on a dataset that has a one minute (60 second) polling rate, you can use the formula to determine that you must have a Notification Limit setting of at least 120:

$$7200 \text{ seconds} / 60 \text{ seconds} = 120$$

## Using the Event Duration Property

Event duration is a NetVoyant property that is equal to the length of time in seconds since the beginning of an event.

For example, if utilization for an interface goes over the threshold exceeded value at 8:00 a.m. and does not go back below the threshold cleared value, the event duration at 9:00 a.m. is 3600.

**Note:** When you view an event in NetVoyant event logs, event duration is referred to as `EventDuration`. When used in event filters for notifications, event duration is referred to as `$EventDuration`.

You can use the event duration property to trigger notifications for events that have continued for a sustained period of time.

For example, you can configure the NetVoyant product to send a notification email when interface utilization has been over threshold for one hour.

**Important:** To use the event duration property to trigger notifications, you must raise the Polling Notification Limit above the default of None. If you do not raise these settings, the NetVoyant product does not recognize events that last for more than one polling cycle as one occurrence and thus all events have an event duration of zero. For more information, see [“Using Polling Notification Limits” on page 249](#).

### Including an Event Duration Window in an Event Filter

Because of event duration difference based on polling queue length differences, we recommend you include an event duration window in event filters that uses the event duration property. This ensures that you will receive a notification for an event even if the event duration is slightly under the event duration limit that you want.

Without this event duration window, you would need to wait until the next polling cycle to receive a notification if an event has lasted just several seconds short of your event duration limit because of slight differences in polling queue lengths.

**Important:** You must also include an upper limit on the `EventDuration` property to ensure that you do not receive multiple notifications for the same sustained event.

We also recommend that you include the `EventCleared` property when using the `EventDuration` property in an event filter to ensure that the event is still active when a delayed notification is sent.

To create a delayed notification with an event duration window of plus or minus 50 seconds that is sent when an event is still active, add the following range for the `EventDuration` property in your event filter:

```
AND $EventDuration >= Seconds - 50
AND $EventDuration <= Seconds + 50
AND $EventCleared == 0
```

where `Seconds` is the length of time in seconds after which you want to notify. For example, to notify after an event has lasted one hour, enter 3600.



# Configuring IP SLA Operations

---

IP SLA operations enable you to measure network performance by simulating network data and services on many Cisco devices. The NetVoyant product enables you to configure IP SLA operations on those Cisco network devices that support this feature. IP SLA operation configuration tasks take place in the NetVoyant Console on the **Groups** tab and in the IP SLA Wizard.

You can review data gathered from your devices as part of these IP SLA operations in the NetVoyant IP SLA reports. For more information about the IP SLA views for reports, see the *NetVoyant User Guide*.

This chapter covers the following topics:

- “NetVoyant Support for Cisco IP SLA” on page 256
- “Configuring IP SLA Operations” on page 258
- “IP SLA Test Configuration Settings” on page 261
- “Viewing and Editing IP SLA Operations” on page 269
- “Using the IP SLA Import Utility” on page 272

## NETVOYANT SUPPORT FOR CISCO IP SLA

The central theme of IP SLA operations is round-trip-time or latency measurement, which has a common designation of RTT. Additionally, errors encountered during the operation and completion statistics for the RTT operations are maintained by the router for all operations. Using SNMP, the NetVoyant product is able to access the RTT results from Cisco routers based on definitions found in the CISCO\_RTTMON\_MIB.

There are several types of IP SLA operations that provide statistics additional to RTT, such as jitter and MOS scores for VoIP, TCP connect times, DNS lookup times, and other useful round-trip-time based statistics.

**Note:** You must configure the **get profile** for a device to configure an IP SLA operation on the device. For more information, see [“Setting SNMP Profiles for a Device” on page 149](#).

### Supported IP SLA Operations

IP SLA operations require multiple poll instances in the NetVoyant product. For more information about poll instances, see [“Data Organization by Poll Instance” on page 68](#).

You can configure the following IP SLA operations in the NetVoyant Console using the IP SLA Wizard:

Operation	Measures	Key applications	Poll instances
ICMP Echo	Round-trip delay from the source router to the destination IP device	<ul style="list-style-type: none"> <li>• IP performance</li> <li>• Connectivity measurement</li> </ul>	1
Path Echo	Round-trip delay Hop-by-hop round-trip delay	<ul style="list-style-type: none"> <li>• Connectivity measurements</li> <li>• Identify bottlenecks in the path</li> </ul>	1
UDP Echo	Round-trip delay of UDP traffic	<ul style="list-style-type: none"> <li>• Server and IP application performance</li> <li>• Connectivity testing</li> </ul>	1
TCP Connect	Time taken to connect to a target device with TCP	Server and application performance	1
HTTP	Round-trip time to retrieve a web page	Web server performance	2
DNS	DNS lookup time	Web or DNS server performance	1



Operation	Measures	Key applications	Poll instances
UDP Jitter	<ul style="list-style-type: none"> <li>• Round-trip delay</li> <li>• One-way delay</li> <li>• One-way jitter</li> <li>• One-way packet loss</li> <li>• Connectivity testing of networks that carry UDP traffic, such as voice</li> </ul> <p><b>Note:</b> One-way delay requires time synchronization between source and target routers.</p>	<ul style="list-style-type: none"> <li>• Voice and data network performance</li> <li>• General IP performance</li> </ul>	2
UDP Jitter for VoIP	<ul style="list-style-type: none"> <li>• Round-trip delay for VoIP traffic</li> <li>• One-way delay for VoIP traffic</li> <li>• One-way jitter for VoIP traffic</li> <li>• One-way packet loss for VoIP traffic</li> <li>• MOS and ICPIF voice quality scoring capability</li> </ul> <p><b>Note:</b> One-way delay requires time synchronization between source and target routers.</p> <p>Codec Support:</p> <ul style="list-style-type: none"> <li>• G.711 u-law Codec simulation</li> <li>• G.711 a-law Codec simulation</li> <li>• G.729A Codec simulation</li> </ul>	VoIP network and performance	2
DHCP	Round-trip time to get an IP address from a DHCP server	DHCP server response time	1
FTP	Round-trip time to transfer a file using FTP	FTP server performance	1

## CONFIGURING IP SLA OPERATIONS

You can configure IP SLA tests on a router that supports IP SLA operations using the NetVoyant IP SLA Wizard. The wizard guides you through configuring each operation, enabling you to apply meaningful names and descriptions, and saving the operational configuration for the operation to the router. Additionally, the IP SLA Wizard enables you to enter multiple source routers and target responders for each operation.

### To configure an IP SLA operation using the IP SLA Wizard:

1. From the **Tools** menu in the NetVoyant Console, select **IP SLA Wizard**.
  - Click **Next** to step through the wizard.
  - Click **Back** to step backwards to a previous step.
2. Click **Next** once to display the Select Measurement Type screen.

3. Select the **IP SLA Test Type**.

This determines the type of operation performed. You can select any IP SLA operation described in the previous section.

4. Edit the following parameters to define the IP SLA operation:

Parameter	Description
<b>Name</b>	Enter a name to help you identify the IP SLA operation.
<b>Description</b>	<i>(Optional)</i> Enter a description to help you identify what the IP SLA operation measures.
<b>Timeout</b>	Enter the amount of time in milliseconds that the IP SLA operation waits for a response from a request packet.
<b>Frequency</b>	Enter the rate in seconds at which the IP SLA operation repeats.
<b>VerifyData</b>	Select <b>True</b> to configure the IP SLA operation to check each reply packet for data corruption. Select <b>False</b> to not use this option.

Parameter	Description
<b>RTT Threshold</b>	Enter the upper threshold value in milliseconds for calculating network monitoring statistics created by the IP SLA operation.
<b>Save to Running config</b>	<p>Select this check box to save the IP SLA operation to the router's configuration.</p> <p>This feature allows the IP SLA test to be seen in the router's running configuration, making it possible to save the test (an additional procedure) to the startup configuration.</p> <p>When this check box is not selected, the test cannot be seen in the running configuration or saved to the startup configuration. If the router reboots, the test is lost and the NetVoyant product generates a polling alarm for the IP SLA test until re-discovery disables the poll instance.</p>
<b>Source Routers</b>	<p>Enter the IP address for the Cisco devices on which you want to configure the IP SLA operation, and use commas to separate multiple IP addresses.</p> <p>You can click <b>Edit</b> to select source routers from a list of devices known to support IP SLA. For more information about selecting a list of source routers, see <a href="#">“Selecting Source Routers for IP SLA Operations” on page 259</a>.</p>

- Click **Next** to configure the IP SLA operation settings specific to the operation type.
- Configure the settings specific to the IP SLA operation type that you selected in step 3.  
For more information about these settings, see [“IP SLA Test Configuration Settings” on page 261](#).
- Click **Next**.
- On the last screen of the wizard, click **Finish**.

## Selecting Source Routers for IP SLA Operations

When you configure an IP SLA operation, you must identify the routers that will execute the operation. If the IP addresses are known, you can enter these in the Source Routers field in the IP SLA Wizard using commas to separate multiple addresses. If you do not know the IP addresses, you can search for and select the routers for the operation.

### To locate and select source routers for an IP SLA operation:

- In the Select Measurement Type panel of the IP SLA Wizard, click the **Edit** button next to the **Source Routers** text box.  
The **IP SLA Source Routers** dialog box opens. The list on the left displays the devices (routers and switches) that support IP SLA.
- If the list is extensive, use the **Filter** text box to apply a filter expression to the list of available devices.
  - Enter a text string to use for filtering the list. For example, enter 192\* to view only those available routers having an IP address that begins with 192.
  - Click **Search** to search for the available devices according to the filter.
- Select an IP address from the list and use the **>>** button to add it to the source routers list on the right.

You can select multiple IP addresses and add each one to the source routers list.

4. When the desired IP addresses are added to the list, click **Done**.

## Setting Target Addresses for IP SLA Operations

Use the test parameters panel to specify the destination (target) for sending tests. For many operations, this can be almost anything with an IP address such as a workstation, server, router, or switch.

For the Jitter operation (Enhanced UDP Operation for Voice), the target must be a router that can act as a responder using the `rtr responder` IOS command. For example:

```
Router (config)# rtr responder
```

You can enter one or more IP addresses (separated by commas or spaces) or click the **Edit** button to search for and select IP addresses.

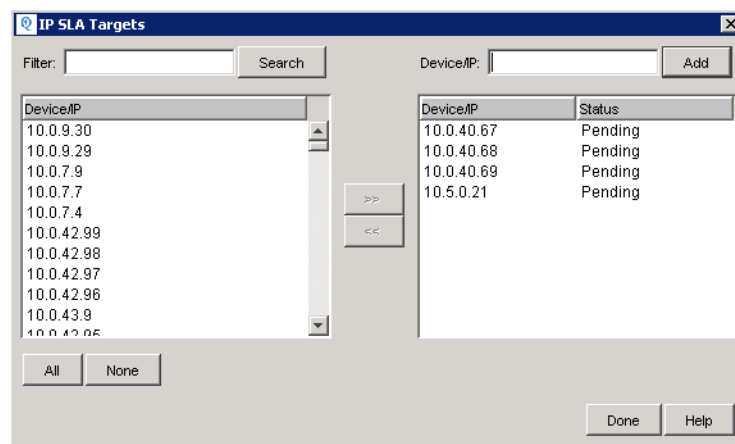
### To set target addresses for an IP SLA operation:

1. In the Select Parameters panel of the IP SLA Wizard, click the **Edit** button next to the **Target Addresses** text box.

The **Target Addresses** dialog box opens. The list on the left displays the devices (routers and switches) that support IP SLA.

2. If the list is extensive, use the **Filter** text box to apply a filter expression to the list of available devices.
  - Enter a text string to use for filtering the list. For example, enter `192*` to view only those available routers having an IP address that begins with 192.
  - Click **Search** to search for the available devices according to the filter.
3. Select an IP address from the list and use the **>>** button to add it to the target addresses list on the right.

You can select multiple IP addresses and add each one to the target addresses list.



4. When the desired IP addresses are added to the list, click **Done**.

## IP SLA TEST CONFIGURATION SETTINGS

Before configuring an IP SLA operation, be sure that you are familiar with the configuration settings for that type of operation. The configuration settings for each type of supported IP SLA operation are listed in the following sections. The valid range of inputs and defaults (if applicable) for each setting are also listed.

### ICMP Echo Test Configuration Settings

An ICMP echo test measures the round-trip delay for the full path. Modify the following settings to configure this test:

Setting	Description	Valid range	Default
<b>Target Addresses</b>	Enter one or more IP addresses (separated by commas or spaces) or click the <b>Edit</b> button to search for and select IP addresses.  For more information, see “ <a href="#">Setting Target Addresses for IP SLA Operations</a> ” on page 260.	N/A	N/A
<b>ToS Setting</b>	<i>(Optional)</i> For measuring the quality of service between two endpoints.  The ToS setting enables you to identify the ToS bits of the packets to be sent. This is especially important in validating service levels and obtaining the most accurate measure of voice quality.	N/A	0
<b>Request Packet Size</b>	<i>(Optional)</i> The protocol data size in the payload of the IP SLA operation’s request packet	28 to 1500 bytes	28
<b>Source Address</b>	<i>(Optional)</i> Enter the source address on the router for greater accuracy.	N/A	N/A
<b>VRF Name</b>	<i>(Optional)</i> Allows monitoring of MPLS VPNs by specifying a VPN routing/forwarding (VRF) name to which the operation belongs.	N/A	N/A

### Path Echo Test Configuration Settings

A path echo test measures the round-trip delay and hop-by-hop round-trip delay. Modify the following settings to configure this test:

Setting	Description	Valid range	Default
<b>Target Addresses</b>	You can enter one or more IP addresses (separated by commas or spaces) or click the <b>Edit</b> button to search for and select IP addresses.  For more information, see “ <a href="#">Setting Target Addresses for IP SLA Operations</a> ” on page 260.	N/A	N/A

Setting	Description	Valid range	Default
<b>ToS Setting</b>	<i>(Optional)</i> For measuring the quality of service between two endpoints.  The ToS setting enables you to identify the ToS bits of the packets to be sent. This is especially important in validating service levels and obtaining the most accurate measure of voice quality.	N/A	0
<b>Request Packet Size</b>	<i>(Optional)</i> The protocol data size in the payload of the IP SLA operation's request packet.	28 to 1500 bytes	28
<b>Source Address</b>	<i>(Optional)</i> Enter the source address on the router for greater accuracy.	N/A	N/A
<b>VRF Name</b>	<i>(Optional)</i> Allows monitoring of MPLS VPNs by specifying a VPN routing/forwarding (VRF) name to which the operation belongs.	N/A	N/A

## UDP Echo Test Configuration Settings

A UDP echo test measures server and IP application performance and tests connectivity. Modify the following settings to configure this test:

Setting	Description	Valid range	Default
<b>Target Addresses</b>	You can enter one or more IP addresses (separated by commas or spaces) or click the <b>Edit</b> button to search for and select IP addresses.  For more information, see <a href="#">“Setting Target Addresses for IP SLA Operations” on page 260</a> .	N/A	N/A
<b>Target Port</b>	The port over which requests are directed as part of the IP SLA operation.	Port max = 65535	0
<b>ToS Setting</b>	<i>(Optional)</i> For measuring the quality of service between two endpoints.  The ToS setting enables you to identify the ToS bits of the packets to be sent. This is especially important in validating service levels and obtaining the most accurate measure of voice quality.	N/A	0
<b>Request Packet Size</b>	<i>(Optional)</i> The protocol data size in the payload of the IP SLA operation's request packet.	16 to 1500 bytes	16
<b>Enable Control Messages</b>	Set this to True when the target is also configured as a Responder. This provides for better timing measurements during the RTT test. This is enabled by default.	True/False	True
<b>Source Address</b>	<i>(Optional)</i> Enter the source address on the router for greater granularity.	N/A	N/A
<b>VRF Name</b>	<i>(Optional)</i> Allows monitoring of MPLS VPNs by specifying a VPN routing/forwarding (VRF) name to which the operation belongs.	N/A	N/A

## TCP Connect Test Configuration Settings

A TCP connect test measures the time taken to connect to a target device with TCP. Modify the following settings to configure this test:

Setting	Description	Valid range	Default
<b>Target Addresses</b>	You can enter one or more IP addresses (separated by commas or spaces) or click the <b>Edit</b> button to search for and select IP addresses.  For more information, see “ <a href="#">Setting Target Addresses for IP SLA Operations</a> ” on page 260.	N/A	N/A
<b>Target Port</b>	The port over which requests are directed as part of the IP SLA operation.	Port max = 65535	0
<b>ToS Setting</b>	<i>(Optional)</i> For measuring the quality of service between two endpoints.  The ToS setting enables you to identify the ToS bits of the packets to be sent. This is especially important in validating service levels as well as obtaining the most accurate measure of voice quality.	N/A	0
<b>Enable Control Messages</b>	Set this to True when the target is also configured as a Responder. This provides for better timing measurements during the RTT test. This is enabled by default.	True/False	True
<b>Source Address</b>	<i>(Optional)</i> Enter the source address on the router for greater accuracy.	N/A	N/A

## HTTP Echo Test Configuration Settings

An HTTP echo test measures the round-trip time to retrieve a web page. Modify the following settings to configure this test:

Setting	Description	Valid range	Default
<b>HTTP Operation</b>	Select the type of HTTP operation you want to perform. You can select one of the following: <ul style="list-style-type: none"> <li>• <b>httpGet</b> - Performs a standard GET request as defined by the default for the Command.</li> <li>• <b>httpRaw</b> - Performs the Commands you enter.</li> </ul>	httpGet/ httpRaw	httpGet
<b>URL</b>	The full URL of the destination HTTP server.	N/A	N/A
<b>Command</b>	The commands you want to perform as part of the IP SLA operation.  <b>Note:</b> You do not need to enter commands for the default httpGet operation.	N/A	N/A
<b>HTTP Version</b>	The HTTP version to use in the IP SLA operation.	N/A	1.0

Setting	Description	Valid range	Default
<b>HTTP Proxy</b>	<i>(Optional)</i> The full URL of the Proxy server to use in the IP SLA operation.	N/A	N/A
<b>Download Cached Pages</b>	Specifies whether cached HTTP pages can be downloaded as part of this IP SLA operation. By default, cached HTTP can be downloaded. <ul style="list-style-type: none"> <li>• Select <b>True</b> to specify that cached HTTP pages can be downloaded.</li> <li>• Select <b>False</b> to disable the download of cached HTTP pages.</li> </ul>	True/False	True
<b>Source Address</b>	<i>(Optional)</i> Enter the source address on the router for greater accuracy.	N/A	N/A

## DNS Test Configuration Settings

A DNS test measures DNS look-up time. Modify the following settings to configure this test:

Setting	Description	Valid range	Default
<b>DNS Name to Lookup</b>	The DNS name on which you want to perform a lookup as part of this IP SLA operation.	Hostname	N/A
<b>DNS Name Server</b>	The IP address of the DNS name server to be used as part of the IP SLA operation.	IP address	N/A
<b>Source Address</b>	<i>(Optional)</i> Enter the source address on the router for greater accuracy.	N/A	N/A

## UDP Jitter Test Configuration Settings

A UDP jitter test measures voice and data network performance and general IP performance. Modify the following settings to configure this test:

Setting	Description	Valid range	Default
<b>Target Addresses</b>	You can enter one or more IP addresses (separated by commas or spaces) or click the <b>Edit</b> button to search for and select IP addresses. For more information, see <a href="#">“Setting Target Addresses for IP SLA Operations”</a> on page 260.	N/A	
<b>Target Port</b>	The port over which requests are directed as part of the IP SLA operation.	Port max = 65535	5000
<b>ToS Setting</b>	<i>(Optional)</i> For measuring the quality of service between two endpoints. The ToS setting enables you to identify the ToS bits of the packets to be sent. This is especially important in validating service levels as well as obtaining an accurate measure of voice quality.	N/A	160



Setting	Description	Valid range	Default
<b>Request Packet Size</b>	<i>(Optional)</i> The protocol data size in the payload of the IP SLA operation's request packet.	N/A	200
<b>Inter-packet Delay</b>	<i>(Optional)</i> The time, in milliseconds, between the packets sent as part of the IP SLA operation.	N/A	20 ms
<b>Number of Packets</b>	<i>(Optional)</i> The number of packets to be sent as part of the IP SLA operation.	N/A	10
<b>Enable Control messages</b>	Set this to True when the target is also configured as a Responder. This provides for better timing measurements during the RTT test. This is enabled by default.		
<b>Measurement Precision</b>	The unit of measurement used for the operation if <b>Specify</b> is selected.	Milliseconds or Microseconds	
<b>Specify</b>	Indicates whether the operation uses the Measurement Precision command. <ul style="list-style-type: none"> <li>Select the check box to turn on the <b>Measurement Precision</b> command.</li> <li>Clear the check box to turn off the <b>Measurement Precision</b> command.</li> </ul>	N/A	N/A
<b>Source Address</b>	<i>(Optional)</i> Enter the source address on the router for greater granularity.	N/A	N/A
<b>VRF Name</b>	<i>(Optional)</i> Allows monitoring of MPLS VPNs by specifying a VPN routing/forwarding (VRF) name to which the operation belongs.	N/A	N/A

## VoIP Jitter (Enhanced UDP) Test Configuration Settings

A VoIP jitter test measures round-trip delay, one-way delay, one-way jitter, and one-way packet loss for VoIP traffic. Also performs simulation for Codecs G.711 u-law, G.711 a-law, and G.729A. Modify the following settings to configure this test:

Setting	Description	Valid range	Default
<b>Target Addresses</b>	You can enter one or more IP addresses (separated by commas or spaces) or click the <b>Edit</b> button to search for and select IP addresses. For more information, see <a href="#">“Setting Target Addresses for IP SLA Operations”</a> on page 260.	N/A	N/A
<b>Target Port</b>	The port over which requests are directed as part of the IP SLA operation.	Port max = 65535	5000
<b>ToS Setting</b>	<i>(Optional)</i> For measuring the quality of service between two endpoints. The ToS setting enables you to identify the ToS bits of the packets to send. This is especially important in validating service levels as well as obtaining an accurate measure of voice quality.	N/A	160

Setting	Description	Valid range	Default
<b>Request Packet Size</b>	<i>(Optional)</i> The protocol data size in the payload of the IP SLA operation's request packet.	N/A	200
<b>Codec Type</b> <i>(optional)</i>	Select the type of codec to be used for voice simulation as part of the IP SLA operation. The codec enables the operation to generate VoIP scores in addition to latency, jitter, and packet loss statistics.	* G.711 a-Law - 64 kbps PCM compression method * G.711 u-Law - 64 kbps PCM compression method * G729a - 8 kbps CS-ACELP compression method	G.711 a-Law
<b>Codec Inter-packet Interval</b>	The time, in milliseconds, between the packets sent as part of the IP SLA operation. <b>Note:</b> Do not edit the values for the Codec Inter-packet Interval unless you have a specific reason to override the defaults. For example, to simulate a different codec.	N/A	20 ms
<b>Codec Payload Size</b>	The size of data payload sent in each packet as part of the IP SLA operation. <b>Note:</b> Do not edit the values for the Codec Payload Size unless you have a specific reason to override the defaults. For example, to simulate a different codec.	N/A	200
<b>Codec Number of Packets</b>	Enter the number of packets to send as part of the IP SLA operation. <b>Note:</b> Do not edit the values for the Codec Number of Packets unless you have a specific reason to override the defaults. For example, to simulate a different codec.	N/A	30
<b>ICPIF Advantage Factor</b>	Select the ICPIF Advantage Factor that best represents the level of voice-quality expected for the voice test. The value you specify is subtracted from the measured impairment values. You can use this option to correct the ICPIF and MOS values for network conditions.	Conventional Wire Line (0) Mobility within Building (5) Mobility within Geographic Area (10) Access to Hard to Reach Location (20)	Conventional Wire Line (0)

Setting	Description	Valid range	Default
<b>Enable Control Messages</b>	Set this to True when the target is also configured as a Responder. This provides for better timing measurements during the RTT test. This is enabled by default.	True/False	True
<b>Measurement Precision Specify</b>	The unit of measurement used for the operation if <b>Specify</b> is selected.	Milliseconds or Microseconds	Milliseconds
<b>Specify</b>	Indicates whether the operation uses the Measurement Precision command. <ul style="list-style-type: none"> <li>Select the check box to turn on the <b>Measurement Precision</b> command.</li> <li>Clear the check box to turn off the <b>Measurement Precision</b> command.</li> </ul>	N/A	N/A
<b>Source Address</b>	<i>(Optional)</i> Enter the source address on the router for greater accuracy.	N/A	N/A
<b>VRF Name</b>	<i>(Optional)</i> Allows monitoring of MPLS VPNs by specifying a VPN routing/forwarding (VRF) name to which the operation belongs.	N/A	N/A

## DHCP Test Configuration Settings

A DHCP test measures round-trip time to get an IP address from a DHCP server. Modify the following settings to configure this test:

Setting	Description	Valid range	Default
<b>Enable Control Messages</b>	Set this to True when the target is also configured as a Responder. This provides for better timing measurements during the RTT test. This is enabled by default.	True/False	True
<b>Source Address</b>	<i>(Optional)</i> Enter the source address on the router for greater accuracy.	N/A	N/A

## FTP Test Configuration Settings

An FTP test measures FTP server performance. Modify the following settings to configure this test:

Setting	Description	Valid range	Default
<b>ToS Setting</b>	<i>(Optional)</i> For measuring the quality of service between two endpoints.  The ToS setting enables you to identify the ToS bits of the packets to send. This is especially important in validating service levels as well as obtaining the most accurate measure of voice quality.		0
<b>FTP URL</b>	The full URL of the FTP location that you want to test as part of this IP SLA operation.		
<b>FTP Mode</b>	Select the FTP Mode to use for the IP SLA operation.	Active/Passive	Passive
<b>Enable Control Messages</b>	Set this to True when the target is also configured as a Responder. This provides for better timing measurements during the RTT test. This is enabled by default.	True/False	True
<b>Source Address</b>	<i>(Optional)</i> Enter the source address on the router for greater accuracy.	N/A	N/A

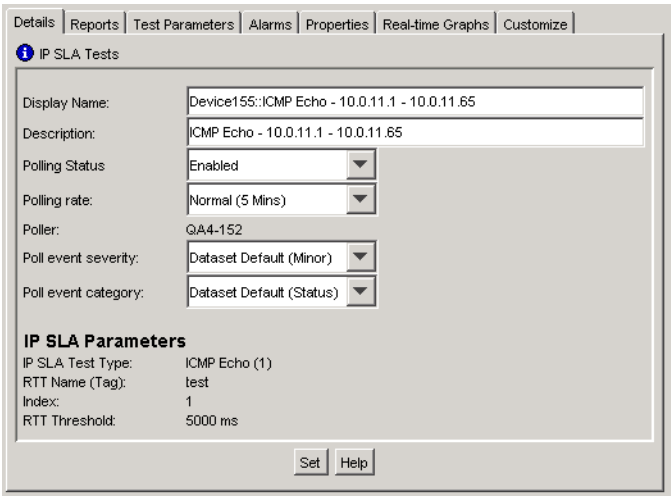
# VIEWING AND EDITING IP SLA OPERATIONS

Use the **Group** tab in the NetVoyant Console to view details for an IP SLA operation or to edit the test configuration. You can also disable polling for a defined IP SLA operation.

**To view or edit an existing IP SLA operation in NetVoyant:**

- 1. In the NetVoyant Console, select the **Group** tab.
- 2. Expand the device to view its poll tables.
- 3. Expand the IP SLA poll table.
- 4. Select the IP SLA operation.

The details for the operation appear in the context panel.



- 5. You can view and edit the following parameters on the **Details** tab:

Parameter	Description
Display Name	The name of the IP SLA operation, which is used to reference the IP SLA operation in reports.  NetVoyant reports display names of IP SLA operations. The NetVoyant Console tree-tab panel displays the descriptions of IP SLA operations.
Description	A description of the IP SLA operation, which is used to reference the IP SLA operation in the NetVoyant Console.  NetVoyant reports display names of IP SLA operations. The NetVoyant Console tree-tab panel displays the descriptions of IP SLA operations.
Polling Status	The polling status for the IP SLA operation poll instance.  For more information about the polling status for a poll instance or interface, see <a href="#">“Polling Status and Expiration” on page 161</a> .
Polling rate	The polling group to which the IP SLA operation belongs. The polling group determines how often poll instance data is gathered and rolled up.  For more information, see <a href="#">“Configuring Polling for Poll Instances and Interfaces” on page 166</a> .  <b>Note:</b> By default, most IP SLA datasets have only one defined polling rate. Changing polling rates for most IP SLA operations is not recommended.

Parameter	Description
<b>Poller</b> ( <i>read-only</i> )	The NetVoyant server that gathers data for the IP SLA operation. In a standalone configuration, the poller is always the Master server. In a distributed configuration, the Poller is the NetVoyant server that polls the device to which the IP SLA operation belongs.
<b>Poll event severity</b>	The severity of a missed poll event for the IP SLA operation. For more information, see <a href="#">“Setting the Event Severity for a Poll Instance or Interface”</a> on page 167.
<b>Poll event category</b>	Use this setting to assign a category for poll events associated with the IP SLA operation. <b>Note:</b> If your NetVoyant system is registered with the NetQoS Performance Center as a data source, this category is used to filter events in the Map and Map Event List.
<b>IP SLA Parameters</b>	Displays basic IP SLA parameters for the operation. For more information about the displayed IP SLA parameters, see your device’s documentation.

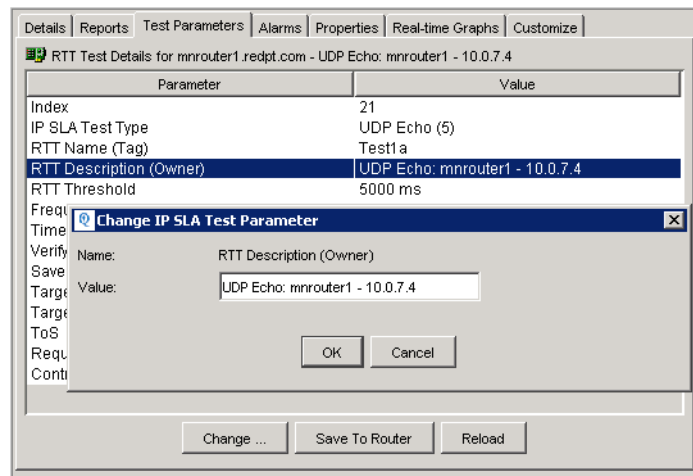
6. Click **Set** to save your changes.

7. Click the **Test Parameters** tab.

For more information about the displayed IP SLA parameters, see your device’s documentation.

**Note:** To edit IP SLA operation parameters on a device, you must have the correct **Set Profile** for the device in the NetVoyant Console. For more information, see [“Setting SNMP Profiles for a Device”](#) on page 149.

8. Select a parameter and click **Change** or double-click the parameter to edit its value.



9. Enter a new **Value**.

10. Click **OK**.

**Warning:** If you edit a test and save it to the router with an inappropriate value for a parameter, you will receive an error and the original operation will be removed from the router. Verify your changes before saving them.

11. Click **Save To Router** to save your changes.

This saves the updated IP SLA operation parameters to the router’s configuration.

12. Click **Reload** to view the updated parameter values.

## Disabling Polling for an IP SLA Operation

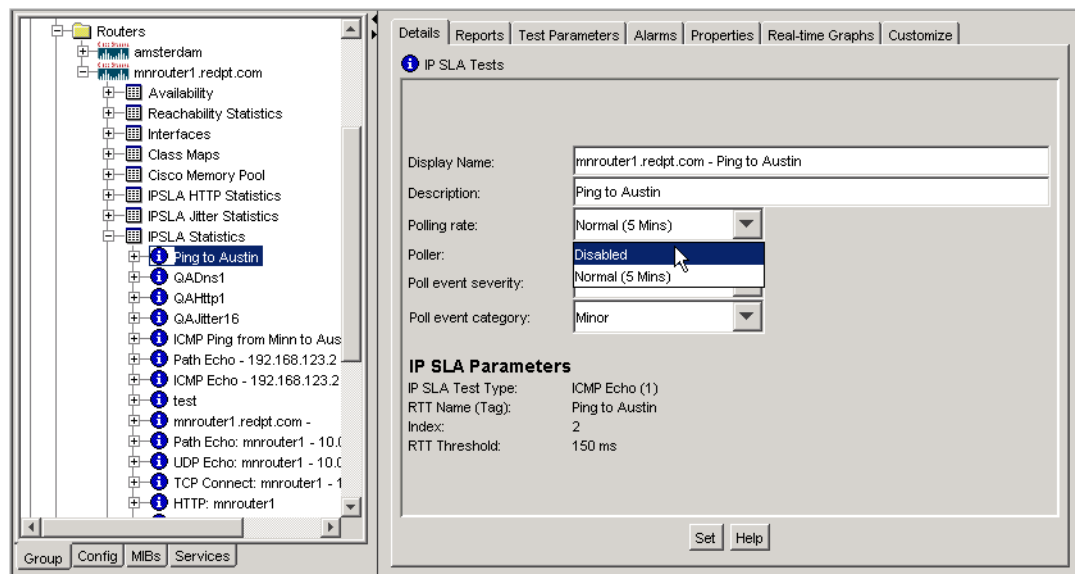
Disable polling for a configured IP SLA operation to exclude it from polling. By disabling polling rather than deleting the operation, you can enable polling for the operation if you need to do so in the future.

### To disable polling for an IP SLA operation:

1. In the NetVoyant Console, select the **Group** tab.
2. In the tree-tab panel, expand the Master server and group structure to locate the device.
3. Expand the device.
4. Expand the IP SLA poll table.
5. Select the IP SLA operation.

The details for the operation appear in the context panel.

6. To disable polling for the poll instance, select **Disabled** from the **Polling rate** list.



7. Click **Set**.

**Note:** To hide devices, poll instances, and interfaces that are disabled for polling in the NetVoyant Console, clear the **Show Disabled from Polling** option in the **View** menu.

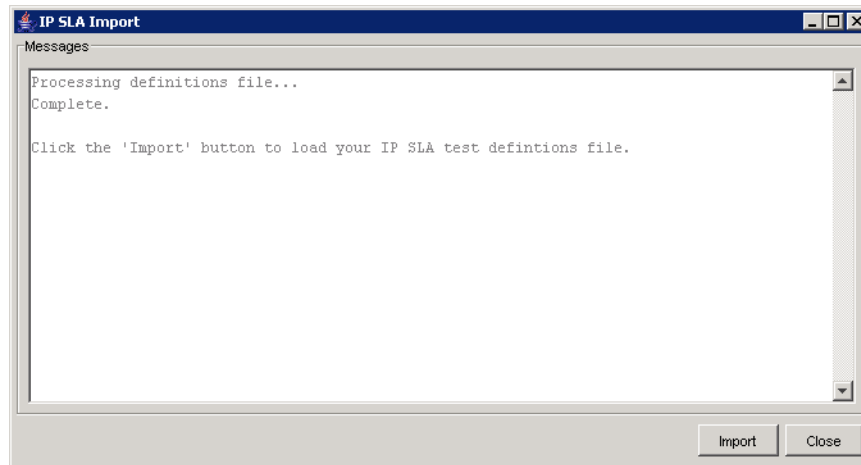
## USING THE IP SLA IMPORT UTILITY

The IP SLA Import Utility provides the ability to import IP SLA test definitions from an XML-formatted file. You can access this tool in the NetVoyant Console. The utility attempts to read and validate the test definitions and writes the tests to the routers and switches that execute the tests.

### To import IP SLA test definitions from an XML file:

1. From the **Tools** menu in the NetVoyant Console, select **IP SLA Import**.

The **IP SLA Import** dialog box opens.



The utility reads an internal configuration file that contains a list of tests supported, mappings of XML tags to MIB OIDs, and default values for each field. It verifies and then loads the contents of this configuration file.

**Note:** You could change the contents of this file if you need to do so; for example, you could change the default value of an OID. Perform this procedure only under the supervision of NetVoyant Technical Support because the internal format of this file is not documented.

2. Click **Import**.

The **Import IP SLA Definitions** dialog box opens.

3. Select the file containing the definitions and click **Add**.

The utility reads and verifies the selected file. The **IP SLA Import** dialog box lists the test definitions and reports errors or warnings.

4. If the test definitions are valid, click **Load** to load the tests to the devices that will execute the tests.

If there are errors in the test, you can correct the input file and attempt the import again.

The utility writes the test to the router. Errors appear or a successful load is noted.



## IP SLA Import XML File Format

You can use the IP SLA import utility to import a test definition from an XML-formatted file. This file must be formatted in XML according to the following rules:

```
<?xml version="1.0"?>
<ipsla>
  <rtt [attributes] />
</ipsla>
```

**Example:**

```
<?xml version="1.0"?>
<ipsla>
  <rtt
    Router="mnrouter1, 10.1.1.0, 192.168.1"
    RttType="echo"
    Name="$RttType to $TargetAddress"
    Tag="$RttType from $router to $TargetAddress"
    Threshold="500"
    Frequency="60"
    Timeout="1000"
    VerifyData="true"
    Nvgen="true"

    Protocol="ipIcmpEcho"
    TargetAddress="10.0.1.1"
    PktDataRequestSize="20"
    PktDataResponseSize="20"
    TOS="128"
  />
</ipsla>
```

**Attributes for the <rtt> Tag**

The following attributes are used for the rtt tag:

Attribute	Usage
Router	This can be specified as a list of source routers for the test by listing the names or IPs in a comma-separated list.
Index	<i>(Optional)</i> If specified, overwrites test at this index.
Owner	This is equivalent to the NetVoyant “Name” and is a text string of up to 16 characters.

Attribute	Usage																																						
Tag	<p>This is equivalent to the “Description” and is a text string of up to 255 characters. You can specify a template using the other fields in the test. For example, to specify the test type, source, and destination, you would specify this for the Tag field:</p> <pre>"\$RttType - \$Router - \$TargetAddress"</pre>																																						
RttType	<p>This is a required attribute that identifies the test type. The following valid values correspond to the test the supported IP SLA operations and map to text strings for naming purposes:</p> <table> <thead> <tr> <th>RttType Value</th><th>Maps to Test Text String</th></tr> </thead> <tbody> <tr><td>echoICMP</td><td>Echo</td></tr> <tr><td>pathEchoPath</td><td>Echo</td></tr> <tr><td>fileIOFile</td><td>I/O</td></tr> <tr><td>scriptScript</td><td></td></tr> <tr><td>udpEchoUDP</td><td>Echo</td></tr> <tr><td>tcpConnectTCP</td><td>Connect</td></tr> <tr><td>httpHTTP</td><td></td></tr> <tr><td>dnsDNS</td><td></td></tr> <tr><td>jitterUDP</td><td>Jitter (with or without codec)</td></tr> <tr><td>dlswDLSw</td><td></td></tr> <tr><td>dhcpDHCP</td><td></td></tr> <tr><td>ftpFTP</td><td></td></tr> <tr><td>voipVoIP</td><td>Call Setup</td></tr> <tr><td>rtpVoIP</td><td>RTP</td></tr> <tr><td>lspGroupLSP</td><td>Path Group</td></tr> <tr><td>icmpjitterICMP</td><td>Jitter</td></tr> <tr><td>lspPingLSP</td><td>PING</td></tr> <tr><td>lspTraceLSP</td><td>Trace</td></tr> </tbody> </table>	RttType Value	Maps to Test Text String	echoICMP	Echo	pathEchoPath	Echo	fileIOFile	I/O	scriptScript		udpEchoUDP	Echo	tcpConnectTCP	Connect	httpHTTP		dnsDNS		jitterUDP	Jitter (with or without codec)	dlswDLSw		dhcpDHCP		ftpFTP		voipVoIP	Call Setup	rtpVoIP	RTP	lspGroupLSP	Path Group	icmpjitterICMP	Jitter	lspPingLSP	PING	lspTraceLSP	Trace
RttType Value	Maps to Test Text String																																						
echoICMP	Echo																																						
pathEchoPath	Echo																																						
fileIOFile	I/O																																						
scriptScript																																							
udpEchoUDP	Echo																																						
tcpConnectTCP	Connect																																						
httpHTTP																																							
dnsDNS																																							
jitterUDP	Jitter (with or without codec)																																						
dlswDLSw																																							
dhcpDHCP																																							
ftpFTP																																							
voipVoIP	Call Setup																																						
rtpVoIP	RTP																																						
lspGroupLSP	Path Group																																						
icmpjitterICMP	Jitter																																						
lspPingLSP	PING																																						
lspTraceLSP	Trace																																						
Threshold	Default = 5000																																						
Frequency	Default = 60																																						
Timeout	Default = 5000																																						
VerifyData	Default = false																																						
Nvgen	Default = false																																						

Attribute	Usage
Protocol	<p>If not specified, usually this can default by RttType.</p> <ul style="list-style-type: none"> <li>• notApplicable</li> <li>• ipUdpEchoAppl</li> <li>• snaLU0EchoAppl</li> <li>• snaLU62Echo</li> <li>• appleTalkEcho</li> <li>• decNetEcho</li> <li>• ipxEcho</li> <li>• isoClnsEcho</li> <li>• vinesEcho</li> <li>• xnsEcho</li> <li>• apolloEcho</li> <li>• netbiosEchoAppl</li> <li>• httpAppl</li> <li>• jitterAppl</li> <li>• dhcpAppl</li> <li>• mplsLspPingAppl</li> <li>• rtpAppl</li> <li>• ipIcmpEcho</li> <li>• snaRUEcho</li> <li>• snaLU2EchoAppl</li> <li>• snaLU62EchoAppl</li> <li>• appleTalkEchoAppl</li> <li>• decNetEchoAppl</li> <li>• ipxEchoAppl</li> <li>• isoClnsEchoAppl</li> <li>• vinesEchoAppl</li> <li>• xnsEchoAppl</li> <li>• apolloEchoAppl</li> <li>• ipTcpConn</li> <li>• dnsAppl</li> <li>• dlswAppl</li> <li>• ftpAppl</li> <li>• voipAppl</li> <li>• icmpJitterAppl</li> </ul>
TargetAddress	This can be specified as a list of addresses separated by commas.
PktDataRequestSize	For ICMP, Path Echo, UDP Echo, and Jitter without a codec, this is the packet size sent.
TargetPort	Specifies the target port (in addition to the target address) of the IP SLA operation. For some tests this is required, and for others it is optional.
SourceAddress	Allows you to specify which interface to use to send the test.
SourcePort	Allows you to specify the port to use for sending the test.
ControlEnable	Enables sending control messages to a target that is configured as a Responder.
TOS	This is the “Type of Service” field in the IP header. It can be set to different values to get higher or lower priority on the network.
LSREnable	If this object is enabled, it means that the application calculates response time for a specific path as defined in <code>rttMonEchoPathAdminEntry</code> .
TargetAddressString	This is the name to look up for a DNS test.
NameServer	This is the Name server to use for a DNS test.

Attribute	Usage														
Operation	<p>This is used for several different test types. For an HTTP test, this would be <code>httpGet</code> or <code>httpRaw</code>. The following are the possible values:</p> <table> <tr> <td><code>httpGet(1)</code></td><td>- HTTP get request</td></tr> <tr> <td><code>httpRaw(2)</code></td><td>- HTTP request with user defined payload</td></tr> <tr> <td><code>ftpGet(3)</code></td><td>- FTP get request</td></tr> <tr> <td><code>ftpPassive(4)</code></td><td>- FTP passive mode</td></tr> <tr> <td><code>ftpActive(5)</code></td><td>- FTP active mode</td></tr> <tr> <td><code>voipDTAlertRinging(6)</code></td><td>- Voip post dial delay detect point: Alerting / Ringing</td></tr> <tr> <td><code>voipDTConnectOK(7)</code></td><td>- Voip post dial delay detect point: Connect / OK</td></tr> </table>	<code>httpGet(1)</code>	- HTTP get request	<code>httpRaw(2)</code>	- HTTP request with user defined payload	<code>ftpGet(3)</code>	- FTP get request	<code>ftpPassive(4)</code>	- FTP passive mode	<code>ftpActive(5)</code>	- FTP active mode	<code>voipDTAlertRinging(6)</code>	- Voip post dial delay detect point: Alerting / Ringing	<code>voipDTConnectOK(7)</code>	- Voip post dial delay detect point: Connect / OK
<code>httpGet(1)</code>	- HTTP get request														
<code>httpRaw(2)</code>	- HTTP request with user defined payload														
<code>ftpGet(3)</code>	- FTP get request														
<code>ftpPassive(4)</code>	- FTP passive mode														
<code>ftpActive(5)</code>	- FTP active mode														
<code>voipDTAlertRinging(6)</code>	- Voip post dial delay detect point: Alerting / Ringing														
<code>voipDTConnectOK(7)</code>	- Voip post dial delay detect point: Connect / OK														
HTTPVersion	Specifies the HTTP version (1.0 or 1.1).														
URL	Specifies the URL to query in HTTP test.														
Cache	This can be True or False														
Interval	Interpack interval for Jitter (non-Codec) tests														
NumPackets	Number of packets to send for Jitter (non-Codec) tests.														
Proxy	HTTP proxy, if required.														
String1	Used for HTTP requests that need longer URLs.														
String2	Used for HTTP requests that need longer URLs.														
String3	Used for HTTP requests that need longer URLs.														
String4	Used for HTTP requests that need longer URLs.														
String5	Used for HTTP requests that need longer URLs.														
Mode	Values can be <code>ftpPassive</code> or <code>ftpActive</code> , used to specify active/passive for FTP operations.														
VrfName	This field is used to specify the VPN name in which the RTT operation will be used. For regular RTT operations, this field should not be configured. The agent will use this field to identify the VPN routing Table for this operation.														
CodecType	Specifies the codec to be used for Jitter (with Codec) tests.														
CodecInterval	Specifies the interpacket delay for Jitter (with Codec) tests.														
CodecPayload	Specifies the payload for the codec.														
CodecNumPackets	Specifies the number of packets to send for Jitter (with Codec) tests.														
ICPIFAdvFactor	<p>This is used while calculating the ICPIF values and is valid only for Jitter while calculating the ICPIF value. This advantage factor depends on the type of access and how the service is to be used.</p> <table> <tr> <td>Conventional Wire-line</td><td>0</td></tr> <tr> <td>Mobility within Building</td><td>5</td></tr> <tr> <td>Mobility within geographic area</td><td>10</td></tr> <tr> <td>Access to hard-to-reach location</td><td>20</td></tr> </table>	Conventional Wire-line	0	Mobility within Building	5	Mobility within geographic area	10	Access to hard-to-reach location	20						
Conventional Wire-line	0														
Mobility within Building	5														
Mobility within geographic area	10														
Access to hard-to-reach location	20														
LSPFECType	For more information about support for this attribute, see the documentation for the associated IP SLA MIB file.														

Attribute	Usage
LSPSelector	A string that specifies a valid 127/8 address. This address is of the form 127.x.y.z. It is not used to route the MPLS echo packet to the destination but is used for load balancing in cases where the IP payload's destination address is used for load balancing.
LSPReplyMode	This object specifies the reply mode for the LSP Echo requests. (Default= replyIpv4Upd)
LSP TTL	<p>This object represents the TTL setting for MPLS echo request packets. For a ping operation, this represents the TTL value to be set in the echo request packet. For a trace operation, it represents the maximum ttl value that can be set in the echo request packets starting with TTL=1.</p> <p>For 'echo' based on mplsLspPingAppl, the default TTL will be set to 255, and for 'pathEcho' based on mplsLspPingAppl, the default will be set to 30.</p> <p><b>Note:</b> This object cannot be set to the value of zero. The default value of zero signifies the default TTL values to be used for 'echo' and 'pathEcho' based on 'mplsLspPingAppl'.</p>
LSPExp	This object represents the EXP value put as the precedence bit in the MPLS echo request IP header.
Precision	This is used to specify millisecond or microsecond resolution on jitter tests.
ProbePakPriority	This object specifies the priority that will be assigned to probe packet. This value can be set only for jitter operations.
OWNTPSyncTolAbs	This object specifies the total clock synchronization error on source and responder that is considered acceptable for one-way measurement when NTP is used as the clock synchronization mechanism. The total clock synchronization error is the sum of NTP offsets on source and responder. The value specified in microseconds. This value can be set only for jitter operations with precision of microsecond.
OWNTPSyncTolPct	This object specifies the total clock synchronization error on source and responder that is considered acceptable for one-way measurement when NTP is used as the clock synchronization mechanism. The total clock synchronization error is the sum of NTP offsets on source and responder. This value is expressed as the percentage of actual one-way latency that is measured. This value can be set only for jitter operations with precision of microsecond.
OWNTPSyncTolType	This object specifies whether the value specified for one-way NTP sync tolerance is an absolute value or percent value.
CalledNumber	This string stores the called number of post dial delay. This object is applicable to VoIP post dial delay probe only. The number will be like the one a user could actually dial. It has the number required by the local country dial plan plus E.164 number. The maximum length is 24 digits. Only numeric digits (0-9) are allowed
DetectPoint	This is the code that represents the detect point of post dial delay. This object is applicable to SAA post dial delay probe only.
GKRegistration	This is a boolean value that represents VoIP GK registration delay. It is applicable to SAA GK registration delay probe only.
SourceVoicePort	This object is a string which specifies the voice-port on the source gateway. This object is applicable to RTP probe only.

Attribute	Usage
CallDuration	For more information about support for this attribute, see the documentation for the associated IP SLA MIB file.
LSPReplyDscp	<p>This object specifies the DSCP value to be set in the IP header of the LSP echo reply packet. The value of this object will be in the range of DiffServ codepoint values between 0 and 63.</p> <p><b>Note:</b> This object cannot be set to a value of 255. This default value specifies that DSCP is not set for this row.</p>
LSPNullShim	This object specifies whether to add the explicit-null label to LSP echo requests sent while performing RTT operations.

# Managing NetVoyant Services

---

Managing the NetVoyant Services takes place in the NetVoyant Console on the **Services** tab. The NetVoyant services are application processes that perform underlying NetVoyant functions, such as discovering your network (Topology Service), managing and sharing information about Management Information Bases (MIBs Service), collecting data from your devices (Polls Service), notifying you and your team of events in NetVoyant (Notify Service), receiving incoming SNMP traps (Traps Service), and collecting ICMP ping data from your devices (Ping Service).

This chapter covers the following topics:

- [“About the NetVoyant Services” on page 280](#)
- [“Managing NetVoyant Services” on page 281](#)
- [“Starting and Stopping Services” on page 281](#)
- [“Configuring a Service’s Start Mode or Logging Level” on page 283](#)

## ABOUT THE NETVOYANT SERVICES

The NetVoyant product runs the following services:

Service	Description	Functions
Topology	Responsible for discovering your devices, their capabilities, and supported data types and changes on your network.	<ul style="list-style-type: none"> <li>• Discovers and records the topology of your network within your discovery scope using ICMP and SNMP.</li> <li>• Discovers and records each device's SNMP support for MIB tables that are enabled for discovery.</li> <li>• Discovers and records changes in your network during regular re-discovery.</li> <li>• Records configuration changes that you make to your devices, poll instances, and interfaces.</li> <li>• Logs events relating to topology changes.</li> </ul>
MIBs	Responsible for managing and communicating MIB support.	<ul style="list-style-type: none"> <li>• Compiles new MIBs into the database.</li> <li>• Communicates which MIB tables are enabled for discovery to the Topology Service.</li> <li>• Provides you with information about supported MIBs in the MIB Browser.</li> </ul>
Polls	Responsible for collecting and preparing data from your devices.	<ul style="list-style-type: none"> <li>• Reads polling configuration from the database.</li> <li>• Collects and records data from your devices, poll instances, and interfaces.</li> <li>• Logs events related to device availability and threshold violations.</li> </ul>
Notify	Responsible for sending notifications according to your settings.	<ul style="list-style-type: none"> <li>• Processes events to determine whether they match configured event filters.</li> <li>• Sends notifications according to notification configuration.</li> </ul>
Traps	Responsible for receiving incoming SNMP traps.	<ul style="list-style-type: none"> <li>• Receives incoming SNMP traps.</li> <li>• Logs trap events.</li> </ul> <p><b>Note:</b> If you have the NetQoS Event Manager installed on the same machine with NetVoyant, the Event Manager trap receiver is disabled by default.</p>
Ping	Responsible for collecting polling data that requires ICMP pings, such as device availability and reachability.	<ul style="list-style-type: none"> <li>• Sends ICMP pings to your devices to collect polling data.</li> <li>• Records ICMP ping data to the database.</li> </ul>

**About the NetVoyant Service Manager.** The NetVoyant Service Manager is the Windows service used to start and stop the other NetVoyant services. You can start and stop the NetVoyant Service Manager from the Microsoft Management Console (MMC). For more information, see [“Starting and Stopping Services”](#) on page 281.



## MANAGING NETVOYANT SERVICES

You can perform most administrative tasks relating to the NetVoyant services on the **Services** tab in the NetVoyant Console.

On the Master server in a distributed system, you can manage all services running on the Master and on each remote poller. On a remote poller, you can manage all the services running on that poller. In a standalone system, you can manage all services on the Master Console. For more information about NetVoyant configuration types, see [“About the Master Server and Pollers” on page 21](#).

**Warning:** Starting, stopping, or configuring NetVoyant services can cause the NetVoyant product to stop functioning. Contact NetQoS technical support for assistance with these tasks.

You can perform the following tasks to manage NetVoyant services:

Task	More information
Start and stop services.	<a href="#">“Starting and Stopping Services” on page 281</a>
Configure each service’s start mode and logging level.	<a href="#">“Configuring a Service’s Start Mode or Logging Level” on page 283</a>

## STARTING AND STOPPING SERVICES

You can start and stop individual NetVoyant services on the **Services** tab in the NetVoyant Console. You can also start and stop NetVoyant services on an individual server by starting and stopping the NetVoyant Service Manager in the Microsoft Management Console.

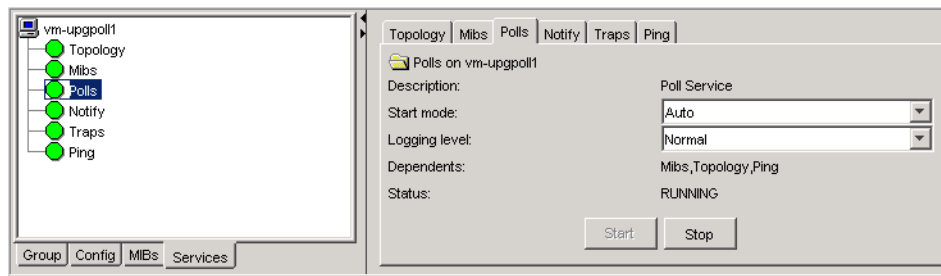
**Warning:** Stopping a service or the NetVoyant Service Manager can cause the NetVoyant product to temporarily stop collecting and reporting on data.

### Starting and Stopping Individual Services on the Services Tab

We recommend that you stop any services that list a dependent service before stopping the dependent service itself. You must start all dependencies of a service prior to starting a service. If you do not start dependencies before starting a service, the NetVoyant Service Manager starts the dependent services for you.

#### To start or stop a service on the Services tab:

1. In the NetVoyant Console, click the **Services** tab.
2. Under the NetVoyant Master server or remote poller (*distributed system only*), select the service.  
The details of the service appear in the context panel.



In particular, **Dependents** lists those services that must be started before starting this service. For example, the Polls service information in the preceding figure indicates that the Mibs, Topology, and Ping services are dependents. If the Polls service is not currently running, these other services must be running before you can start the Polls service.

3. Perform one of the following tasks:

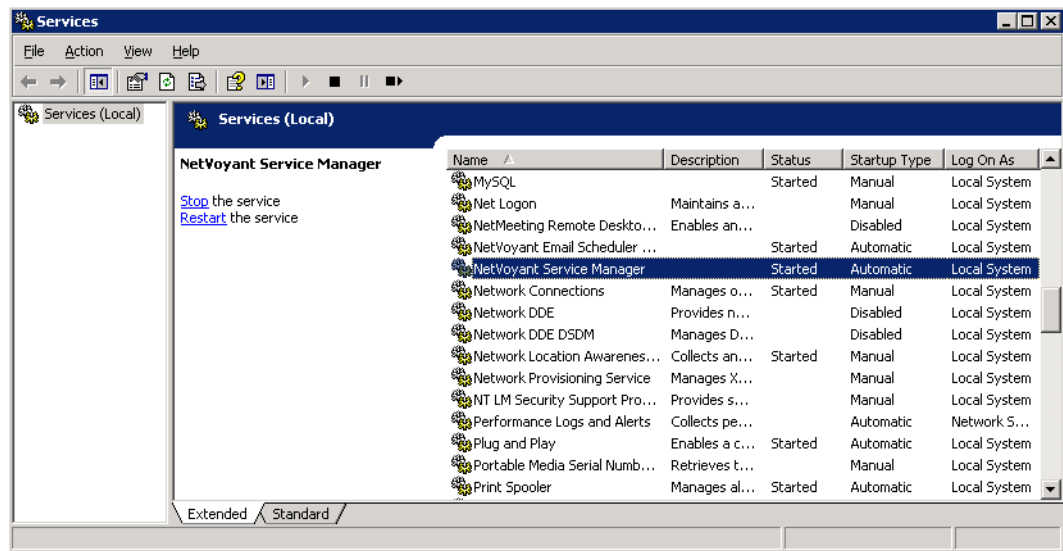
- To start the service, click **Start**.  
The service's status changes from STOPPED or FAILED to STARTING and then to RUNNING.
- To stop the service, click **Stop**.  
The service's status changes from RUNNING or STARTING to STOPPING and then to STOPPED.

## Starting or Stopping All Services

Services can also be managed in the Microsoft Management Console. If you are not familiar with using this administrative tool, see the Microsoft Management Console documentation.

### To start or stop NetVoyant services in the Microsoft Management Console:

1. On the Windows desktop, double-click the **Services** shortcut to open the Microsoft Management Console.  
If this shortcut is not present on the desktop, you can select **Administrative Tools > Services** from the Windows **Start** menu.
2. Scroll down to find the **NetVoyant Service Manager** service.



3. Perform one of the following tasks:

- To start the service, right-click the **NetVoyant Service Manager** service and select **Start**.
- To stop the service, right-click the **NetVoyant Service Manager** service and select **Stop**.

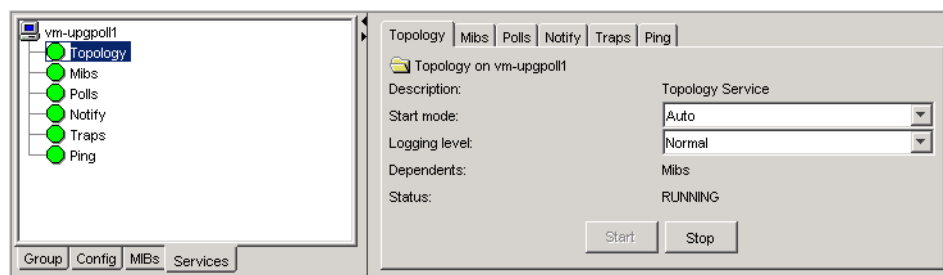
## CONFIGURING A SERVICE'S START MODE OR LOGGING LEVEL

Use the **Services** tab to configure the start mode of NetVoyant services and control how much logging information appears in the event log panel.

**To configure the start mode or logging level for a service:**

1. In the NetVoyant Console, click the **Services** tab.
2. Under the NetVoyant Master server or remote poller (*distributed system only*), select the service.

The details of the service appear in the context panel.



3. You can view and edit the following settings for a service:

Parameter	Edit enabled?	Description
<b>Description</b>	No	A brief description of the service.
<b>Start mode</b>	Yes	How the NetVoyant Service Manager starts the service. You can select one of the following start modes: <ul style="list-style-type: none"> <li>• <b>Auto</b> - Starts the service automatically when the system is rebooted.</li> <li>• <b>Manual</b> - Starts this service only when you manually initiate a start on the <b>Services</b> tab in the NetVoyant Console.</li> </ul>
<b>Logging level</b>	Yes	Determines how much logging information the service displays in the event log panel. Select one of the following logging levels: <ul style="list-style-type: none"> <li>• <b>Warning</b> - The service displays only logs that are not normal.</li> <li>• <b>Normal</b> - The service displays logs at a normal level.</li> <li>• <b>Normal (Debug)</b> - The service displays more logs than normal to assist with debugging.</li> <li>• <b>Normal (Verbose)</b> - The service displays as much information as possible in the event log.</li> </ul>
<b>Dependents</b>	No	The dependencies of a service.  Before a service starts, its dependent services must already be started. If you start a service before starting its dependents, the NetVoyant Service Manager first starts dependent services. If the dependent services fail to start, it does not start the service.
<b>Status</b>	No	The current running status of the service. A service can have one of the following statuses: <ul style="list-style-type: none"> <li>• <b>RUNNING</b> - The services is running normally.</li> <li>• <b>STOPPING</b> - The service is stopping.</li> <li>• <b>STOPPED</b> - The service is not running.</li> <li>• <b>STARTING</b> - The service is starting up after being stopped.</li> <li>• <b>FAILED</b> - The service failed to start and is not running.</li> </ul>

## Configuring Event Log Retention

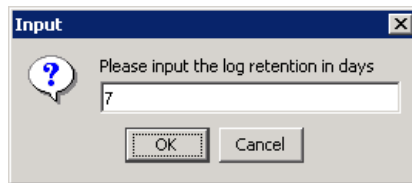
You can configure how long the NetVoyant product retains event logs, which are available in the NetVoyant Console event log panel and in Service Exception report views. For more information about the Service Exception views available in NetVoyant reports, see the *NetVoyant User Guide*.

**Note:** It is recommended that you retain log files for seven to 30 days.

### To configure event log retention:

1. From the **Logs** menu in the NetVoyant Console, select **Set log retention**.

This opens the **Input** dialog box.



2. Enter the length of time in days that you want to retain event logs.
3. Click **OK**.



# Reporting Administration

---

The security features in the NetVoyant reporting tool are similar to those of other NetQoS products and were designed for compatibility with the NetQoS Performance Center. Permissions to access report pages and perform certain tasks are tied to the roles associated with user accounts. An administrator creates a user account for each NetVoyant operator and determines his or her level of product privilege, or access. This design provides a flexible and secure way to determine the product features and reports that each different type of user can use or view.

The product privileges and roles associated with each user account can be shared among NetQoS products. After you register the NetVoyant product with the NetQoS Performance Center, you must manage users, roles, and permissions across all NetQoS products from the NetQoS Performance Center. You must have Administrator product privileges to add, edit, or delete a user.

The current versions of NetQoS NetVoyant and the NetQoS Performance Center support the NetQoS Single Sign-On product, which coordinates user accounts, permissions, and secure access among NetQoS products. An instance of the Single Sign-On software is automatically installed on each computer where a NetQoS product is installed. Single Sign-On settings, such as whether anonymous users are able to log in, control access to those products. More information about this software is provided in the *Single Sign-On Guide*, which is available on the NetQoS Self-Service Portal.

This chapter outlines administration tasks that are performed in the NetVoyant reporting interface. For more information about using the reporting interface to view and create reports for NetVoyant data, refer to the *NetVoyant User Guide*.

- “Changing Your User Account Password” on page 288
- “Configuring Email Servers and Schedules” on page 289
- “Editing the Report Menus” on page 292
- “Working with Roles and User Accounts” on page 295

## CHANGING YOUR USER ACCOUNT PASSWORD

When a NetVoyant administrator creates a user account, the account includes a password that enables the user to log into the NetVoyant reporting tool. As a user, you can change the password for your account at any time.

### To change your NetVoyant password:

1. From the **Report Pages** menu, select **Administration**.

The Administration page opens.



2. Under NetVoyant, click **Users**.

This lists your user account on the **View User Accounts** page.

**Note:** If the NetVoyant system is registered as a data source in the NetQoS Performance Center, this automatically opens the NetQoS Performance Center user interface to complete the task. For more information about changing your user password in the NetQoS Performance Center, see the *NetQoS Performance Center Administrator and User Guide*.

3. Select your user account and click **Edit**.

The **Edit User Account** page opens.

 A screenshot of the 'Edit User Account' form. The form has a title bar 'Edit User Account' and a sub-header 'Enter New User Information'. It contains several fields: 'Name' (text box with 'nvuser'), 'Description' (text box with 'NetVoyant User'), 'Password' (password box with dots), 'Confirm Password' (password box with dots), 'Role' (dropdown menu with 'Network Operator'), 'Type' (dropdown menu with 'Viewer'), and 'Permissions' (checkboxes for 'Enabled' and 'Allow user to export views'). There are 'Save' and 'Cancel' buttons at the bottom right.

4. Enter or edit the following parameters:

Parameter	Description
<b>Password</b>	Enter the new password for the user account. Passwords are limited to 20 characters.
<b>Confirm Password</b>	Re-enter the password to confirm.

5. Click **Save**.



## CONFIGURING EMAIL SERVERS AND SCHEDULES

NetVoyant administrators can configure a Simple Mail Transfer Protocol (SMTP) server that allows users to send or schedule emails in the NetVoyant reporting tool. Users can set up and edit their own email schedules if a NetVoyant administrator has configured the SMTP server. NetVoyant administrators can view, edit, or delete existing email schedules.

### Adding an SMTP Server

A NetVoyant administrator must configure a Simple Mail Transfer Protocol (SMTP) server to enable users to send or schedule emails in NetVoyant. If a user attempts to email a report page and an SMTP server has not been configured for the NetVoyant system, it will alert the user to contact an administrator.

#### To add an SMTP server to NetVoyant:

1. From the **Report Pages** menu, select **Administration**.

The Administration page opens.



2. In the NetVoyant section, click **Email Server**.

The **Email Server Settings** page opens.

 A screenshot of the 'Email Server Settings' form. The form has a title bar 'Email Server Settings' and a subtitle 'Enter Email Server Settings'. It contains the following fields:
 

- ☒ Enable Email
- SMTP Server Address: austext1.netqos.local
- Email Reply Address: administrator@yourcompany.com
- Email Format: HTML (selected from a dropdown menu)

 At the bottom right, there are 'Save' and 'Cancel' buttons.

3. Enter or edit the following settings:

Parameter	Description
<b>Enable Email</b>	Select to enable users to send and schedule emails in the NetVoyant reporting tool.
<b>SMTP Server Address</b>	Enter the IP address or name of the SMTP server.
<b>Email Reply Address</b>	Edit the email reply address. This address is used as the from address for sent emails.
<b>Email Format</b>	Select the format in which you want to send emails. <ul style="list-style-type: none"> <li>• HTML</li> <li>• Text</li> </ul>

4. Click **Save**.

This adds the designated SMTP server and enables users to send report pages in emails.

## Viewing, Editing, or Deleting an Email Schedule

NetVoyant users can create, edit or delete email schedules. Setting up an email schedule can automatically provide data for daily, weekly or monthly reports. Viewer and Designer user accounts can create a schedule when they email report pages and can only view or modify schedules they have created. NetVoyant administrators can view, edit, or delete all existing email schedules.

### To view, edit, or delete an email schedule:

1. From the **Report Pages** menu, select **Administration**.



The **Administration** page opens.

2. Under **User Settings**, click **Email Schedules**.

The **Email Schedules** page lists the currently configured email schedules.

Scheduled Email				
Owner ▲	Subject	Recipients	Schedule	Next Delivery
<input type="radio"/> nvadmin	Management Summary	manager@netqos.com	Weekly (America/Chicago)	-
<input checked="" type="radio"/> nvadmin	Top Deviation from Normal	admin@netqos.com	Weekly (America/Chicago)	7/28/2009 1:00 AM
<input type="radio"/> nvadmin	Top Closest to Threshold	admin@netqos.com	Weekly (America/Chicago)	8/2/2009 1:00 AM
<input type="radio"/> nvadmin	Operations Summary	manager@netqos.com	Every Mon - Fri (America/Chicago)	7/28/2009 1:00 AM

1 of 1

Max Per Page: 10 ▼

Edit Delete

**Note:** If there are no currently schedules emails, the page provides an alert for this condition.

3. To delete an email schedule, select the schedule and click **Delete**.
4. To view or edit an email schedule, select the schedule and click **Edit**.

5. You can view or edit the following settings:

Parameter	Description
<b>Owner</b>	<i>(Read-only)</i> The user account that created the email schedule.
<b>Sent To</b>	The email addresses to which the report page is sent.
<b>Subject</b>	The subject line for the email.
<b>Message</b>	The message sent in the body of the email.
<b>Time Zone</b>	The time zone used for generating the report data.
<b>Archive Email</b>	Select this check box to save a copy of the generated report PDF to a database. This does not archive the email message or recipient information.
<b>Scheduling Options</b>	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Send Daily</b> - Select which days of the week to send the email.</li> <li>• <b>Send Weekly</b> - Select which day of the week to send the email.</li> <li>• <b>Send Monthly</b> - Select to send the email on the last day of each month.</li> <li>• <b>Send Quarterly</b> - Select the last month of the first quarter (sends the email on the last day of each quarter).</li> <li>• <b>Send Yearly</b> - Select the last month of the year (sends the email on the last day of the year).</li> </ul>
<b>Send email at</b>	Use this setting to specify a time of day to send the email. By default, scheduled reports are generated just after midnight (typically around 1:00 a.m., as soon as nightly rollups are completed) in the selected time zone on the day or days selected in the scheduling options. This option specifies a time of day to send the email

6. Click **Save**.

## EDITING THE REPORT MENUS

Administrator and Designer user accounts can edit the titles for shared menus and the report pages that appear in each shared menu. Use this feature to customize the report menus for your organization so that the most useful reports are easy to access.

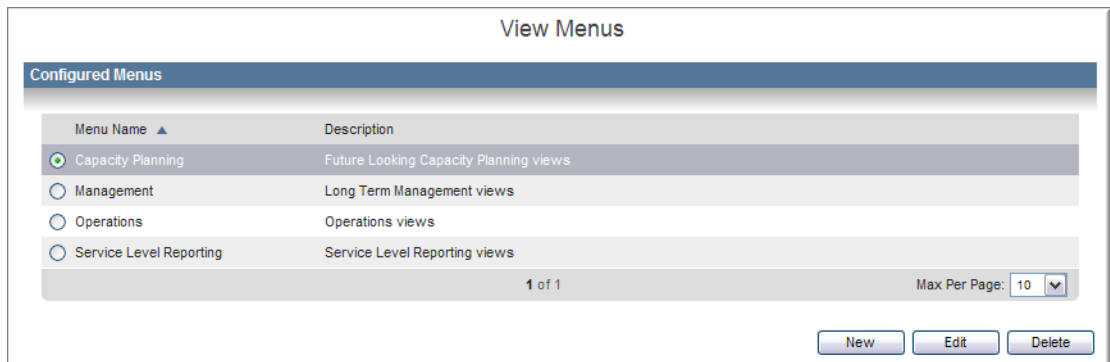
### To edit the report menu titles or report pages:

1. From the **Report Pages** menu, select **Administration**.



1. The **Administration** page opens.
2. Under **User Settings**, click **Menus**.

The **View Menu** page opens.



3. Perform one of the following actions:
  - To create a new menu, click **New**.
  - To edit an existing menu, select the menu and click **Edit**.
  - To delete a menu, select the menu and click **Delete**.

If you are adding a new menu or editing an existing one, the NetVoyant reporting tool displays the **Edit Report Menu** page.

4. Enter or edit the following parameters:

Parameter	Description
<b>Name</b>	Enter the name that you want to use as the heading for the menu.
<b>Description</b>	Enter a description to help you and other users identify what types of report pages are in the menu.
<b>Selected Pages</b>	<p>Perform the following actions to add, reorder, or remove the report pages that are listed in the menu:</p> <ul style="list-style-type: none"> <li>• To move a report page to the list of <b>Selected Pages</b>, select an existing report page from the list of <b>Available Pages</b> and click the right arrow.</li> <li>• To rearrange the report pages in the menu, click the up and down arrows.</li> <li>• To remove a report page from the menu, select a report page in the list of <b>Selected Pages</b> and click the left arrow.</li> </ul>

5. Perform one of the following actions:

- To save the report menu, click **Save**.
- To save the menu and add an additional menu, click **Save & Add Another**.

This adds the menu to the list of available menus.

6. Edit a role to provide access to the menu.

This adds the menu to the menu bar for that role. For more information about roles, see [“Working with Roles and User Accounts”](#) on page 295.

7. (Optional) Repeat step 6 to add the menu to other roles.

## Configuring Global Settings

You can configure the number of items that the NetVoyant reporting tool shows by default in all views; however, individual users can configure their own views to include a greater or lesser number of items while displaying a view on a report page. For more information, see [“Including More Data in a View”](#) on page 22.

**Note:** You must be a NetVoyant administrator to configure the global settings.

### To edit the global settings in NetVoyant:

1. From the **Report Pages** menu, select **Administration**.

The Administration page opens.



2. Under **NetVoyant**, click **Global Settings**.

The **Edit Global Settings** page opens.

A screenshot of the 'Edit Global Settings' page. The page has a title bar 'Edit Global Settings' and a subtitle 'Enter Global Settings For Views'. There are three input fields with labels: 'Default max rows for tables (200 max):', 'Default max pie chart slices (15 max):', and 'Default max rows for top-n bar/area charts (50 max):'. Each field has a value of '10' entered. At the bottom, there are 'Save' and 'Cancel' buttons.

3. You can edit the following global settings for views in the reporting interface:

Setting	Description	Default	Maximum
<b>Default max rows for tables</b>	Sets the maximum number of rows to display in table views.	10	200
<b>Default max pie chart slices</b>	Sets the maximum number of items to display in pie chart views.	10	15
<b>Default max rows for top-n bar/area charts</b>	Sets the maximum number of items to display in top-n bar and area charts.	10	50

4. Click **Save**.

This updates all views to reflect your changes.

## WORKING WITH ROLES AND USER ACCOUNTS

Roles define how users can access and interact with NetVoyant reports. An administrator must create a user account for each user that will log in to the NetVoyant reporting tool and assign one or more roles for the user. Assigning a role to a user account grants that user the access rights and menu access assigned to that role. Only a NetVoyant administrator can create and edit roles.

**Note:** If your installation of the NetVoyant product is bound to NetQoS Performance Center as a data source, roles and user accounts must be managed in the NetQoS Performance Center. For more information about managing user accounts and roles in the NetQoS Performance Center, see the *NetQoS Performance Center Administrator and User Guide*.

### NetVoyant Default Roles

The NetVoyant product installs with a set of default roles that are already defined and ready to use. These are standard roles that are used in most IT organizations and define the area access allocated to each user. Roles provide a means of protecting sensitive information based on organizational function.

The following are the default roles that are pre-configured for NetVoyant installations:

Role	Description	Access rights	Default Menus
Director of IT	Plans and directs the organization's information technology and manages the IT staff.	<ul style="list-style-type: none"> <li>• Enable Role</li> <li>• Drill into Views</li> <li>• Edit Share Views</li> <li>• Persist Shared View Edits</li> </ul>	<ul style="list-style-type: none"> <li>• My Pages</li> <li>• Service Level Reporting</li> </ul>
Network Engineer	Plans, implements, and supports network solutions and monitors network performance on a daily basis.	<ul style="list-style-type: none"> <li>• Enable Role</li> <li>• Drill into Views</li> <li>• Edit Share Views</li> <li>• Persist Shared View Edits</li> </ul>	<ul style="list-style-type: none"> <li>• My Pages</li> </ul>
Network Manager	Coordinates network solutions with engineers and operators and monitors network performance on a weekly basis.	<ul style="list-style-type: none"> <li>• Enable Role</li> <li>• Drill into Views</li> <li>• Edit Share Views</li> <li>• Persist Shared View Edits</li> </ul>	<ul style="list-style-type: none"> <li>• My Pages</li> <li>• Management</li> <li>• Capacity Planning</li> <li>• Service Level Reporting</li> <li>• Operations</li> </ul>
Network Operator	Monitors network performance and troubleshoots issues on a daily basis.	<ul style="list-style-type: none"> <li>• Enable Role</li> <li>• Drill into Views</li> <li>• Edit Share Views</li> <li>• Persist Shared View Edits</li> </ul>	<ul style="list-style-type: none"> <li>• My Pages</li> </ul>

Role	Description	Access rights	Default Menus
NOC Manager	Manages the network operations center and its personnel.	<ul style="list-style-type: none"> <li>• Enable Role</li> <li>• Drill into Views</li> <li>• Edit Share Views</li> <li>• Persist Shared View Edits</li> </ul>	<ul style="list-style-type: none"> <li>• My Pages</li> <li>• Capacity Planning</li> </ul>
VP of Infrastructure	Provides oversight and direction for maintaining and improving the organization's infrastructure.	<ul style="list-style-type: none"> <li>• Enable Role</li> <li>• Drill into Views</li> <li>• Edit Share Views</li> <li>• Persist Shared View Edits</li> </ul>	<ul style="list-style-type: none"> <li>• My Pages</li> <li>• Operations</li> </ul>

## Adding and Editing Roles

Roles define how users access and interact with NetVoyant views and reports. When a user account is assigned to a role, that user inherits the access rights for that role.

**Note:** If your installation of the NetVoyant product is bound to the NetQoS Performance Center as a data source, roles and user accounts must be managed in the NetQoS Performance Center. For more information about managing user accounts and roles in the NetQoS Performance Center, see the *NetQoS Performance Center Administrator and User Guide*.

### To add or edit a role:

1. From the **Report Pages** menu, select **Administration**.

The **Administration** page opens.



2. Under **User Settings**, click **Roles**.

The existing roles are listed on the **View User Roles** page.



**View User Roles**

**Configured Roles**

Current role: Network Manager

Role Name ▲	Description	Status	Users
<input checked="" type="radio"/> Director of IT	Plans and directs the organization's information technology and manages the IT staff.	Enabled	0
<input type="radio"/> Network Engineer	Plans, implements, and supports network solutions and monitors network performance on a daily basis.	Enabled	0
<input type="radio"/> Network Manager	Coordinates network solutions with engineers and operators and monitors network performance on a weekly basis.	Enabled	2
<input type="radio"/> Network Operator	Monitors network performance and troubleshoots issues on a daily basis.	Enabled	2
<input type="radio"/> NOC Manager	Manages the network operations center and its personnel.	Enabled	0
<input type="radio"/> VP of Infrastructure	Provides oversight and direction for maintaining and improving the organization's infrastructure.	Enabled	0

1 of 1 Max Per Page: 10 ▼

3. Perform one of the following actions:

- To create a new role click **New**.  
The **Add User Role** page opens.
- To edit an existing role, select the role and click **Edit**.  
The **Edit User Role** page opens.

**Add User Role**

**Enter Role Information**

Name:

Description:

Access Rights: ☒ Enable Role ☒ Drill into Views  
☒ Edit Shared Views ☒ Persist Shared View Edits

Menus For This Role:

Top Menu	Sub Menu	Description
<input checked="" type="radio"/> Report Pages:	<None>	<Please press the edit button to add sub menus to the Report Pages menu.>

1 of 1 Max Per Page: 10 ▼

4. Enter or edit the following settings for creating a new role or modifying an existing role:

Parameter	Description
<b>Name</b>	Enter or edit a name to identify the role.
<b>Description</b>	(Optional) Enter or edit the description of the role.

Parameter	Description
<b>Access Rights</b>	<p>Enable or disable the following rights (permissions):</p> <ul style="list-style-type: none"> <li>• <b>Enable Role</b> - Enables you and other NetVoyant administrators to assign this role to user accounts.</li> <li>• <b>Drill into Views</b> - Enables users in this role to click views to drill into more detailed information.</li> <li>• <b>Edit Shared Views</b> - Enables users in this role to edit menus, report pages, and views that are shared with other users. All users can edit the report pages and views in the My Pages menu.</li> <li>• <b>Persist Shared View Edits</b> - If the role can edit shared views, this right enables those changes to be seen by other users and maintained by the NetVoyant reporting tool. If you disable this access right, changes made by a user in this role to shared menus, pages, or views are not visible to other users and are removed when the user logs out.</li> </ul>
<b>Menus For This Role</b>	<p>To configure what menus are visible to users in the role, click <b>Edit</b> and perform the following actions:</p> <ul style="list-style-type: none"> <li>• To enable a menu, select the menu in the list of <b>Available Sub Menus</b> and click the right arrow to move it to the list of <b>Selected Sub Menus</b>.</li> <li>• To remove a menu, select the menu in the list of <b>Selected Sub Menus</b> and click the left arrow to move it to the list of <b>Available Sub Menus</b>.</li> <li>• To rearrange a menu, select the menu and click the up or down arrow.</li> </ul> <p>Click <b>OK</b> when you are finished.</p>

5. Perform one of the following actions:

- To save the role, click **Save**.
- To save the role and add an additional role, click **Save & Add Another**.

This creates the role and you can now apply the role to existing or new user accounts.

**Note:** You can proxy a role to validate how users in that role can view and manipulate report pages in the NetVoyant reporting interface before assigning users to the role. For more information, see “Proxying a Role” on page 304.

### To delete a role:

1. From the **Report Pages** menu, select **Administration**.

The Administration page opens.

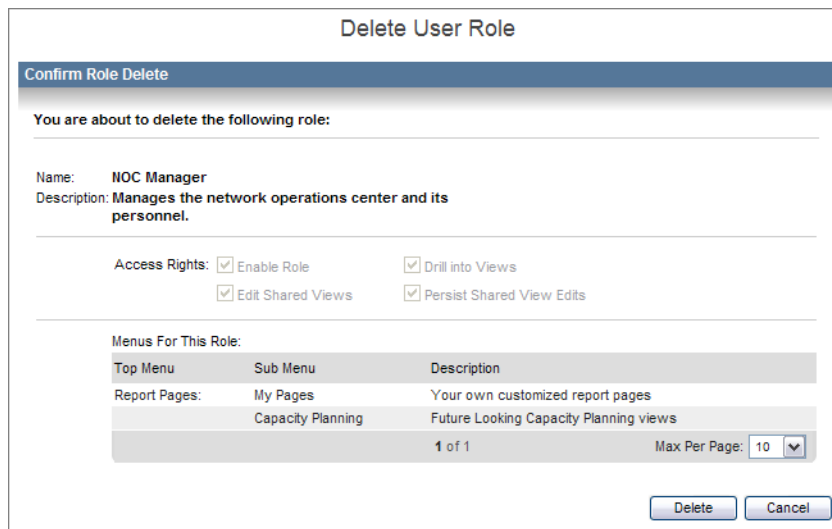


2. Under **User Settings**, click **Roles**.

This lists the existing roles on the **View User Roles** page.

3. Select the role and click **Delete**.

This opens the **Delete User Role** page, which displays information about the role so that the administrator can review it before removing the role.



**Delete User Role**

**Confirm Role Delete**

You are about to delete the following role:

Name: **NOC Manager**  
 Description: **Manages the network operations center and its personnel.**

Access Rights: ☒ Enable Role ☒ Drill into Views  
☒ Edit Shared Views ☒ Persist Shared View Edits

Menus For This Role:

Top Menu	Sub Menu	Description
Report Pages:	My Pages	Your own customized report pages
	Capacity Planning	Future Looking Capacity Planning views

1 of 1 Max Per Page: 10

Delete Cancel

4. To confirm, click **Delete**.

## Adding or Editing a NetVoyant User

As a NetVoyant administrator, you can add new users as well as edit user accounts. You set a password that the user can change later or you can reset a password if a user has forgotten it.

**Note:** If your installation of the NetVoyant product is bound to the NetQoS Performance Center as a data source, roles and user accounts must be managed in the NetQoS Performance Center. For more information about managing user accounts and roles in NetQoS Performance Center, see the *NetQoS Performance Center Administrator and User Guide*.

### To add or edit a NetVoyant user:

1. From the **Report Pages** menu, select **Administration**.

The **Administration** page opens.



2. Under **User Settings**, click **Users**.

This lists the existing user accounts on the **View User Accounts** page.

3. Perform one of the following actions:

- To create a new user account, click **New**.  
The **Add New User** page opens.
- To edit an existing user account, select the user account and click **Edit**.  
The **Edit User Account** page opens.
- To delete a user account or multiple user accounts, select the user account and click **Delete**.

4. Enter or edit the following parameters:

Parameter	Description
<b>Name</b>	Enter or edit the name for the user account, which is used to log in to the NetVoyant product.
<b>Description</b>	<i>(Optional)</i> Enter or edit a description of the user account.
<b>Email Address</b>	Enter an email address for the user.
<b>Password</b>	Enter or edit the password for the user account, which is used to log in to the NetVoyant product. The password is limited to 20 characters.
<b>Confirm Password</b>	Re-enter the password to confirm.
<b>Time Zone</b>	<p>Select a time zone for the user.</p> <p>The time zone determines how reports label data with time for this user. For example, if a user has a time zone of Central Standard Time (CST) instead of the default of Universal Coordinated Time (UTC) and the user views a report with data for 8:00 a.m.to 9:00 a.m., the NetVoyant reporting tool displays data for 8:00 a.m. to 9:00 a.m. CST.</p>
<b>Role</b>	<p>Select a role to determine user permissions and available menus for the user account.</p> <p>For more information about Netvoyant user roles, see <a href="#">“NetVoyant Default Roles”</a> on page 295 and <a href="#">“Adding and Editing Roles”</a> on page 296.</p>
<b>Type</b>	<p>Select one of the following user account types:</p> <ul style="list-style-type: none"> <li>• <b>Administrator</b> - A NetVoyant administrator manages user accounts and roles and performs other administrative tasks. An administrator can also edit and create report pages, views, and menus.</li> <li>• <b>Designer</b> - A designer can edit and create report pages, views, and shared menus. (This is equivalent to the Power User account type in the NetQoS Performance Center.)</li> <li>• <b>Viewer</b> - A viewer can view report pages and add report pages to their own My Pages menu.(This is equivalent to the User account type in the NetQoS Performance Center.)</li> </ul>

Parameter	Description
<b>Permission Group</b>	<i>(Optional)</i> To indicate which devices or networks a user can view or access in NetVoyant reports, click <b>Change Group</b> . For more information about setting permission groups for a user account, see <a href="#">“Changing User Permission Groups” on page 301</a> .
<b>Allow user to export views</b>	Select this setting to enable the user to generate URLs for views or export the SQL commands for a view.
<b>Enabled</b>	Select to make the user account active. If this option is not selected, the user cannot log in to the NetVoyant product.

5. Perform one of the following actions:

- To save the user account, click **Save**.
- To save the user account and create an additional user account, click **Save & Add Another**.

NetVoyant creates the user account.

**Note:** As an administrator, you can proxy a user account to validate how the user can view and manipulate report pages in the NetVoyant reporting interface before making the account available to the user. For more information, see [“Proxying a User Account” on page 302](#).

## Changing User Permission Groups

Permission groups determine the data that can be accessed by the user account. The groups created by a NetVoyant administrator to create meaningful reports and views are assigned in the User Account settings to determine what groups and managed objects can be included in reports for that user. This helps to streamline reporting for the user by filtering the data to their area of responsibility. It also provides added security within an organization by restricting users to only the data that they should access.

**Note:** If your installation of the NetVoyant product is bound to the NetQoS Performance Center as a data source, roles and user accounts must be managed in the NetQoS Performance Center. For more information about managing user accounts and roles in the NetQoS Performance Center, see the *NetQoS Performance Center Administrator and User Guide*.

### To change the Permission Groups for a user:

1. In the **Edit User Account** page, click **» Change Group**.

For more information about opening the Edit User Account page to modify user account settings, see [“Adding or Editing a NetVoyant User” on page 299](#).

Select Group

Use the search option to search for a more limited group of choices.

Group Filter:  Search

Path	Members	Description
/	2	
/Devices	10	
/Devices/Firewalls	0	
/Devices/Hubs	0	
/Devices/Network Termination	0	
/Devices/Other	0	
/Devices/Printers	0	
/Devices/Probes	0	
/Devices/Routers	0	
/Devices/Servers	0	

1 2 3 4 5 6 Max Per Page: 10

Cancel

This opens the **Select Group Permissions** dialog box, which lists groups, networks, and custom groups, as well as the number of devices (members) in each group, and a description.

- (Optional) In the dialog box, enter a **Group Filter** and click **Search** to limit the groups by name.

You can use \* as a wildcard. For example, you can enter Aus\* to display only those groups that begin with the text “Aus” in their names, such as Austin, Australia, Austria, and so on.

To display more groups, select a larger **Size** from the list at the lower-right corner of the group list.

- To limit what the user can view to a group or network, click the name of group or network.

**Note:** When you select a parent group, all child groups (or sub-groups) are included. Groups should be organized in such a way so that devices and networks are members of groups according to area of responsibility and access requirements.

This closes the dialog box, and the selected group appears in the **Edit User Account** page next to the **Permission Group** setting.

Permission Group: Servers Change Group

☐ Allow user to export views

☒ Enabled

- Click **Save** to save the changes to user account.

## Proxying a User Account

Proxying a user account enables you to validate significant changes or enhancements to the available report pages. Only a NetVoyant administrator can proxy a user account. As an administrator, you can also proxy a user account to create a new report page in the My Pages menu for that user. For more information about adding a report page to a user’s My Pages menu, see [“Adding Pages to a User’s My Pages Menu” on page 303](#).

As a proxy, you view and manipulate pages in the NetVoyant reporting tool in exactly the same way as the role or user account that you assume.

**Note:** If your installation of the NetVoyant product is bound to the NetQoS Performance Center as a data source, roles and user accounts must be managed in NetQoS Performance Center. For more

information about managing user accounts and roles in the NetQoS Performance Center, see the *NetQoS Performance Center Administrator and User Guide*.

### To proxy a user account:

1. From the **Report Pages** menu, select **Administration**.

The Administration page opens.



2. Under **User Settings**, click **Users**.

This lists the existing user accounts on the **View User Accounts** page.

Configured User Accounts				
User Name ▲	Type	Role	Permissions	Status
<input type="checkbox"/> nqadmin	Administrator	Network Manager	/	Built-In
<input checked="" type="checkbox"/> nquser	Viewer	Network Operator	/	Built-In
<input type="checkbox"/> nvadmin	Administrator	Network Manager	/	Built-In
<input type="checkbox"/> nvuser	Viewer	Network Operator	/	Built-In

1 of 1 Max Per Page: 10 ▼

Proxy New Edit Delete

3. Select the user account and click **Proxy**.
4. Perform the required actions or test the user account.
5. Log out of the NetVoyant reporting tool to return to your own user account.

## Adding Pages to a User's My Pages Menu

The **My Pages** menu enables users to collect private report pages that contain the report views most useful to them. As a NetVoyant administrator, you can add a report page to a user's My Pages menu by proxying the user account and adding the report page directly. You must be a NetVoyant administrator to add report pages to other users' My Pages menus.

**Note:** If your installation of the NetVoyant product is bound to the NetQoS Performance Center as a data source, roles and user accounts must be managed in NetQoS Performance Center. For more information about managing user accounts and roles in NetQoS Performance Center, see the *NetQoS Performance Center User Guide*.

### To add a page to a user's My Pages menu:

1. Proxy the user's account.

For more information about proxying a user's account, see [“Proxying a User Account” on page 302](#).

2. Add the page or pages to the **My Pages** menu.
3. Log out of the NetVoyant reporting tool.

When the user logs in, the NetVoyant reporting tool displays the report page on the **My Pages** menu.

## Proxying a Role

Proxying a role enables you to validate significant changes or enhancements to available report pages. As a proxy, you view and manipulate pages in the NetVoyant reporting tool in exactly the same way as the role that you assume. You must be a NetVoyant administrator to proxy a role.

You can also proxy an individual user account. For more information, see [“Proxying a User Account”](#) on page 302.

**Note:** If your installation of the NetVoyant reporting tool is bound to the NetQoS Performance Center as a data source, roles and user accounts must be managed in NetQoS Performance Center. For more information about managing user accounts and roles in NetQoS Performance Center, see the *NetQoS Performance Center User Guide*.

### To proxy a user role:

1. From the **Report Pages** menu, select **Administration**.

The Administration page opens.



2. Under **User Settings**, click **Roles**.

The **View User Roles** page opens and lists the existing roles. Your current role appears at the top of the list in the displayed page.

View User Roles

Configured Roles

Current role: Network Manager

Role Name ▲	Description	Status	Users
<input checked="" type="radio"/> Director of IT	Plans and directs the organization's information technology and manages the IT staff.	Enabled	0
<input type="radio"/> Network Engineer	Plans, implements, and supports network solutions and monitors network performance on a daily basis.	Enabled	0
<input type="radio"/> Network Manager	Coordinates network solutions with engineers and operators and monitors network performance on a weekly basis.	Enabled	2
<input type="radio"/> Network Operator	Monitors network performance and troubleshoots issues on a daily basis.	Enabled	2
<input type="radio"/> NOC Manager	Manages the network operations center and its personnel.	Enabled	0
<input type="radio"/> VP of Infrastructure	Provides oversight and direction for maintaining and improving the organization's infrastructure.	Enabled	0

1 of 1

Max Per Page: 10 ▼

Proxy

New

Edit

Delete

3. Select the role and click **Proxy**.



The **Current role** appears at the top of the list changes to reflect the proxied role.

4. Perform the required actions or test the role.
5. Return to the **View User Roles** page and click **Return Role**.



# NetVoyant Properties and Operators

---

Properties are variables that the NetVoyant product uses to customize the definition of objects, such as devices, events, interfaces, or poll instances. You can use properties in expressions, alarm thresholds, and notifications.

You can use the NetVoyant operators when creating or editing expressions and thresholds.

This appendix covers the following topics:

- [“Working with NetVoyant Properties” on page 308](#)
- [“Adding, Viewing, or Setting Values for Properties” on page 316](#)
- [“Using NetVoyant Operators in Expressions” on page 319](#)

## WORKING WITH NETVOYANT PROPERTIES

The NetVoyant product includes default properties defined for your objects in the NetVoyant product; for example, `ifSpeed` or `ifName` for interface speed and interface name. You can also create your own properties and edit the values for properties.

You can modify the defined properties on the **Show All Properties** tab for a device, poll instance, or interface.

You can view properties for a dataset on the **Properties** tab. These properties should be modified only under the supervision of NetQoS Technical Support or Professional Services staff. For more information, see [“Using Dataset Properties” on page 111](#).

**Note:** When you refer to a property in an expression, place a \$ symbol before its name; for example, `$ifSpeed`.

### Using Properties in Dataset Expressions

There are many default properties that you can use to include dynamic content in your expressions.

#### Using a Default Property in a Normal Dataset Expression

You could use the pre-defined `ifSpeed` property, which represents an interface’s speed setting that you can configure by interface. The NetVoyant product uses this property to define interface utilization using the following expression:

```
((ifInOctets+ifOutOctets)*800)/(duration*$ifSpeed)
```

**Note:** The “duration” is a built-in variable that returns the duration of the polling interval in seconds.

This expression defines the utilization of an interface in the Interface Statistics dataset based upon the two OIDs `ifInOctets` and `ifOutOctets`, the duration of the polling interval, and the value for the `ifSpeed` property, which is set and can be configured by interface.

#### Default Poll Instance and Interface Properties

The following are many of the built-in poll instance and interface properties you can use in expressions:

Property	Description
<code>CirIn</code>	<i>(Frame Relay circuits only)</i> The incoming Committed Information Rate for a frame relay circuit, which indicates how much bandwidth is guaranteed by your service provider. The <code>CirIn</code> can range from zero to the <code>EirIn</code> .
<code>CirOut</code>	<i>(Frame Relay circuits only)</i> The outgoing Committed Information Rate for a frame relay circuit, which indicates how much bandwidth is guaranteed by your service provider. The <code>CirOut</code> can range from zero to the <code>EirOut</code> .
<code>EirIn</code>	<i>(Frame Relay circuits only)</i> The incoming Excess Information Rate for a frame relay circuit, which is typically the circuit speed.
<code>EirOut</code>	<i>(Frame Relay circuits only)</i> The outgoing Excess Information Rate for a frame relay circuit, which is typically the circuit speed.
<code>ifIndex</code>	The index for the interface’s SNMP <code>ifEntry</code> table.

Property	Description
ifName	The name of the interface; for example, Serial1/0.
ifSpeed	<i>(Interfaces only)</i> An interface's speed as defined by the ifSpeed field in the SNMP ifEntry table; for example, 1.54 Mbps. You can configure an interface's speed in the NetVoyant Console by editing the ifSpeed field for the interface. For more information, see <a href="#">“Editing the Interface Speeds” on page 170</a> .
ifSpeed_in	<i>(Interfaces only)</i> An interface's inbound speed as defined by the ifSpeed_in field in the SNMP ifEntry table; for example, 1.54 Mbps. You can configure an interface's speed in the NetVoyant Console by editing the ifSpeed_in field for the interface. For more information, see <a href="#">“Editing the Interface Speeds” on page 170</a> .
ifSpeed_out	<i>(Interfaces only)</i> An interface's inbound speed as defined by the ifSpeed_out field in the SNMP ifEntry table; for example, 1.54 Mbps. You can configure an interface's speed in the NetVoyant Console by editing the ifSpeed_out field for the interface. For more information, see <a href="#">“Editing the Interface Speeds” on page 170</a> .
ifType	<i>(Interfaces and Frame Relay circuits only)</i> An interface or circuit's type as defined by the ifType field in the SNMP ifEntry table; for example, frame-relay.

## Using Properties in Notifications

You can use default notification properties to trigger notifications and include in notification messages. These event properties are available in the **Filter Definition** dialog box when set the filter expression for a subscribed event type for a notification. For more information about using filter expressions in notifications, see [“Writing an Event Filter Expression” on page 241](#).

**Note:** Display the details for an event to view properties you can use to filter the events that trigger a notification or to provide information in notification messages.

The following are properties that you can use in notifications:

Property	Description
domain_name	This is always the “NetworkManagement” string. It is generally not very useful for notifications.
event_name	<p>A description of the event that triggered a notification. Including the description of an event in a notification message can enable you to quickly identify the source of the event.</p> <p>Example description for a polling event</p> <p>avail: polling failed for 10.0.7.249: 100% SNMP Loss</p> <p>Example description for a threshold event</p> <p>Threshold exceeded for 10.0.7.10:1 (in_discardrate = 45.312500)</p>

Property	Description
type_name	<p>The type of event that triggered a notification. Events can be one of the following types:</p> <ul style="list-style-type: none"> <li>• <b>Log:</b> Log events track actions that NetVoyant services perform along with topology changes in your network or devices. You can configure the logging level of the NetVoyant services. For more information, see <a href="#">“Configuring a Service’s Start Mode or Logging Level”</a> on page 283.</li> <li>• <b>Polling:</b> Polling events track the SNMP polls that NetVoyant sends to your devices. Polling alarms indicate that a device did not respond to an SNMP request during a scheduled polling cycle.</li> <li>• <b>Trap:</b> Trap events track incoming SNMP traps. You can configure new trap events for the types of SNMP traps that you expect the NetVoyant product to receive. For more information, see <a href="#">“Adding or Editing an SNMP Trap Event”</a> on page 325.</li> <li>• <b>Threshold:</b> Threshold events track threshold violations on your devices. A threshold event occurs when a value for an expression goes beyond a threshold limitation value that you set for the alarm rule. You can configure threshold events by specifying threshold triggered and cleared values in an alarm rule. For more information, see <a href="#">“Defining Thresholds for Alarm Rules”</a> on page 201.</li> </ul>
Address	<p>The IP address of the device.</p> <p><b>Note:</b> The device name can be a name or an IP. This is always the IP address.</p>
Dataset	<p>The name of the dataset that contains the expression threshold that triggered a notification.</p> <p>For example, if a notification is triggered by a device being unavailable, the Dataset is avail (Device Availability).</p>
Device	<p>The device that initiated the event that triggered a notification. You can use the Device property to trigger notifications for specific devices.</p> <p>For example, you can configure the NetVoyant product to send a notification email to an operations team when a mission-critical server becomes unavailable. For more information, see <a href="#">“Triggering Notifications by Device Name or Address”</a> on page 244.</p>
EventCategory	<p>The category of the event that triggered a notification.</p> <p>An event can be one the following categories:</p> <ul style="list-style-type: none"> <li>• <b>Status:</b> Indicates that a status change occurred. Polling events are in the status category.</li> <li>• <b>Threshold:</b> Indicates that a threshold event occurred.</li> <li>• <b>Configuration:</b> Indicates that a configuration change occurred.</li> </ul>
EventCode	<p>This is the SNMP status for the event. It is useful in some polling cases to show the raw SNMP status (timeout, transport problem, an so on).</p>

Property	Description
EventCleared	<p>Indicates whether an event has cleared. This occurs when the offending expression value returns below the threshold-cleared value or when you manually clear an event.</p> <p>You can use the <code>EventCleared</code> property to trigger notifications for events that have continued for a sustained period and have not yet cleared. For example, you can configure the NetVoyant product to send a notification email when interface utilization has been over threshold for one hour and has not cleared.</p> <p><code>EventCleared</code> can have the following values:</p> <ul style="list-style-type: none"> <li>• <b>0</b> - Indicates that the event has not yet cleared.</li> <li>• <b>non-zero value</b> - Indicates that the event has cleared.</li> </ul>
EventDuration	<p>The length of time in seconds since an event started. For example, this has a value of 3600 for an event that has lasted an hour. You can use the <code>EventDuration</code> property to trigger notifications for events that continue for a sustained period.</p> <p>For example, you can configure the NetVoyant product to send a notification email when interface utilization has been over threshold for one hour.</p> <p><b>Important:</b> If you do not raise the Threshold Notification Limit or Polling Notification Limit settings above the default of 1, it does not recognize events that last for more than one polling cycle as one occurrence and thus all events have an event duration of zero. For more information, see <a href="#">“Using Polling Notification Limits” on page 249</a>.</p> <p>For more information, see <a href="#">“Using the Event Duration Property” on page 252</a>.</p>
EventSequence	The unique sequence number generated for each event.
EventServer	The name of the server that originated the event. For a distributed system, this provides information about which poller generated the alarm.
EventSeverity	<p>The severity of the event that triggered a notification. You can use the <code>EventSeverity</code> property to trigger different types of notifications for different types of events.</p> <p>For example, you can configure the NetVoyant product to send notification emails only for Critical threshold events. For more information, see <a href="#">“Triggering Notifications by Event Severity” on page 247</a>.</p> <p>Events can be one of the following severity levels:</p> <ul style="list-style-type: none"> <li>• Normal</li> <li>• Warning</li> <li>• Minor</li> <li>• Major</li> <li>• A custom event severity. For more information, see <a href="#">“Configuring Event Severities” on page 224</a>.</li> </ul>
EventSupplier	The service that initiated the event that triggered a notification. For more information on NetVoyant services, see <a href="#">“About the NetVoyant Services” on page 280</a> .

Property	Description
EventTimestamp	<p>The date and time at which the event that triggered a notification was received. You can use the EventTimestamp property to trigger notifications for events that occurred at a given time.</p> <p>For example, you can configure the NetVoyant product to send a notification email to an operation team only when an event occurs after 7 p.m. server time.</p>
ExpressionName	<p>The name of the expression that triggered a notification.</p> <p>For example, if a notification is triggered by an interface with utilization over threshold, the ExpressionName is ifutil from the Interface Statistics dataset.</p>
ExpressionThreshold	<p>The threshold value that was crossed for this alarm. For example, if the threshold test is ifutil &gt; 50, then ExpressionThreshold would be 50.</p>
ExpressionValue	<p>The value of the expression for the poll instance that triggered a notification.</p> <p>For example, if a notification is triggered by an interface with utilization of 93.15%, the ExpressionValue would be 93.15.</p>
PollInstance	<p>The poll instance that initiated the event that triggered a notification.</p>
Profile	<p>The name of the alarm profile that contains the alarm rule and threshold that was exceeded or cleared.</p>
Rule	<p>The name of the alarm rule that contains the threshold that was exceeded or cleared.</p>
URL	<p>A system generated URL that links to a report for the object that generated the alarm.</p>
ErrorCode	<p>A code to assist technical support in diagnosing issues.</p> <p>It is generally the same as the EventCode.</p>
EventDevice	<p>The numeric identifier for the device that initiated the event that triggered a notification.</p>
EventPollInstance	<p>The numeric identifier for the poll instance that initiated the event that triggered a notification.</p>
EventSource	<p>The service or device that initiated the event that triggered the notification.</p> <p>For more information on NetVoyant services, see <a href="#">“About the NetVoyant Services” on page 280</a>.</p>



Property	Description
EventType	<p>The type of event that triggered a notification. Events can be one of the following types:</p> <ul style="list-style-type: none"> <li>• <b>Log:</b> Log events track actions that NetVoyant services perform along with topology changes in your network or devices. You can configure the logging level of the NetVoyant services. For more information, see <a href="#">“Configuring a Service’s Start Mode or Logging Level” on page 283.</a></li> <li>• <b>Polling:</b> Polling events track the SNMP polls that NetVoyant sends to your devices. Polling alarms indicate that a device did not respond to an SNMP request during a scheduled polling cycle.</li> <li>• <b>Trap:</b> Trap events track incoming SNMP traps. You can configure new trap events for the types of SNMP traps that you expect the NetVoyant product to receive. For more information, see <a href="#">“Adding or Editing an SNMP Trap Event” on page 325.</a></li> <li>• <b>Threshold:</b> Threshold events track threshold violations on your devices. A threshold event occurs when a value for an expression goes above the threshold exceeded value that you set for the expression. You can configure threshold events by specifying threshold triggered and cleared values in an alarm rule. For more information, see <a href="#">“Defining Thresholds for Alarm Rules” on page 201.</a></li> </ul>
SNMPEnterpriseID	<p>The SNMP Enterprise ID of the SNMP agent sending the SNMP trap that triggered a notification.</p> <p>This is only valid for v1 traps.</p>
TrapCommunity	The SNMP profile used to authenticate the sender that sent an SNMP trap that triggered a notification.
TrapName	The name of the trap event that triggered a notification, if it has been configured.
TrapType	<p>The trap type of an SNMP trap that triggered a notification.</p> <p>The type of SNMP trap is indicated by the SNMP agent’s MIB definition. The TrapType defines what variables are sent as variable bindings in the MIB-specific bindings and the purpose of the trap.</p>
TrapUpTime	The time at which the device sent the SNMP trap that triggered a notification.
TrapVersion	The version number of the trap that triggered a notification.
Variable bindings	Fields that are unique to the SNMP trap or SNMP agent that initiated the SNMP trap that triggered a notification. For more information, see <a href="#">“Using Variable Bindings” on page 330.</a>

## Using Event Properties

You can view default properties called event properties in event and alarm logs. All event properties can be used as notification properties.

Property	Description
EventType	<p>The type of event that triggered a notification.</p> <p>Events can be one of the following types:</p> <ul style="list-style-type: none"> <li>• <b>Log:</b> Log events track actions that NetVoyant services perform along with topology changes in your network or devices. You can configure the logging level of the NetVoyant services. For more information, see <a href="#">“Configuring a Service’s Start Mode or Logging Level” on page 283.</a></li> <li>• <b>Polling:</b> Polling events track the SNMP polls that NetVoyant sends to your devices. Polling alarms indicate that a device did not respond to an SNMP request during a scheduled polling cycle.</li> <li>• <b>Trap:</b> Trap events track incoming SNMP traps. You can configure new trap events for the types of SNMP traps that you expect the NetVoyant product to receive. For more information, see <a href="#">“Adding or Editing an SNMP Trap Event” on page 325.</a></li> <li>• <b>Threshold:</b> Threshold events track threshold violations on your devices. A threshold event occurs when a value for an expression goes above the threshold exceeded value that you set for the expression. You can configure threshold events by specifying threshold triggered and cleared values in an alarm rule. For more information, see <a href="#">“Defining Thresholds for Alarm Rules” on page 201.</a></li> </ul>
EventTimestamp	The date and time at which the event was received.
EventSource	The service or device that initiated the event.
EventSeverity	<p>The severity of the event.</p> <p>Events can be one of the following severities:</p> <ul style="list-style-type: none"> <li>• Normal</li> <li>• Warning</li> <li>• Minor</li> <li>• Major</li> <li>• A custom event severity. (For more information, see <a href="#">“Configuring Event Severities” on page 224.</a>)</li> </ul>
EventCategory	<p>The category of the event.</p> <p>An event can be one the following categories:</p> <ul style="list-style-type: none"> <li>• <b>Status:</b> Indicates that the a status change occurred. Polling events are in the status category.</li> <li>• <b>Threshold:</b> Indicates that a threshold event occurred.</li> <li>• <b>Configuration:</b> Indicates that a configuration change occurred.</li> </ul>
ErrorCode	A code to assist technical support in diagnosing issues.

Property	Description
EventCleared	<p>Indicates whether an event has cleared. This occurs when the offending expression value returns below the threshold cleared value or when you manually clear an event.</p> <p>You can use the <code>EventCleared</code> property to trigger notifications for events that continued for a sustained period and have not yet cleared.</p> <p>For example, you can configure the NetVoyant product to send a notification email when interface utilization has been over threshold for one hour and has not cleared.</p> <p><code>EventCleared</code> can have the following values:</p> <ul style="list-style-type: none"> <li>• <b>0</b> - Indicates that the event has not yet cleared.</li> <li>• <b>non-zero value</b> - Indicates that the event has cleared.</li> </ul>
EventDuration	<p>The length of time in seconds since an event started.</p> <p>For example, it has a value of 3600 for an event that lasted an hour.</p> <p>You can use the <code>EventDuration</code> property to trigger notifications for events that continued for a sustained period.</p> <p>For example, you can configure the NetVoyant product to send a notification email when interface utilization has been over threshold for one hour.</p> <p><b>Important:</b> If you do not raise the Threshold Notification Limit or Polling Notification Limit settings above the default of 1, it does not recognize events that last for more than one polling cycle as one occurrence and thus all events have an event duration of zero. For more information, see <a href="#">“Using Polling Notification Limits” on page 249</a>.</p> <p>For more information, see <a href="#">“Using the Event Duration Property” on page 252</a>.</p>
EventDevice	The numeric identifier for the device that initiated the event.
EventPollInstance	The numeric identifier for the poll instance that initiated the event.
Device	The device that initiated the event.
PollInstance	The poll instance that initiated the event.
Variablebindings	Fields supplied by the SNMP agent that initiated the trap that are unique to the SNMP trap or SNMP agent type. For more information, see <a href="#">“Using Variable Bindings” on page 330</a> .
TrapCommunity	The SNMP profile used to authenticate the trap sender.
TrapName	The name of the trap event, if it has been configured.
TrapType	The type of SNMP trap as indicated by the SNMP agent’s MIB definition. The <code>TrapType</code> defines what variables are sent as variable bindings in the MIB-specific bindings and the purpose of the trap.
TrapUpTime	The time at which the device sent the trap.
SNMPEnterpriseID	SNMP Enterprise ID of the SNMP agent sending the trap.
TrapVersion	The version number of the trap.

## ADDING, VIEWING, OR SETTING VALUES FOR PROPERTIES

Properties are variables used to customize the definition of objects, such as devices or poll instances. You can use properties in expressions, notifications, and reports.

The NetVoyant product includes default properties defined for your objects; for example, `ifSpeed` and `ifName` for interface speed and interface name. You can also create your own properties and edit the values for properties on the **Show All Properties** tab for the object in the NetVoyant Console.

**Note:** Interfaces have properties that you can set on the **Details** tab. For more information, see “Editing the Interface Speeds” on page 170 and “Managing Device Interfaces” on page 170.

### Setting a Property Value

The NetVoyant product enables you to set custom properties for networks, devices, datasets and many of the objects used to monitor and gather data.

For networks, devices, and poll instances, the **Show All Properties** tab provides an easy way to quickly access properties customized for the object.

### To set a property value for an object:

1. Select the object in the tree-tab panel to view the object’s details in the context panel.

For example, to set the properties for an interface on a router, expand the Master server, expand **Devices > Routers**, expand the router, and select the interface.

2. Click the **Show All Properties** tab.

This tab shows existing properties for the object. From here, you can add new properties, change the value for an existing property, or change the system mode for a property.

**Note:** If the Show All Properties tab does not appear in the context panel, click the **Customize** tab to select the Show All Properties tab for display.

Details		Alarms		Reports		Real-time Graphs	
Connections		Thresholds		Show All Properties		Customize	
Properties for 10.0.7.70:FastEthernet0/0							
Property Name		Property Value		Property Mode		System Mode	
Name		10.0.7.70:FastEthernet...		Normal		Normal	
ifSpeed		1.0E8		Normal, Details Tab		Normal	
ifDescr		FastEthernet0/0		Normal		Normal	
ifName		Fa0/0		Normal		Normal	
ifType		6		Read-only, Details Tab		Normal	
ifIndex		1		Normal		Normal	
ifAlias				Normal		Normal	
Description		FastEthernet0/0		Normal		Normal	

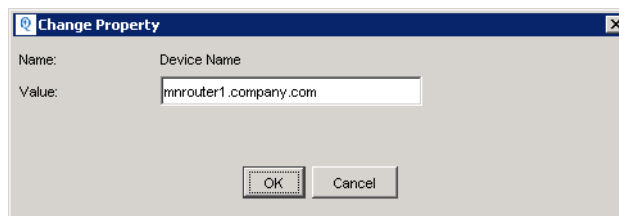
The tab displays the following parameters for each property:

Parameter	Description
<b>Property Name</b>	The name of the property used to identify it. When you include a property in an expression or threshold, you enter a \$ symbol before the property name; for example, \$PropertyName
<b>Property Value</b>	The value of the property for this object; for example, for an interface named interface1, the property ifName property could have a value of Interface1.
<b>Property Mode</b>	The property mode of a property indicates whether you can edit the value for a property and where you can edit it. The property mode can be set to one of the following: <ul style="list-style-type: none"> <li>• <b>Normal</b> - You can edit the value of a property with a normal property mode.</li> <li>• <b>Read-only</b> - You cannot edit the value of a property with a read-only property mode.</li> <li>• <b>Details Tab</b> - The property is on the <b>Details</b> tab for the related object; for example, the Details tab for the device. You can edit the value for this property on the <b>Show All Properties</b> tab or on the Details tab.</li> </ul>
<b>System Mode</b>	The system mode of a property indicates whether the value for a property can be modified. The system mode can be set to one of the following: <ul style="list-style-type: none"> <li>• <b>Normal</b> - All default NetVoyant properties are initially set to Normal, indicating that it can edit the property value during rediscovery.</li> <li>• <b>Read-Only</b> - All properties that you create are initially set to Read-Only, indicating that it cannot edit the property value during rediscovery. If you manually edit the value for a property, the NetVoyant product changes the system mode to read-only so that it does not overwrite your entry.</li> </ul>

3. Perform one of the following tasks:

- To add a new property, click **Add**. This opens the **Add Property** dialog box.
- To edit an existing property's value, select the property and click **Change**. This opens the **Change Property** dialog box.

**Note:** You cannot edit a property that has a property mode of **Read-only**.



4. Enter or edit the following parameters:

Parameter	Description
<b>Name</b>	For a new property, enter the Name of the property used to identify it. When you include a property in an expression or threshold, enter a \$ symbol before the property name; for example: \$PropertyName
<b>Value</b>	Enter the value of the property for this object; for example, for an interface named interface1, the property ifName could have a value of Interface1.

5. Click **OK**.

#### To remove a property:

- ▶ Select the property and click **Remove**.

#### To set a property's system mode to Normal:

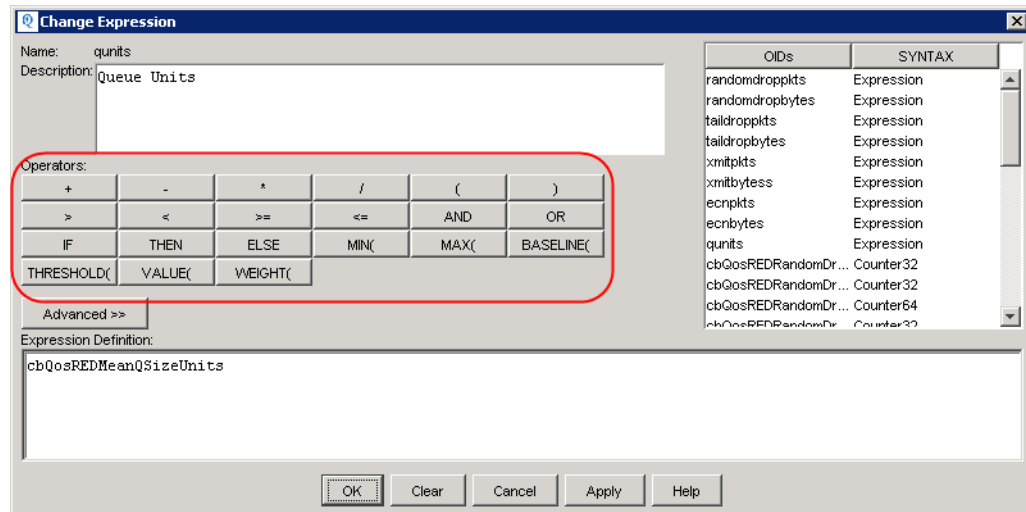
- ▶ Select the property and click **Reset System Mode**.

**Note:** You can also create properties while editing expressions for datasets.

## USING NETVOYANT OPERATORS IN EXPRESSIONS

You can use the NetVoyant operators when creating or editing expressions or thresholds. For your convenience, they are included as buttons in the Expression editors.

### Operators available in the Expression editor



The Expression editor provides the following NetVoyant operators:

### Mathematical Symbols

Symbol	Usage
+	OIDname1 + OIDname2
-	OIDname1 - OIDname2
*	OIDname1 * OIDname2
/	OIDname1 / OIDname2
(	(OIDname1 + OIDname2) / OIDname3
)	(OIDname1 + OIDname2) / OIDname3

### Evaluations

Symbol	Usage
>	<p>ExpressionName &gt; X</p> <p>where ExpressionName is the name of an expression defined for the dataset and X is a number or an expression that evaluates to a number.</p> <ul style="list-style-type: none"> <li>“is greater than”</li> <li>This is useful for setting thresholds that are triggered when an expression goes above a certain value.</li> </ul>

Symbol	Usage
<	<p>ExpressionName &lt; X</p> <p>where ExpressionName is the name of an expression defined for the dataset and X is a number or an expression that evaluates to a number.</p> <ul style="list-style-type: none"> <li>• “is less than”</li> <li>• This is useful for setting thresholds triggered when an expression goes below a certain value.</li> </ul>
>=	<p>ExpressionName &gt;= X</p> <p>where ExpressionName is the name of an expression defined for the dataset and X is a number or an expression that evaluates to a number.</p> <ul style="list-style-type: none"> <li>• “is greater than or equal to”</li> <li>• This is useful for setting thresholds that are triggered when an expression reaches or goes above a certain value.</li> </ul>
<=	<p>ExpressionName &lt;= X</p> <p>where ExpressionName is the name of an expression defined for the dataset and X is a number or an expression that evaluates to a number.</p> <ul style="list-style-type: none"> <li>• “is less than or equal to”</li> <li>• This is useful for setting thresholds that are triggered when an expression reaches or goes below a certain value.</li> </ul>

## Logical Connectors

Connector	Usage
AND	<p>X AND Y</p> <p>where X and Y are expressions that can be evaluated as TRUE or FALSE.</p> <p>For example:</p> <pre>(ifAdminStatus==1) AND (opstatus&lt;100.0)</pre> <ul style="list-style-type: none"> <li>• Boolean “AND”</li> <li>• This is useful for setting thresholds that are triggered when both parts of the boolean expression are met.</li> </ul>
OR	<p>X OR Y</p> <p>where X and Y are expressions that can be evaluated as TRUE or FALSE.</p> <p>For example:</p> <pre>(ifAdminStatus==1) OR (opstatus&lt;100.0)</pre> <ul style="list-style-type: none"> <li>• Boolean “OR”</li> <li>• This is useful for setting thresholds that are triggered when either part of the boolean expression is met.</li> </ul>



Connector	Usage
IF/THEN/ ELSE	<p>IF X THEN Y ELSE Z</p> <p>where X is an expression that can be evaluated as true or false and Y and Z are expressions.</p> <p>For example:</p> <pre>IF \$ifHighSpeed != 0 THEN \$ifHighSpeed * 1000000 ELSE \$ifSpeed</pre> <ul style="list-style-type: none"> <li>• Logical “If, then, else”</li> <li>• This is useful for setting expressions that are calculated differently depending on the values of other expressions or properties.</li> </ul> <p><b>Note:</b> In addition to if/then/else conditional statements, NetVoyant expressions also support the conditional syntax: <code>a &lt; b ? a : b</code></p>

## Functions

Function	Usage
MIN(	<p>MIN(Expression)</p> <p>Returns the minimum value for the expression during the rollup period.</p>
MAX(	<p>MAX(Expression)</p> <p>Returns the maximum value for the expression during the rollup period.</p>
BASELINE(	<p>BASELINE(ExpressionName)</p> <p>where ExpressionName is the name of an expression defined for the dataset.</p> <p>For each poll instance, the NetVoyant product evaluates the function as the current baseline calculation of the expression for a given poll instance. It typically calculates baselines on an hourly basis.</p>
THRESHOLD(	<p>THRESHOLD(ExpressionName)</p> <p>where ExpressionName is the name of an expression defined for the dataset.</p> <p>Returns the threshold of the expression.</p>
WEIGHT(	<p>WEIGHT(min, expression, max, weight)</p> <p>where min and max are numeric values, min is less than max, and weight is a value between 0 and 1.</p> <p>This function evaluates the current value of the expression between the min and max values and creates a weighting based on the value of the weight parameter.</p> <p>A weight parameter that is closer to zero ramps up quickly with any changes from the min value. A weight parameter that is closer to 1 ramps up slowly until the value is close to the max value. A weight parameter that is equal to 0.5 specifies a linear ranking of values.</p> <p>For example, the Interface Statistics dataset includes the following WEIGHT function in an expression for an error rate performance index (errorrate_idx):</p> <pre>WEIGHT(0, in_errorrate, THRESHOLD(in_errorrate), 0)</pre> <p>This function evaluates the in_errorrate expression between zero and the threshold for the expression and ramps up quickly as the value deviates from zero.</p>

<b>Function</b>	<b>Usage</b>
VALUE (	<p>VALUE(expression1, expression2)</p> <p>For each poll instance, the NetVoyant product evaluates the function as <code>expression1</code>, if <code>expression1</code> is not null; otherwise, it evaluates the function to <code>expression2</code>.</p> <p>Often VALUE functions are used to include properties in expressions or thresholds. In this case, the function typically uses the following syntax:</p> <p>VALUE(\$PropertyName, X)</p> <p>where <code>PropertyName</code> is the name of a property that already exists or is one that you want to create and <code>X</code> is a number.</p> <p>The NetVoyant product evaluates the function to the value of the property if it exists for the poll instance or to <code>X</code> if it does not.</p>

# Managing NetVoyant SNMP Traps

---

The SNMP agents on your devices collect and store SNMP data that the NetVoyant product collects during polls; however, the SNMP agents on your devices also can send notifications called SNMP traps. SNMP traps can be triggered by such events as a network link going down, a new device coming online, or a performance threshold being crossed. The types of SNMP traps that a device sends depends on the type of device and the capabilities of its SNMP agent.

**Note:** If the NetQoS Event Manager software is installed on a server where NetQoS NetVoyant is installed and running, it potentially creates a situation where the NetVoyant and Event Manager trap receivers are in contention to receive incoming traps. To avoid this issue, the Event Manager installation program automatically disables the Event Manager trap receiver component whenever it detects the presence of the NetVoyant product on the target computer. The component that is disabled allows the Event Manager to process events sent by NetQoS ReporterAnalyzer.

This appendix covers the following topics:

- [“Working with NetVoyant SNMP Traps” on page 324](#)
- [“Adding or Editing an SNMP Trap Event” on page 325](#)
- [“Using Variable Bindings” on page 330](#)

## WORKING WITH NETVOYANT SNMP TRAPS

The alarm log panel in the NetVoyant Console displays all incoming trap events. These events are also included in the exception reports available in the NetVoyant reporting tool. To view more information about an incoming trap event listed in the alarm log panel, double-click the trap event to open the event details for the trap event. This provides information that the SNMP agent sent in the related trap.

**Note:** Although the NetVoyant product comes with trap events defined for several standard SNMP traps, we recommend you add and define trap events for the SNMP traps that you expect your devices to send. For more information, see [“Adding or Editing an SNMP Trap Event”](#) on page 325.

### Configuring How the NetVoyant Product Receives SNMP Traps

The NetVoyant product can receive any SNMP trap without configuration. However, you might want to configure how it displays unique content supplied by a device (variable bindings) in trap logs.

Using the NetVoyant MIB compiler, compile the MIBs containing the trap definitions for the SNMP agents from which you are receiving traps. For more information on compiling MIBs, see [“Adding MIBs to the NetVoyant Product”](#) on page 185.

Use the variable bindings defined in each MIB to customize the alarm logs generated by the traps. For more information about how to customize trap logs, see [“Adding or Editing an SNMP Trap Event”](#) on page 325 and [“Including Dynamic Content in SNMP Trap Events”](#) on page 328.

### Configuring an External Source to Receive NetVoyant Traps

You can configure the NetVoyant product to deliver notifications as SNMP traps. When an event occurs that matches your filtering criteria, it sends an SNMP trap according to your specifications.

To ensure that the external events manager can understand NetVoyant SNMP traps, you must compile the MIBs that contain the NetVoyant SNMP trap definitions into the events manager.

The NetVoyant MIBs are located in the following directory:

D:\NetVoyant\mibs\

Compile the following MIBs into your event manager:

- redpoint-mib
- netvoyant-mib

See your event manager’s documentation for assistance with compiling this MIB into the event manager.

## Creating a Notification for Incoming SNMP Traps

You can configure NetVoyant to notify you when it receives incoming SNMP traps. You can configure these notifications to notify differently based on different trap types or sources or according to another event property. For more information, see [“Triggering Notifications for Incoming SNMP Traps”](#) on page 246.

## Configuring a Trap Notification

You can configure the NetVoyant product to deliver notifications as SNMP traps. When an event occurs that matches your filtering criteria, it sends an SNMP trap according to your specifications. For more information, see [“Creating a Notification”](#) on page 227.

## ADDING OR EDITING AN SNMP TRAP EVENT

Although the NetVoyant product comes with trap events defined for several standard SNMP traps, it is recommended you add and define trap events for the SNMP traps that you expect your devices to send. This helps generate customized trap event logs for your devices that are more meaningful and helpful to you. It also enables you to configure the NetVoyant product to send notifications when it receives a selected type of SNMP trap.

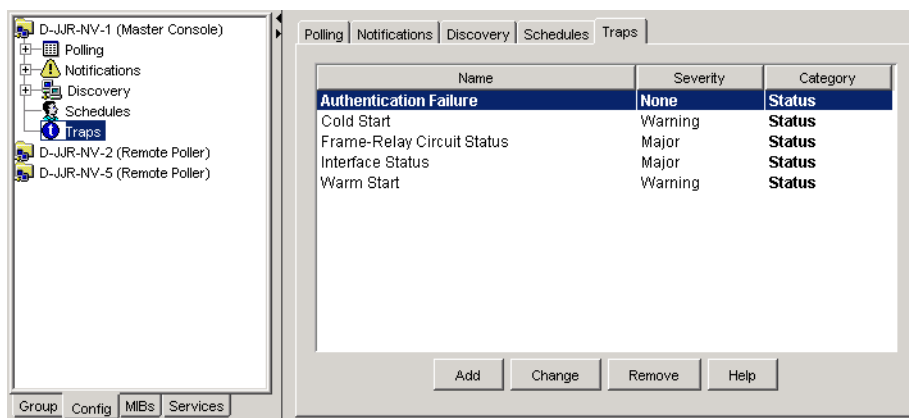
The following are the default trap events:

Trap event	Description
Authentication Failure	Sent when an SNMP agent receives a non-authorized SNMP request. This occurs when the requester used an incorrect SNMP profile to query the agent.
Cold Start	Sent when an SNMP agent starts up. These traps usually occur when a device has restarted.
Frame-Relay Circuit Status	Sent when an SNMP agent detects a change in a frame-relay circuit.
Interface Status	Sent when an SNMP agent detects a change in an interface status. This indicates that one of the following has occurred: <ul style="list-style-type: none"> <li>• An interface that was up (linkUp) has gone down (linkDown).</li> <li>• An interface that was down (linkDown) has gone up (linkUp).</li> </ul>
Warm Start	Sent when an SNMP agent reinitializes itself.

### To add or edit an SNMP trap event:

1. From the **Config** tab in the NetVoyant Console, expand the Master console.
2. Select the **Traps** item in the tree.

The **Traps** tab appears in the context panel and displays the existing trap events.





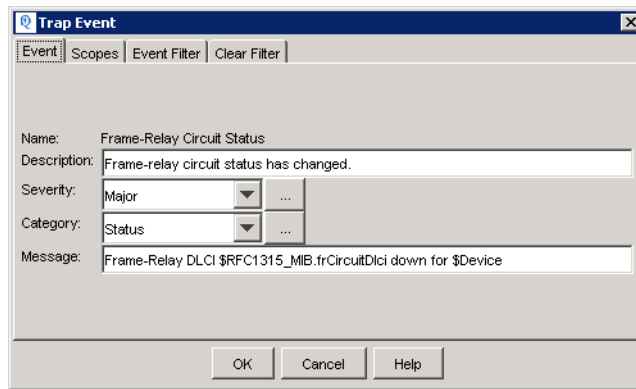
3. Perform one of the following actions:

- To edit an existing trap event, select a trap event and click **Change**.
- To add a new trap event, click **Add**.

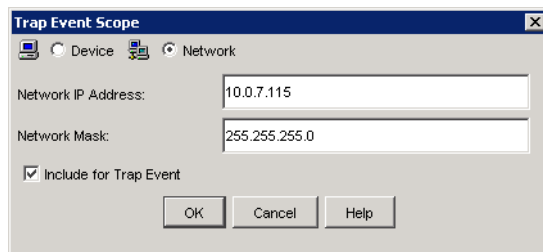
The **Trap Event** dialog box opens.

4. On the **Event** tab, enter or edit the following parameters:

Parameter	Description
<b>Name</b>	For a new trap event, enter a name for the trap event. The trap event's name is used to identify the trap event in alarm logs, notifications, and NetVoyant exception reports.
<b>Description</b>	Enter or edit the description for the trap event. The trap event's description can help you identify the type of trap.
<b>Severity</b>	<p>Select a severity level for the trap event from the list.</p> <p>Events can be one of the following severity levels: Normal, Warning, Minor, Major, or Critical.</p> <p>To view and adjust the event severities by color, click </p>
<b>Category</b>	<p>Select the category for the trap event from the list. It is recommended that you select "Status" for trap events.</p> <p>To view and adjust the event categories, click </p>
<b>Message</b>	<p>Enter the message that you want to display in the alarm log for trap events of this type.</p> <p>You can configure the message for a trap event to include dynamic content based on properties or variable bindings sent in the trap message. For more information, see <a href="#">"Including Dynamic Content in SNMP Trap Events"</a> on page 328.</p>



5. (Optional) On the **Scopes** tab, click **Add** to add a range of devices from which the NetVoyant product can receive the trap event. If you do not enter scopes, it can receive this trap from any device.
  - a. Perform one of the following actions:
    - To add a network to the trap event scope, select **Network** and enter the network IP address and network mask.
    - To add an individual device to the trap event scope, select **Device**, enter the device name or IP address.
  - b. Perform one of the following actions:
    - To include the network or device in the trap event scope, select the **Include for Trap Event** check box.
    - To exclude the network or device from the trap event scope, clear the **Include for Trap Event** check box.
  - c. Click **OK**.

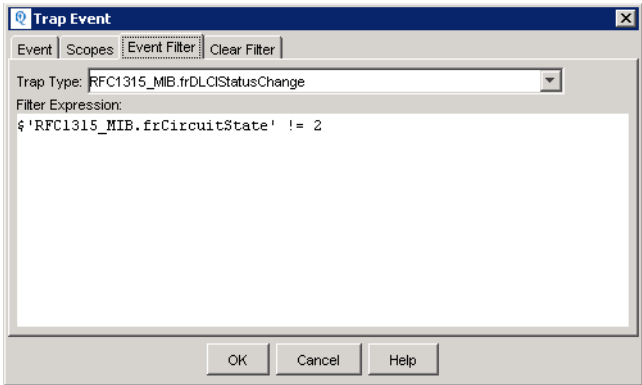


6. On the **Event Filter** tab, select the trap type and specify a filter expression to limit the types of events considered to be a trap event of this type.

If the filter expression for the event filter evaluates as true, the NetVoyant product logs a trap event of this type.

- a. Use the drop-down menu to select a **Trap Type**.  
The available trap types are named using a MIBName . TrapType convention, where:
  - MIBName is the name of the MIB in which the trap type is defined. This MIB must already be compiled into the NetVoyant product. For more information, see [“Configuring How the NetVoyant Product Receives SNMP Traps” on page 324](#).
  - TrapType is the name of the trap type as defined in the MIB.

- b. Enter the **Filter Expression** as an expression that evaluates to true or false. You can include variable bindings defined in the trap definition in your filter expression. For more information, see “Including Dynamic Content in SNMP Trap Events” on page 328.



- 7. On the **Clear Filter** tab, select the trap type and specify a filter expression to define when a trap event of this type is considered to be over.  
  
If the filter expression for the clear filter evaluates as true after a trap event has occurred, the NetVoyant product logs the trap event as over.  
  
The parameters on this tab are identical to those on the **Event Filter** tab.
- 8. Click **OK**.  
  
This adds the new trap event to the list of exiting trap events.

Including Dynamic Content in SNMP Trap Events

You can configure the message that appears for a trap event or the event filters that trigger or end a trap event using content that is specific to the trap event.

For example, you could include the device name in the alarm log message for a trap event. You could also start a trap event using an event filter that filters for traps alerting on inactive frame relay circuits.

Use the following variables in trap event messages and event filters to include dynamic content:

Variable type	Description
Properties	<p>The NetVoyant product stores information about trap events in variables called event properties.</p> <p>To include a property from the trap event details, use the following syntax:</p> <p>\$PropertyName</p> <p>where <i>PropertyName</i> is the name of the property.</p> <p>For more information, see “Using Event Properties” on page 314.</p>
Variable bindings	<p>Each SNMP trap received includes information about why the trap was sent. This information is sent in the form of variables called variable bindings.</p> <p>To include a variable binding, use the following syntax described in “Syntax for Referencing Variable Bindings” on page 331.</p>



For example, you could enter the following message for a trap event:

```
Frame-Relay DLCI $RFC1315_MIB.frCircuitDlci down for $Device
```

If a trap of this type is received, the following content in the message is resolved:

- The `$Device` property to the name or IP address of the device that initiated the trap event.
- The `$RFC1315_MIB.frCircuitDlci` variable binding to the identifier for the failing virtual circuit (`frCircuitDlci`), as defined in the RFC1315 MIB.

## USING VARIABLE BINDINGS

Each SNMP trap that the NetVoyant product receives includes information about why the trap was sent. This information is sent in the form of variables called variable bindings.

You can view the variable bindings for a trap event by viewing the details for the trap event.

### Determining Variable Bindings from a MIB Trap Definition

To include information from variable bindings in a trap event message or filter, you might need to determine the variable bindings in a trap before receiving the trap.

**Note:** To use variable bindings from a trap defined in a MIB not already in the NetVoyant product, you must first compile the MIB. For more information, see [“Adding MIBs to the NetVoyant Product” on page 185](#).

To determine the variable bindings sent in a trap, you can reference the MIB definition for the SNMP agent that sends the trap. You can view MIB definitions in the `D:\NetVoyant\mibs` directory in the NetVoyant Master Console. You can also find MIB definitions online or by contacting a device’s vendor.

In the MIB definition, search for `TRAP-TYPE` to locate the trap definitions. Use variables defined in the trap definition in your trap event message or filter.

For example, the RFC1315 MIB has a “Frame-Relay Circuit Status” trap definition called `frDLCIStatusChange`. In the RFC1315 definition, this trap is defined as the following:

```
frDLCIStatusChange TRAP-TYPE
    ENTERPRISE frame-relay
    VARIABLES { frCircuitIfIndex, frCircuitDLci, frCircuitState }
    DESCRIPTION
        "This trap indicates that the indicated Virtual
        Circuit has changed state. It has either been
        created or invalidated, or has toggled between
        the active and inactive states."
```

This trap definition defines three variables:

- `frCircuitIfIndex`
- `frCircuitDLci`
- `frCircuitState`

You can use these variables in your trap event message or filter.

## Syntax for Referencing Variable Bindings

The syntax for referencing variable bindings is different depending on whether you are referencing the variable binding in one of the following contexts:

Context	Description
Message	<p>To include a variable binding in an SNMP trap event message, use the following syntax:</p> <pre>\$MIBName.VariableBinding</pre> <p>where:</p> <ul style="list-style-type: none"> <li>• <b>MIBName</b> is the name of the MIB in which the variable binding is defined.</li> <li>• <b>VariableBinding</b> is the name of the variable binding as defined in the trap definition.</li> </ul> <p>For example, you could refer to a variable binding in the following message:</p> <pre>\$RFC1315_MIB.frCircuitState</pre> <p>This message references the <code>frCircuitState</code> variable binding defined in the RFC1315 MIB.</p>
Event filter	<p>To include a variable binding in an event filter, use the following syntax:</p> <pre>\$ 'MIBName.VariableBinding'</pre> <p>where:</p> <ul style="list-style-type: none"> <li>• <b>MIBName</b> is the name of the MIB in which the variable binding is defined.</li> <li>• <b>VariableBinding</b> is the name of the variable binding as defined in the trap definition.</li> </ul> <p>For example, you could refer to a variable binding in the following event filter:</p> <pre>\$ 'RFC1315_MIB.frCircuitState' != 2</pre> <p>This event filter references the <code>frCircuitState</code> variable binding defined in the RFC1315 MIB.</p>

**Note:** The only difference in syntax between messages and event filters is that the event filter syntax requires single quotes (') around the reference to the variable binding. A message does not require quotes.

## Determining Appropriate Values for Variable Bindings

When creating event filters or messages based upon variable bindings, it is useful to know what the values for a variable binding represent. For example, you could create an event filter defined as the following:

```
$ 'RFC1315_MIB.frCircuitState' != 2
```

The NetVoyant product starts a trap event based on this event filter if it receives a trap in which the `frCircuitState` variable binding defined in the RFC1315 MIB does not equal 2. If you do not know what the appropriate values for `frCircuitState` are or what they mean, you could not set an appropriate event filter.

To determine the possible values for a variable binding, search the MIB to find the object definition for the variable binding itself.

For example, the RFC1315 MIB contains the following object definition for the frCircuitState variable binding:

```
frCircuitState OBJECT-TYPE
    SYNTAX INTEGER {
        invalid (1),
        active (2),
        inactive (3)
    }
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION
        "Indicates whether the particular virtual circuit is operational. In the
        absence of a Data Link Connection Management Interface, virtual circuit entries
        (rows) may be created by setting virtual circuit state to 'active', or deleted
        by changing Circuit state to 'invalid'. Whether or not the row actually
        disappears is left to the implementation, so this object may actually read as
        'invalid' for some arbitrary length of time. It is also legal to set the state
        of a virtual circuit to 'inactive' to temporarily disable a given circuit."
    DEFVAL { active }
    ::= { frCircuitEntry 3 }
```

From this definition, you can determine that the value “2” equals an “active” state; therefore, the trap event defined earlier starts a trap event if the frCircuitState is not “active.”

---

# Index

---

## Numerics

95th percentile 107

## A

access control list 66

access rights 295, 298

Ack 139

acknowledging alarms 218

    devices 138

    interfaces 167

    poll instances 167

administrating reporting 287–305

advanced calculations 107

alarm profiles 191–208

    alarm rules 199

    assigning to groups 197

    creating 195

    default 192

    duplicating 196

    editing 197

alarm rules 199

    event severity 205

    thresholds 201

alarms

    acknowledging 218

    alarm details 211

    alarm logs 209

    alarm profiles 191–208

    clearing from logs 219

    colors 217

    deleting from the database 220

    devices 138

    interfaces 167

    poll instances 167

    saving logs 216

    source 215

AND 320

ARP cache 44, 117, 137

authentication 37

auto-enable polling 73, 88

auto-include expression 126

automatic grouping 125

availability 280, 310

    devices 141

    notifications 240, 242

Average 107

## B

bandwidth 57

BASELINE 321

baselines 108–111

    adding/removing 108

## C

Cisco IP SLA. See IPSLA

Coefficient of Variation 107

command line notifications 236

community strings 35

configuration 32

    device classes and models 59

    devices 135

    discovery 49

    discovery scopes 40

    discovery seeds 43

    event severities 224

    groups 122

    interface types 57

    poller 22

    polling 85

    profiles 34

    SNMP profiles 34, 35

    troubleshooting 65

Configuration Wizard 33

    device classes 45

    discovery scopes 41

    discovery seeds 44

    initiating discovery 46

    SNMP profiles 34

Console properties 26

CSV files

    saving logs 216

custom datasets 80

    polling groups 84

## D

daily rollups 100

data collection 94

data organization 68

data retention 99

data storage 103

data validation severity 73

database

    backups 30

    deleting events/alarms 220

- notifications 227
- storage 73, 103
- database notifications 236
- dataset storage requirement 73
- Dataset Wizard 80
- datasets 76
  - auto-enable polling 88
  - configuring 67–111
  - custom 80
  - default polling group 96
  - disabling discovery 74
  - disabling polling 86
  - discovery rules 73
  - discovery settings 74
  - editing parameters 71
  - enabling discovery 74
  - enabling polling 86
  - expressions 104
  - model 75
  - periodic discovery 72
  - poll event category 73
  - poll event severity 72
  - poll tables 141
  - Polling Notification Limit 249
  - selective discovery 72
  - viewing data by poll instance 69
- default poll group 124
- delayed notifications 248–253
- device access control list 66
- device alias 148
- device classes 147
  - adding 61
  - changing 61
  - configuring 59
  - configuring polling 45
  - Other 60
  - removing 62
- device models 147
  - adding 63
  - configuring 59
  - disabling polling 64
  - editing 63
  - sysObjectID 62, 64
- Device Wizard 116
- devices
  - acknowledging alarms 138
  - adding to groups 127
  - adding to the discovery scope 116
  - alarms 138
  - availability 141
  - classifying 147
  - configuring 135
  - deleting 153
  - device alias 148
  - discovery 150
  - excluding from discovery 153
  - expiration 55
  - group membership 125
  - interfaces 139, 170
  - locating in the console 154
  - maintenance schedules 132
  - managing 115–175
  - MIBs supported 143
  - off-line 149
  - poll tables 141
  - polling 130
  - polling status 148
  - real-time graph 143
  - removing from groups 128
  - Telnet sessions 155
- DHCP 267
- disabling polling 85
  - datasets 86
  - device models 64
  - devices 148
  - for groups 123
  - for interfaces 166
  - for networks 124
  - for poll instances 166
  - interfaces without traffic 92
  - IP SLA operations 271
  - non-operational interfaces 91
- discovery 50
  - automatic group population 126
  - configuring 49
  - configuring options 52
  - dataset model 75
  - datasets 74
  - device naming parameters 56
  - devices 150
  - disabling a device 151
  - discovery parameters 54
  - discovery seeds 43
  - excluding devices 153
  - expiration 55
  - full 49
  - full discovery interval 53
  - initiating 46
  - interval 53
  - interval offset 53
  - monitoring 47
  - non-SNMP devices 55
  - NPC Sync 54
  - out-of-scope devices 55
  - partial 49
  - periodic discovery 53
  - periodic discovery options 52
  - ping sweep 54
  - rediscovering devices 152
  - rules by poll instance 76
  - selective dataset discovery 72
  - system resource parameters 57
- discovery logs 48
- Discovery Monitor 47
- discovery queue size 47
- discovery rules 73, 76
- discovery scopes 40
  - adding devices 116

- excluding 41
- importing 42
- IP addresses 41
- discovery seeds 43
  - extended discovery 44
- DNS 264
- Does Not Resolve 55, 131, 149

## E

- Edit Shared Views 298
- email notifications 231
- email servers 289
- enabling polling 85
  - datasets 86
- escalated notifications 206, 247
- event duration 252
- event filter expressions 229
- event filters. *See also* notifications, event filters.
- Event Manager 280
  - poll event category 164
- event properties 314
- event severities 224
  - alarm rules 205
  - colors 217
  - interfaces 167
  - notifications 247
  - poll instances 167
- event timestamp 246
- events 189–224
  - clearing from logs 219
  - colors 217
  - deleting from the database 220
  - duration 252
  - event details 211
  - event logs 209
  - event retention 57
  - saving logs 216
  - severity levels 224
  - source 215
  - threshold violations 190
  - thresholds for multiple events 206
- exclusions 132
- expiration 55
- Expression Editor 105
  - operators 319
- expressions 104–108
  - advanced calculations 107
  - auto-include 126
  - baselines 108–111
  - creating for datasets 105
  - custom datasets 82
  - datasets 104
  - event filters 229, 241
  - properties 206, 308
  - thresholds 201

## F

- filter definitions 241
- Find Utility 154

- FTP 268
- full discovery 49

## G

- get profile 150
- global settings 294
- groups 118–130
  - assigning alarm profiles 197
  - automatic grouping 125
  - configuring 122
  - copying/pasting devices 127
  - custom 121
  - default 118
  - disabling polling 123
  - excluding data 129
  - maintenance schedules 132
  - membership 121, 125
  - polling 130
  - rediscover 152
  - removing devices 128
  - reporting interface 120

## H

- HASP 18
- hourly rollups 100
- HTTP echo 263

## I

- ICMP echo 261
- ICMP ping 155
- IF/THEN/ELSE 321
- ifIndex 140
- ifOperStatus 140
- ifSpeed 170
- IFType 173
- image files 62
  - manufacturer's image file 64
- interface speed 170
  - resetting 171
- interface types 57
  - mass operations 173
- interfaces 139, 161–175
  - acknowledging alarms 167
  - deleting data 169
  - details 162
  - event severity 167
  - excluding data in groups 129
  - group membership 125
  - icons 142
  - naming 78
  - real-time graph 172
  - speed 170
- interpolate missed polls 86
- interval offset 53
- intervals
  - polling 97
  - rollups 99
  - sub-minute polling 98
- IP addresses 41

**IP SLA**

- RTT threshold 259
- save to running config 259
- IP SLA Import utility 272
  - XML file format 273
- IP SLA operations
  - configuring 255–278
  - DHCP 267
  - disabling polling 271
  - DNS 264
  - echo 261
  - editing 269
  - FTP 268
  - HTTP echo 263
  - IP SLA Import utility 272
  - path echo 261
  - set profile 150
  - set profiles 138
  - TCP connect 263
  - UDP echo 262
  - UDP jitter 264
  - UDP jitter 269
  - VoIP jitter 265
- IP SLA Wizard 258

**L**

- licensing 18
  - poll instances 19
- locating devices 154
- logging
  - turn off messages for dataset 73
- logging in 24
- logs 209
  - acknowledging alarms 218
  - clearing events/alarms 219
  - colors 217
  - event log retention 284
  - event severity colors 217
  - filtering in the log panel 221
  - log panel display 221
  - saving to CSV files 216
- long term rollups 100
- time filters 101

**M**

- maintenance schedules 132
  - adding 133
  - editing 133
  - manual exclusions 135
- Maintenance-Auto 131
- Maintenance-Manual 131
- Management Information Bases. *See* MIBs.
- manual maintenance exclusions 135
- manufacturer's image file 62
- Map Event List 72
- mass operation tool 173
- MAX 321
- Maximum 107
- membership matching 125

**MIB Browser 182–184**

- viewing device support 143
- MIB Compiler 187
- MIBs 177–188
  - adding to NetVoyant 185
  - compiling 187
  - custom datasets 81
  - data tables 68
  - datasets 104
  - dependencies 185
  - MIBs Tab 179
  - OID details 181
  - OIDs 179
  - real-time graph 184
  - SNMP Query 184
  - SNMP Query for a device 145
  - support by device 143
- MIBs service 280
- MIBs tab 179
- MIN 321
- Minimum 107
- monitoring
  - discovery 47
  - polling 92
- My Pages menu 303
- MySQL 30

**N**

- NetQoS Performance Center 54
  - Map Event List 72
  - SNMP profiles 39
- NetVoyant Console 24
- NetVoyant services 279–285
- network masks 41
- networks
  - adding manually 116
  - disabling polling 124
- non-operational interfaces 140
- non-SNMP devices 55
- notifications 225–253
  - administrative emails 231
  - availability 242
  - by time period 246
  - commands 226, 236
  - creating 227–229
  - database 227, 236
  - disabling 229
  - email 226, 231
  - enabling 229
  - escalated 206, 247
  - event duration 252
  - event filters 229, 240, 241
  - event severity 247
  - examples 237–240
  - formats 226
  - incoming SNMP traps 246
  - numeric pages 226, 232
  - operational status 243
  - polling events 228



- polling failures 228
- SNMP traps 226, 228, 233
- sustained events 248
- thresholds 228, 238, 240, 243
- Notify service 280
- NPC Sync 54
- numeric pager notifications 232

## O

- Object Identifiers. See OIDs.
- Offline 132
- off-line 149
- OIDs 179
  - data tables 68
  - datasets 104
  - details 181
- operational status 140, 240
  - disabling polling 91
  - notifications 240, 243
- operators 319–322
- OR 320
- Other device class 60
- Out-of-Scope 55, 131
- out-of-scope 55

## P

- pager notifications 232
- partial discovery 49
- passwords 288
- path echo 261
- PBX 239
- Percentile 107
- periodic discovery 53, 72
- permission groups 301
- permissions 295
- ping 155
- Ping service 280
- ping sweep 54
- poll concurrency 96
- poll event category
  - datasets 73
- poll event severity
  - datasets 72
  - IP SLA operations 270
- poll instances 161–175
  - acknowledging alarms 167
  - data organization 68
  - deleting data 169
  - details 162
  - device poll tables 141
  - discovery rules 73
  - event severity 167
  - excluding data in groups 129
  - expiration 74
  - group membership 125
  - icons 142
  - licensing 19
  - naming 78

- protocol distributions (RMON2) 157
  - viewing data 69
- polling 135
  - auto-enable polling 88
  - configuring 85
  - database storage 103
  - device classes 45
  - devices 130
  - disabling 85, 148
  - enabling 85
  - frequency 94
  - groups 123, 130
  - maintenance exclusions 132
  - monitoring 92
  - rollups 99
  - time intervals 97
- polling enabled 72
- polling events 228
- polling groups 94
  - auto-enable polling 88
  - datasets 84
  - default 96
  - poll concurrency 96
  - polling frequency 94
  - polling interval 96
  - rollup interval 96
  - rollups 99
  - time filter definitions 101
- polling interval 96
- Polling Monitor 92
- Polling Notification Limit 73, 249
- polling stations 21
- polling status 148
- Polls service 280
- privacy 37
- probes
  - See RMON2
- profiles 34
- properties 307–318
- protocol distributions 157
- protocol groups 159
- proxying
  - roles 304
  - user accounts 302

## R

- real-time graph
  - devices 143
  - interfaces 172
  - MIBs 184
- rediscovery
  - devices 152
  - full 49
  - individual devices 152
  - initiating 46
  - partial 49
- Remote NetVoyant Console 29
- report menus 298
  - editing 292

- ReporterAnalyzer 54
- reporting 27
  - access rights 298
  - email schedules 289
  - email server 289
  - proxying user accounts 302
  - roles 295
  - user accounts 295
- reporting administration 287–305
- reporting groups 118–130
  - report pages 120
- RMON2
  - configuring a probe 157
  - configuring protocols 157–160
  - protocol distributions 157
  - protocol groups 159
- roles 295
  - adding 296
  - editing 296
  - proxying 304
- rollup intervals 96, 99
  - time filters 101
- rollups 99
  - poll rate 100
  - time intervals 97
- routers
  - IP SLA operations 255–278
- RTT threshold 259
- running config 259

## S

- security credentials 37
- selective dataset discovery 72
  - device ID 75
  - discovery rules 76
- services 279–285
- set profile 150
- Show Disabled from Polling 142, 149
- Single Sign-On 287
- SMTP servers 289
- SNMP profiles 34, 35, 147, 151, 183
  - community strings 35
  - get 150
  - NetQoS Performance Center 39
  - set 150
  - setting for devices 149
  - SNMP retries 137
  - SNMP Timeout 137
  - traps 215
- SNMP Query 145, 184
- SNMP retries 151
- SNMP sysName 56
- SNMP timeout 151
- SNMP traps 323–332
  - acknowledging alarms 218
  - Authentication Failure 325
  - clearing alarms 219
  - Cold Start 325
  - configuring events 325–329

- configuring incoming 324, 325
- configuring outgoing 324, 325
- Event Manager 280
- events 190, 223
- Frame-Relay Circuit Status 325
- including device information 234
- Interface Status 325
- logs 209
- notifications 228, 246, 325
- notifying on incoming 239, 240, 313
- sending as notifications 226, 233–234
- variable bindings. *See* variable bindings.
- Warm Start 325
- SNMPv3 36, 37
- spike events 248
- Standard Deviation 107
- storage requirement 73, 103
- sub-minute polling 98
- SuperAgent 54
- sustained events 249
- sysName 56, 148
- sysObjectID 147
- system configuration 17

## T

- TCP connect 263
- Telnet 155
- THRESHOLD 321
- thresholds 201–208
  - alarm rules 201
  - alarm when/clear when 204
  - fixed value 208
  - multiple levels 206
  - notifications 205, 228, 238, 240, 243
  - properties 206, 308
  - trend plots 204
  - utilization 204
  - violations 190
- time filters 101
- time intervals 97
- Time-to-live 55
- timezones 101
- Top-N views
  - global settings 294
- Topology service 280
  - discovery 48
- traceroute 155
- Traps service 280
- traps. *See* SNMP traps.
- troubleshooting
  - configuration 65
  - devices 143
  - interfaces 172

## U

- UDP echo 262
- UDP Jitter 264
- Unresponsive 55, 132
- user accounts

- adding 299
- editing 299
- permission groups 301
- proxying 302
- roles 295
- utilization 140, 172, 239
  - notifications 240, 248
  - thresholds 204

## **V**

- VALUE 322
- variable bindings 215, 234, 313, 330–332
- verbose logging 232
- VoIP Jitter 265

## **W**

- WAN 239
- WEIGHT 321
- work week 101
- workdays 101
- working hours 101





**Corporate Headquarters**

5001 Plaza on the Lake  
Austin, TX 78746

tel: 512.407.9443

877.835.9575

fax: 512.407.8629

[www.netqos.com](http://www.netqos.com)