User Guide

Table of Contents

Table of Contents ii
Welcome to Netmon Professional Edition 2
What does Netmon do? 2
Key Features and Benefits 3
Automatic Discovery Features 3
Network Monitoring Features 3
Device Monitoring Features 4
Email and Pager Alert Features 4
SNMP Device Monitoring Features 4
Security Monitoring Features 4
SYSLOG and Event Log Server Features 5
Environmental Monitoring Features 5
Reporting and Data Analysis 5
Administration and Management 6
What's New in Netmon 4.6? 6
New Report Builders 6
Redesigned Web Traffic Report 6
Improved Charting 6
Scheduled Reports 7
Asynchronous Reporting 7
Graphical Desktop 7
Operating System Upgrade 7
Core Services Freeze/Crash Detection and Correction 8
Performance Improvements 8
New "Guest" Accounts 8
New Corrective Actions Collection 9
What's New in Netmon 4.5? 9
Major New Features 9
Minor Enhancements and Bugfixes 10
Where to Find Help 11
Installation and Deployment Guide 12
Planning Your Deployment 12
Deployment Scenarios 12
Recommended (Typical) Deployment Location 13

Alternate Deployment: Monitoring Multiple Physical Segments 14
Frequently Asked Questions 15
Installing the Netmon Server Appliance 15
Using the Quick Start Guide 15
Starting up the Netmon Server Appliance 15
Logging into the Netmon System Console 15
Accessing the System Console Using VNC 16
Changing the VNC Password 17
Configuring Basic Networking (IP Address Assignment) 17
Final Deployment Tasks 18
Changing the Operating System Password 18
Getting Started 19
Logging Into the Netmon Application 19
Username and Password for Initial Login 19
Performing Basic Setup Tasks 19
Introducing the Netmon Home Dashboard 20
Panel: Recently Discovered Hosts 21
How Network Auto-Discovery Works 21
Clearing Entries 21
Configuring Alerts 21
Panel: Top Activity Snapshot 21
Panel Actions 22
Panel: Top Web Destinations 22
What is a 'Web Destination'? 22
Panel Actions 22
Panel: Top Web Users 22
Panel Actions 22
Panel: Top Ethernet Protocols 23
Panel Actions 23
Using the Help & Resources Panel 23
Other Panel Actions 23
Monitoring Network Activity 25
How Netmon Monitors Network Traffic 25
Method #1 - Packet / Protocol Analyzer 25
Method #2 - NetFlow Protocol 26

Using Netmon's Built-In Protocol Analyzers 26
Collecting NetFlow Data Streams from Remote Devices 26
Activating NetFlow 26
Using the Visual Network Explorer 27
VNE Basics 27
Customizing Your View 27
Host Legend 28
Activity Legend 28
Other Panel Actions 29
Panel: Active Connections 29
Traffic Stream Direction 30
Host 30
Port 30
Speed 30
Other Tips 30
Panel Actions 31
Panel: Port Scan 31
Using Netmon's Port Scanning Tool 31
Port Scanner Legend 32
Panel Actions 32
Panel: Host Name(s) 33
Searching for Hostnames 33
Removing A Host Name 33
Adding a User Defined Host Name 33
Network Tools 33
Capturing Raw Network Traffic with the Packet Capture Tool 34
DNS Lookup Tool 34
Traceroute Tool 34
Monitoring Network Devices & Services 35
How Netmon Monitors Devices and Services 35
Introducing the Trackers Console 35
Creating a New PING or TCP Service Tracker 35
Attaching Alerts to a PING or TCP Service Tracker 36
Removing an Existing Alert 37
Modifying a PING or TCP Service Tracker 37
Removing a PING or TCP Service Tracker 37

Monitoring Devices (SNMP) 38

Introduction to Simple Network Management Protocol (SNMP) 38

The Good, the Bad and the Ugly 39

SNMP and Security 39

SNMP's Role in Network Monitoring 40

Using the SNMP Automatic Discovery Service 41

Using a Different Community String? 41

Using the Devices Explorer 42

Adding a New SNMP Device 43

Updating an Existing SNMP Device 43

Removing an SNMP Device 44

Using the Device Toolbar 44

Using the Interface Explorer 45

Basic Interface Information 46

Interface Monitoring Options 47

SNMP Interface Graph 47

Configuring Alerts for an Interface 48

Device Dashboards 48

Assigning a Dashboard to a Device 49

Troubleshooting Dashboards 49

Browsing SNMP MIBs 49

How Netmon Retrieves Management Information 49

What is a MIB? 50

Supported MIB Data Types 50

Managing Custom SNMP MIBs 50

Uploading a Custom MIB 50

Viewing a MIB Definition 51

Using the OID Tracker Service 51

What is an OID? 51

Browsing OIDs with the MIB Browser 52

Creating an OID Tracker 52

Attaching Alerts to OID Trackers 53

Modifying an Existing OID Tracker 53

Removing an OID Tracker 53

OID Tracking Tips 53

Processing SNMP Trap Messages 54

Sending SNMP Traps to Netmon 54

Logging SNMP Traps....54
Trap Alert Services....54
Using the Notes Manager....55
Adding a New Note....55
Modifying an Existing Note....55
Removing a Note....55
Monitoring Windows Services....56
Part I - Enabling SNMP support on Windows 2000/XP/2003 Hosts....56
Part II - Monitoring a Windows Service in Netmon....56
Modifying an Existing Windows Service Tracker....58
Monitoring SYSLOG and Event Logs....59
Using the Event Log Explorer....59
Setting Up SYSLOG Clients....59
Browsing SYSLOG Data in Netmon....60
Monitoring Windows Event Logs....60
Considerations for Event Log Monitoring....61
Using the SNARE Windows Agent....61
Searching the Log Repository....61
Configuring Log Alerts....61
Monitoring Disks and Partitions....63
How does Netmon monitor disks and partitions?....63
Monitoring Windows Volumes....63
Adding a New Windows Share....63
Modifying Disk Parameters....64
Removing a Monitored Disk....64
Configuring Alerts for a Monitored Disk....64
Security Considerations for Monitoring Windows Shares....65
Monitoring Linux and Unix Partitions....65
Adding a New Unix Partition (inetd Method)....65
Adding a New UNIX Partition (xinetd Method)....66
Modifying Disk Parameters....68
Removing a Monitored Disk....68
Configuring Email or Pager Alerts for a Monitored Disk....68
Monitoring Websites and Web Applications....69
Introducing the URL Tracking Service....69
Creating a New URL Tracker....69

Attaching Alerts to a URL Tracker 69
Modifying a URL Tracker 70
Removing a URL Tracker....70
Netmon Reports....71
Creating and Saving Custom Reports....71
Report Scheduling & Background Reports....72
What are Background / Asynchronous Reports?....73
Network Activity Report....73
Panel Actions 74
Conversation Report....74
Panel Actions 75
Web Traffic Report 75
Panel Actions 75
UP / DOWN Time Report....75
Panel Actions 76
Bandwidth Activity Report 76
Panel Actions 76
Bandwidth Consumption Report....76
Running a Bandwidth Consumption Report....77
Panel Actions 77
Disk Activity Report 77
Panel Actions 78
Latency Report....78
Panel Actions 78
OID Tracker Report 78
Panel Actions 79
URL Tracker Report....79
Panel Actions 80
Port Scan Report....80
Configuring Network Service Alerts 80
Panel Actions 80
Alert History Report 80
Panel Actions 81
Netmon Login Report....81

Panel Actions 81
File Management 82
Managing the Backups Folder 82
Managing the Enterprise MIBs Folder 82
Managing Netmon Log Files 82
Managing Traffic Capture Files 83
Administration and Management 84
Using the Settings Console 84
Managing Alert Conditionals 85
What is an Alert Conditional? 85
Are Conditionals Mandatory? 85
Using Conditionals Effectively 85
Adding an Alert Conditional 85
Removing an Alert Conditional 86
Managing User Accounts 86
Viewing Account Details 86
Adding a New User Account 86
Modifying a User Account 86
Deleting a User Account 86
Suspending a User Account 86
Managing Account Groups 87
Understanding Permission Inheritance 87
Viewing Group Details 88
Adding a New Group 88
Modifying a Group 88
Deleting a Group 88
Managing Alert Message Templates 88
Customizing an Alert Message Template 88
Restoring Default Templates 89
Managing Alert Response Commands 89
Creating a New Alert Command 89
Modifying an Existing Alert Command 90
Removing an Alert Command 90
Managing Host Names 90
Searching for Hostnames 90
Removing a Host Name 91
Adding a User Defined Host Name 91

Managing Filter Collections 91
Traffic Filters 91
Host Filters 91
Managing Network Ranges 92
Adding a New Network Range 92
Modifying an IP Range 92
Removing an IP Range from the Database 93
Using the Netmon Update Service 93
Checking for Updates Manually 93
Installing Updates from CD-ROM 93
Managing the Port Label Database 94
Adding a New Port Label 94
Modifying a Port Label 94
Removing a Port Label from the Database 94
Built-In Protocol Dictionary 94
Managing Netmon System Services 94
Starting and Stopping Services 95
Overview of Individual Services 95
Configuring Individual Services 96
Changing Service Startup Behavior 97
Shutting Down and Restarting the Netmon Server Appliance 97
Restarting the Server 97
Shutting Down the Server 97
Troubleshooting Guide 98
Finding Help 98
Troubleshooting the Packet Analyzer 98
Troubleshooting Email Alerts 98
Troubleshooting Pager Alerts 99

Welcome to Netmon Professional Edition

Netmon is a full featured network monitoring solution for small to midsize networks. It provides administrators with a complete perspective of their networks, services and devices from a variety of vantage points:

- Network traffic and activity monitoring
- Bandwidth monitoring
- Service monitoring
- Protocol activity monitoring
- Device monitoring and device management
- Web activity monitoring
- SYSLOG monitoring and event log monitoring
- Website and web application monitoring
- Performance monitoring and reporting
- Cisco NetFlow collection, analysis and reporting
- Email and pager notification / alerts
- Environmental monitoring (optional)

With Netmon's integrated email and pager notification system, you and your network management team will be the first to know when urgent situations arise.

What does Netmon do?

Netmon provides a wealth of information on network activity and network-connected devices. This information can be used to identify immediate issues on the network, and it can also be used as a proactive management tool, giving you a clear perspective into your network's health, usage patterns and growth.

Netmon exposes an enormous amount of useful information for your SNMP-capable network devices, with a fully integrated Management Information Base (MIB) browser. Tens of thousands of devices support the SNMP protocol, and Netmon even allows you to upload your own custom MIBs to work with proprietary devices.

Netmon can monitor the up/down status of any device or network service (such as an SMTP server or POP3 server) at an interval which you choose. When a service stops responding for your specified period of time, visual, email and pager alerts can be activated. Netmon can even show you latency trends and uptime statistics for each of your business critical services.

Monitor usage of your Internet bandwidth with Netmon's built in bandwidth monitoring tools. Easily spot bandwidth trends, such as the busiest times of the day, and receive an alert if bandwidth usage exceeds your defined thresholds.

Netmon can also help you to locate spyware, adware and other types of malicious software on your network. Using Netmon, you can also identify many other kinds of malware, including worms and viruses.

Perform sophisticated data mining with powerful reporting tools. Analyze your network activity to virtually any level of detail, across any time frame, and focus on specific activities using Netmon's powerful reporting toolset.

Key Features and Benefits

Automatic Discovery Features

- Automatic discovery of SNMP capable devices
- Automatic NetBIOS and reverse-DNS name resolution
- MAC address detection with ARP Probe Service
- Background Port Scanning Service automatically identifies new services which appear on your network
- Automatic discovery of devices which send NetFlow data to Netmon
- Automatic interface rediscovery on routers, switches and other managed networking devices

Network Monitoring Features

- Integrated Layer 2 (Ethernet) Frame Analyzer
- Integrated Layer 3 and 4 (IP Services) Protocol Analyzer
- Integrated NetFlow Collector (v1, v5 and v7)
- Raw packet capture utility for low-level packet analysis in compatible client software (i.e. Ethereal / Wireshark)
- Automatic NetBIOS and DNS name resolution
- Real-time network activity monitoring with the Visual Network Explorer (VNE)
- Capture and monitor live network activity on remote networks with NetFlow protocol support
- Instantly narrow live activity views to specific hosts and/or protocols with easy to use filters
- Identify the type and nature of all connections to a particular host with a simple double-click
- Monitor internal and external bandwidth utilization
- Built-in port label database identifies thousands of commonly used protocols
- Create and label your own custom protocols
- Protocol Dictionary features detailed information on over 125 IP-layer protocols
- Capture local network activity on up to two (2) separate physical networks with dual onboard Gigabit network cards

Device Monitoring Features

- Assign friendly names and icons to individual hosts for simplified reporting and visibility
- Monitor Windows Services
- Monitor Windows NT/2000/XP/2003 shared folders and volumes
- Monitor Linux/UNIX and Solaris disks and partitions
- Monitor SYSLOG data from routers, firewalls, switches and other SYSLOG-capable systems
- Monitor Windows Event Logs with supplied SNARE Agent software

Email and Pager Alert Features

- Fully integrated email and pager alert system
- Customizable alert message templates
- Support for alert escalation
- Prevent false alerts with Alert Conditionals
- Service or device UP / DOWN notifications
- Bandwidth utilization alerts (in, out or sum of both)
- SNMP Trap Handling / Relaying Service
- ICMP “ping” availability alerts
- Full TCP handshake monitoring (for specific IP network services such as FTP, Telnet, HTTP, SSH and others)
- Service/connection latency alerts (100ms to 1500ms)
- Protocol activity notifications (i.e. P2P traffic)
- Disk capacity & availability alerts (Windows/Linux/UNIX)
- New network service alerts (i.e. opened TCP/UDP port)
- New host detection alerts (based on MAC identification)
- Event log message alerts based on a specific text or regular expression pattern match

SNMP Device Monitoring Features

- Automatic SNMP device discovery service with customizable Community string
- SNMP MIB Browser - Monitor hundreds or thousands of management information points exposed by SNMPv2 capable devices.
- SNMP Trap Alert Service. Relay SNMP trap messages sent from your managed devices through your Netmon server appliance.
- Upload custom SNMP MIBs for proprietary devices

Security Monitoring Features

- On-demand port scanner identifies open ports / services

- Background port scanning service identifies new network services as they appear
- ARP Probe Service identifies new MAC addresses which have appeared on your network

SYSLOG and Event Log Server Features

- Fully integrated SYSLOG server - collect and store logs from all SYSLOG-capable devices in a single location
- Organize syslog/event log data by host, facility and severity level
- Powerful built-in reporting and search capabilities, including support for regular expression pattern matches as well as standard text search
- Integrated email and pager alert facilities, including support for text and regex matching for alerts
- Monitor Windows event logs with supplied agent software.

Environmental Monitoring Features[1]

- Monitor datacenters, server rooms, wiring closets and other locations for temperature or humidity changes
- Detect the presence of water with the included water sensor
- Monitor door contacts and motion sensors
- Detect vibrations and movement with specialized sensors
- Monitor environmental conditions at multiple remote locations, including datacenters, branches and field offices, and process alert messages from a centralized console in your Netmon system.

Reporting and Data Analysis

- Historical database of virtually all monitored activities
- Network, protocol and host activity reports
- Uptime/downtime and service latency reports
- Bandwidth utilization reports
- Sophisticated traffic and protocol analysis toolset
- Build and save custom reports for later one-click delivery
- Printer-friendly report designs
- Snapshot Reports - almost any application panel can be printed directly in a printer-friendly format
- Customizable protocol and host filtering lets you narrow reports to specific hosts and/or network activities
- Customizable logging verbosity settings for each monitored device and service
- Analyze Netmon data in third-party reporting packages such as Crystal Reports.

[1] * Requires optional Enviro-MINI add-on unit(s) (See www.netmon.ca/enviro/ for more information).

Administration and Management

- Netmon security groups allow you to assign distinct capabilities and permissions to Netmon user accounts
- Full control over each distinct monitoring service. Turn off services which aren't needed or required.
- Specify historical data retention policies for each monitoring service. For example, you can tell Netmon to keep 8 weeks of network traffic data, and unlimited SYSLOG data.
- Data backup facilities, from quick configuration-only backups to complete database archiving
- Label your own protocols by adding, editing or removing entries in Netmon's protocol index
- Customize email and pager message templates

What's New in Netmon 4.6?

New Reporting System:

New Report Builders

- The report builder components have been re-designed to improve usability. For example, data-selections are now based on pop-up calendars, and users can also pick from more pre-defined time periods such as "last hour", "this week", "this month", "last month", etc.
- Additionally, the user can drill-down on reporting time-period on individual minutes, providing greater reporting flexibility.
- You may now also specify the number of results to return.

Redesigned Web Traffic Report

- Until Netmon 4.6, the Web Traffic report was simply a list of all the URLs visited by IP addresses on your local network. As of Netmon 4.6, the report output has been re-designed so that the report provides a high-level list of websites visited by IPs, and the user can drill-down in each website to see a list of individual pages visited on that site.
- Netmon also attempts to identify RSS traffic and marks those websites with an RSS icon so as to ensure it is not mistaken for surfing activity.
- You can now instruct Netmon to look for web connections following a specific direction (e.g. local to external, external to local, or both)

Improved Charting

- Most of the report output charts have been revisited to provide a higher degree of accuracy. Netmon chart-based reports now generates more data-points and scales them in an intelligent statistic approach to make it easier to identify issues.

Scheduled Reports

- All Netmon reports now support recurrent scheduling.
- Report output will be saved in the “Completed Reports” folder, in the “Reports” section.
- Ability to schedule reports daily, weekly (on a specific weekday), monthly or yearly.
- Ability to edit scheduled report specifications to change parameters or adjust schedule.
- Ability to apply custom labels to reports that will be used while saving the output.
- Report output archival will ensure your completed reports will not be overwritten once they are re-scheduled.
- Reports can be scheduled to run at any time of the day
- Once a report has been generated, Netmon will send a notification email to the user of your choice.

Asynchronous Reporting

- All Netmon reports now sport a “Run Asynchronously” checkbox. When checked, instead of generating the report on-demand and displaying its output right in your browser (which could take several minutes depending on the report parameters), Netmon will process the report in the background and save the report output in the “Completed Reports” area.

Graphical Desktop

Long gone are the days of having to edit configuration files to configure networking parameters or operating-system parameters. Netmon 4.6 now features a Gnome graphical desktop that allows you to run a local web-browser right from your Netmon appliance, configure network settings for each network interface available, edit any file on the system, manage all aspects of the operating system, etc…

Netmon 4.6 also ships with a VNC server, so you can download a free VNC client and remotely access your graphical desktop to perform any configuration changes, or even open up the web-browser on your Netmon appliance to see sites and web-applications from the perspective of your Netmon system.

Operating System Upgrade

Another big item that we’ve put a lot of work into was the migration to the latest release of our host Operating System, namely, Debian GNU/Linux’s “Etch” release. After 3 years of development, the new release brings massive improvements that will greatly benefit Netmon users. Some of the core changes that will affect Netmon users include:

- PostgreSQL (v7.4 to v8.1) - This upgrade of Netmon’s Database System results in massive performance and reliability enhancements.

- Apache (v1.4 to 2.0) - The web-server component that Netmon relies on has been upgraded to the next major release, which results in slight performance improvements and corrects some issues with long-running reports and SNMP-walks.
- PHP (v4.3 to 5.1) - Netmon's PHP layer will benefit from this upgrade through performance improvements and improved security. This upgrade also corrects some session issues after system reboots.
- GCC Compiler Collection (v3.3 to 4.1) - This compiler upgrade provides performance and stability improvements to the core Netmon background services.
- DBUS (new dependency) - Netmon now uses the DBUS IPC system to allow communication between the different daemons and plugins, which allows Netmon to automatically detect issues and take corrective action if any of the core services stops functionning correctly.
- Linux Kernel (2.4 to 2.6.18) - The new version of the Linux kernel included in this release provides massively increased responsiveness of the application under heavy load, as well as much improved resource management, which translates into much improved performance for the end-user. It also provides much better hardware support for several components used in our Netmon appliances.

Core Services Freeze/Crash Detection and Correction

Starting with Netmon 4.6, the core process manager constantly monitors the status of all Netmon background services to ensure they are always running.

In the event that an error condition could cause a particular service to crash or freeze, this mechanism will attempt to revive the service, and will then send our technical support team a complete snapshot of your Netmon System so we can analyze the issue and deploy a patch to correct it.

Performance Improvements

As outlined in the "Operating System Upgrade" section, several key components of your Netmon system have been upgraded to major new releases, which provide massive performance improvements. This translates into a much more responsive User Interface, faster reports, and a lower packer-drop rate, which results in greater accuracy.

In addition to the Operating-System package upgrades, we've also improved the performance of several key areas in the Netmon application itself, such as the traffic sniffer and its associated plugins, and the User Interface.

New "Guest" Accounts

Netmon 4.6 introduces a new "Demo" or "Guest" type of user-accounts that are allowed to log into the system and access any area that you grant them access to, but will not be able to modify any settings,

create any tracker, or run any sensitive reports that could been seen as a potential security breach. This is the same system we use to grant people access to our main demonstration server.

It is also worth noting that, unlike several applications available today, the “Guest” account restrictions are implemented right at the database-access-layer instead of through front-end restrictions, which means that it cannot be circumvented through XSS (Cross-Site-Scripting) or Javascript hackery, or by forging web-requests.

New Corrective Actions Collection

In Netmon 4.5-r2, we’ve introduced a new feature called “Sophisticated Alert Response Mechanism (SARM)”. This system allows you to bind any command that can be executed on the host operating system to any alert that you create in Netmon. Using SARM, you may either use any of the tools provided as part of the Debian GNU/Linux operating system as a corrective action, and you could also either write your own corrective action script/program in any programming language supported by the OS (Java, C, C++, Python, Ruby, PHP, Perl, Bash, etc…), or use one of the corrective action scripts we have built specifically for Netmon.

With Netmon 4.6, we’ve pre-filled the list of alert commands for many of the alerts available with a collection of interesting alert remediation scripts that you can bind to any new alert. Some of the commands can be used as example while building your own.

For example, one of the commands we’ve provided the “Stop IIS” and “Start IIS” commands, which you can modify to start/stop any other service on your Windows server from your Netmon appliance.

It’s also worth noting that all the Netmon reports can now be executed as command-line programs, which means that they can also be used as alert response scripts. You could, for example, ask Netmon to run a Network Activity report for the last hour if you detect the bandwidth utilization on your router’s “Outside” interface exceeds 70%, or you could ask Netmon to run a complete UP/DOWN time report for all your services at once if you detect that your DMZ is no longer available.

What’s New in Netmon 4.5?

Major New Features

Improved Windows Service Monitoring Monitoring NT services is now even easier. You can browse a list of services and create an OID Tracker with one click from the latest Windows device dashboards.

New and Improved Device Dashboards Existing dashboards have been improved with new graphical instruments and layout, and several new platforms have also been added.

Monitor Microsoft SQL and Exchange Servers Using optional agents from our new technology partner, Informant Systems, you can monitor myriad operational details of your SQL database servers, IIS web servers and Exchange mail servers.

New Backup System You can now back up your Netmon data to a remote file share, as well as choose which types of data you wish to back up. Netmon automatically calculates the size of each database table, so you can determine which monitoring facilities consume most of your disk space.

SNMP Object (OID) Tracker Report You can now generate reports on the managed objects you are monitoring with your Netmon system.

URL Tracker Report You can now generate reports on the performance of your URL Trackers.

Minor Enhancements and Bugfixes

- Syslog / event log searches can now be performed to a granularity of 1 minute
- Added color coding indicators for Syslog / event log facilities and severities
- Added standard Device toolbar for all device dashboards
- Renamed OID Trackers to SNMP Object (OID) Trackers
- Renamed TCP Service Monitors to TCP Service Trackers
- Renamed ICMP Monitors to PING Trackers
- Renamed Disk Monitors to Disk Trackers
- Renamed URL Monitors to URL Trackers
- Faster SNMP walks and OID queries through a new SNMP proxy service.
- Many thanks to Mark James, who provided many of the icons used in the updated user interface.
- Added file size column in the FILES directory viewer
- Users now have the option to enable/disable SNMP Autodiscovery and/or Background Port Scanner on each individual user-defined Network Range.
- Improved interface state monitoring. Netmon now shows the UP/DOWN state of each network interface on device dashboards.
- Added support for the Opera and Safari / Konqueror web browsers
- Port Scan Report now allows users to create TCP service trackers directly from report results
- Added traceroute utility to NETWORKS > TOOLS with new progress indicator component
- Fixed a bug in OID Tracker graphs that would break the graphs if all values were equal to 0*[*]
- Items on the Home Dashboard now refresh individually, instead of causing a full-page refresh
- Fixed a bug that caused certain OIDs to be detected as strings instead of numeric*
- Fixed a bug causing custom OIDs for devices whose ID was <= 10 to never show up in the dashboards*
- Added support for string type OIDs in dashboards*

[*] Customers running Netmon 4.1 received this update as a patch.

- Fixed a bug that caused the system to refuse creating alerts against string OIDs*
- Fixed a bug in the Visual Network Explorer which caused a drop-down box to scroll upward when there were more than 44 Host Filters in the system.

Where to Find Help

Need help with your deployment? Assistance is just a call or click away.

- Visit the online User Guide at www.netmon.ca/support/manuals/
- Use the Live Chat feature on the Netmon website: www.netmon.ca/support/
- Use the Live Chat feature in your Netmon Help & Resources panel[2].
- Email us at support@netmon.ca
- Call us toll-free at **1-800-944-4511**

[2] See *Using the Help & Resources Panel* on page 23 for more information.

Installation and Deployment Guide

Netmon is an extremely flexible product which has been designed to integrate quickly and easily with virtually any IP-based network. It can be deployed in several different ways to facilitate specific monitoring objectives.

Planning Your Deployment

Planning the installation of your Netmon server appliance consists of three main steps:

1. Determine the network(s) that you want to monitor, and choose an appropriate deployment scenario.
2. Determine where to physically place the Netmon server appliance on your selected network segment.
3. Determine whether the Netmon server should obtain an IP address automatically through a DHCP server, or whether it will be necessary to assign one manually.

Deployment Scenarios

Choosing an appropriate physical deployment location is the most important step to achieving your monitoring goals. Ask yourself the following questions:

- **What is the most important network traffic to monitor?** Some organizations are only interested in Internet-bound traffic, while others are primarily concerned about traffic hitting their key servers. On larger networks, these activities could be taking place on completely different physical segments. In this case, you'll want to physically locate your Netmon system on the most important network segment[3].

- **Which network devices do I want to monitor?** (i.e. servers, workstations, switching or routing equipment, etc.) Netmon requires a valid IP route to the devices you wish to monitor. As a general rule of thumb: if you can PING a device, Netmon can monitor it.

- **Do I want an internal or external perspective of my services?** Sometimes the main goal is to monitor your services or devices from the perspective of an external user. In this case, you would need to locate the Netmon server appliance outside the datacenter, on an external network (such as a backup or failover site).

[3] Netmon server appliances have a minimum of two (2) network interface cards (NICs) and can be configured to monitor more than one physical segment (such as a LAN and a DMZ) but those segments must be physically close enough to connect a network cable.

Recommended (Typical) Deployment Location

In most environments, the Netmon server is connected to the core switch on your primary Local Area Network (LAN). From this perspective, it can typically have visibility into all of the following:

- local and Internet-bound network traffic;
- key servers and network equipment;
- workstations and other department-level devices (i.e. printers);
- remote networks and devices[4];

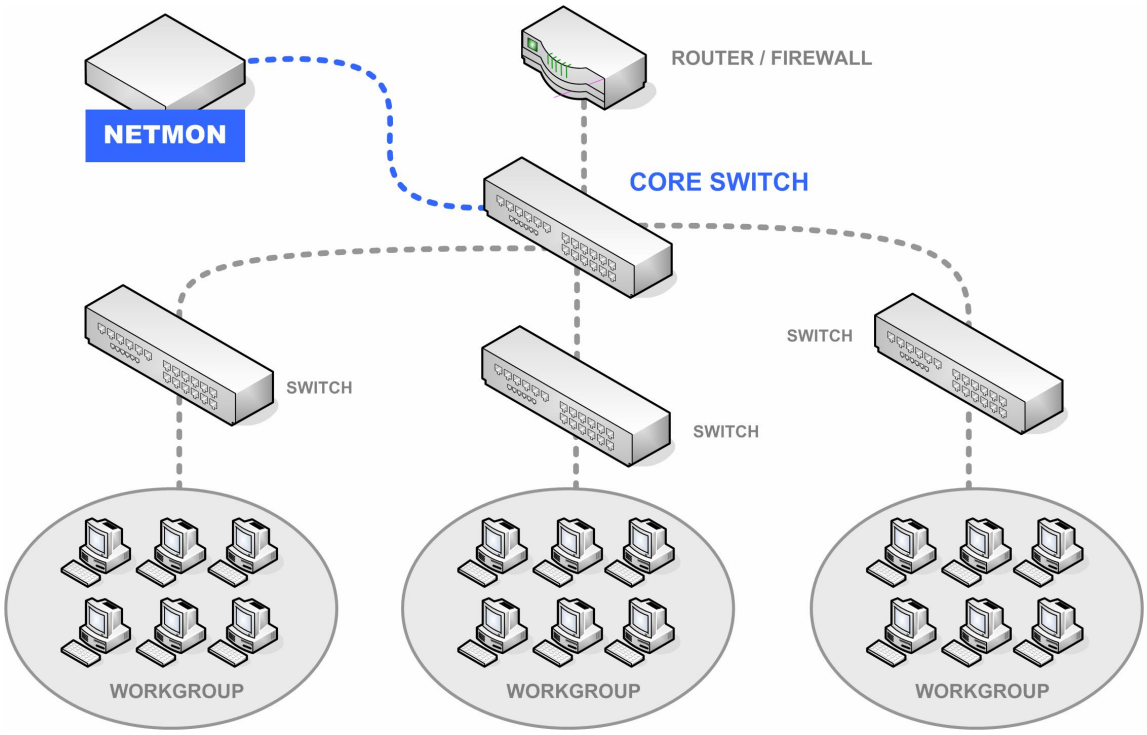


Figure 1 – Typical Netmon deployment scenario

In this diagram, the Netmon server appliance is placed such that it can gather performance data from virtually any device on the network, as well as monitor any network traffic that is hitting the core switch.

[4] Depending on your existing firewall policies, access to remote networks and devices may require configuration changes to your firewall. Monitoring remote network traffic requires NetFlow protocol support on the remote network.

Alternate Deployment: Monitoring Multiple Physical Segments

Netmon server appliances have between 2 and 4 network interfaces, which means that you can monitor more than one physically separate network (such as a LAN and a DMZ). The following illustration depicts this scenario:

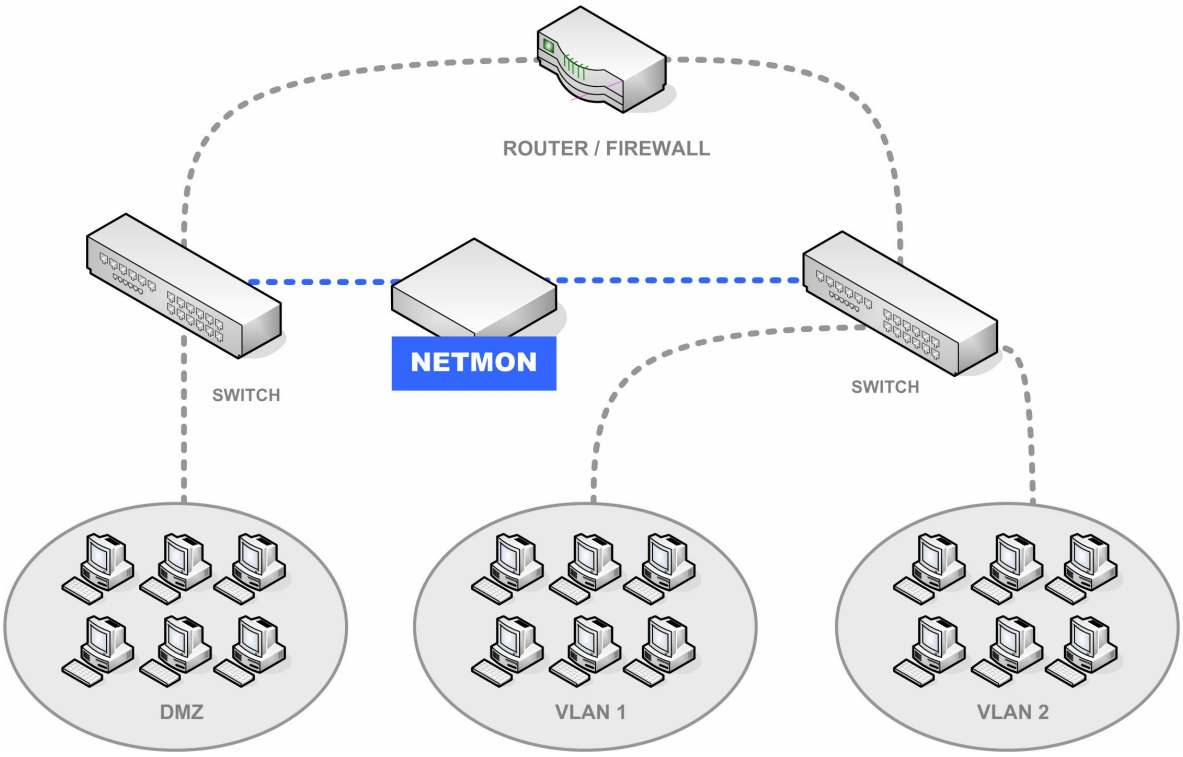


Figure 2 –Monitoring multiple physical segments

In this diagram, the Netmon server appliance has a physical connection to both networks, and can access devices on both networks. Each network interface on the server appliance is given a valid IP address on each network[5].

[5] This arrangement has some security implications. Since the Netmon server appliance lives on both networks, it could potentially be used as a staging point to attack the LAN from the less protected DMZ segment. Fortunately, properly configured, the Netmon server appliance has a fairly small attack surface area compared to other systems that are likely to be present on a DMZ. For enhanced security (and only if you intend to monitor traffic, and not devices) you can assign an invalid 'dummy' IP address to the DMZ interface on your Netmon server appliance.

Frequently Asked Questions

Can I monitor multiple VLANs?

Yes, Netmon can monitor traffic from multiple VLANs, provided your core switch supports frame mirroring across VLANs[6].

I want to monitor activity on a remote branch network. How is this done?

Monitoring network activity at remote sites requires NetFlow protocol support.

Installing the Netmon Server Appliance

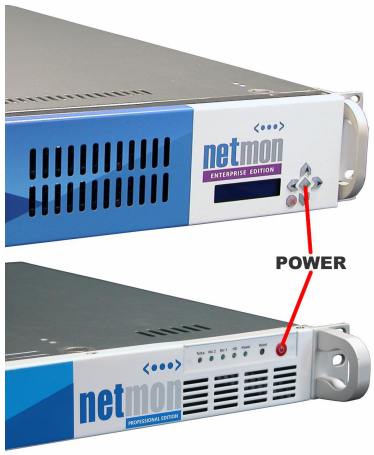
A rack mounting kit, along with installation instructions, is included in your Netmon server appliance package. See the enclosed instructions and materials for specific details on installing your system into a server rack.

Using the Quick Start Guide

This 2-page guide is included in your Welcome Package, and provides instructions for connecting the power cables, keyboard, video, mouse and network connections. Refer to this guide for hardware setup.

Starting up the Netmon Server Appliance

Once power has been connected to the Netmon server appliance, it should start automatically. If it does not, press the red (Netmon Professional) or green (Netmon Enterprise) power button on the front of the appliance, as illustrated here:



Logging into the Netmon System Console

You can log into the operating system console directly on the Netmon server itself, using an attached keyboard, monitor and mouse. Alternatively, you can also access this console remotely using the popular VNC remote desktop tool.

The operating system account you'll use is named **netmon**. The password, by default, is **netmon**, although this may have (and should have[7]) been changed after Netmon was initially deployed. Successfully logging in will give you a screen similar to the following:

[6] See *How Netmon Monitors Network Traffic* on page 25.

[7] See Changing the Operating System Password on page 18.

Figure 3 – Netmon System Console

Accessing the System Console Using VNC

In addition to a direct keyboard, video and mouse connection, the Netmon System Console can also be accessed using the popular VNC remote desktop software.

Download a VNC client onto your Windows workstation from http://www.realvnc.com/

1. Open the VNC client program and connect to XXX.XXX.XXX.XXX:1, where XXX.XXX.XXX.XXX is the IP address of your Netmon server appliance. Don't forget to include ':1' at the end of the IP address.

2. Once connected, it will prompt you for the VNC password. The default password is *netmon*.

VNC uses its own authentication method, separate from the linux system usernames. When connecting to the VNC desktop, it will ask you for a password. This password is the VNC password, NOT the user account password. Once logged in, the user will have limited privilages. When running the network configuration tool, it will prompt you for the system administrator password. Both the root and VNC passwords should be changed immediately after initial setup, and kept in a secure place.

Changing the VNC Password

The password used to access your Netmon System Console via VNC is separate from the normal operating system password. For security reasons, it is a good idea to change this password. To do so, take the following steps:

1. Double-click on the icon on the desktop called Terminal.
2. Run the command **vncpasswd**.
3. Enter a new password.
4. Upon your next VNC, it will prompt for the new password.

Configuring Basic Networking (IP Address Assignment)

Your Netmon server appliance is configured by default to request an automatic IP address assignment through DHCP. In most cases, however, you will want to assign a static IP address to one or more network interfaces.

To assign a static IP or make other networking changes, you'll need to log directly into the Netmon system console, and take the following steps:

1. Double-click the icon on the desktop called Network Admin. You will be prompted for your root password. By default, the password is *netmon*.
2. It will list the available network interfaces. Click on an interface to highlight it, then click Properties.
3. Select either DHCP or Static IP Address. If using a Static IP Address, fill in the IP address, subnet, and gateway.
4. If using a static IP address, click on the DNS tab and enter your DNS servers.
5. Click OK. Your network settings are now changed.
6. Repeat this procedure for each interface that you intend to use.

Note: Normally there is no need to reboot the machine, but under certain circumstances it may be required, especially if you changed your hostname. If you are experiencing network problems after changing your settings, a reboot is recommended.

Final Deployment Tasks

Changing the Operating System Password

Netmon ships with two built-in operating system accounts: root and netmon. The root account is used for configuration and administrative purposes.

For security reasons, it is a good idea to change the password for the root and netmon user accounts right away, as this account has full system-wide privileges, and could provide an easy and dangerous point-of-entry for an attacker.

To change the password, you'll need to log into the system console. Once you have logged in, take the following steps:

1. Double-click on the icon on the desktop called Terminal.
2. Run the command **su**. It will prompt for the current root password, by default it is 'netmon'.
3. You are now running a terminal as the system administrator. Type the command **passwd root** (or **passwd netmon**).
4. Enter your new password.
5. Press CTRL+D, then CTRL+D again. The terminal window closes and your password is now reset.

Getting Started

Once your server has been physically installed and basic setup has been completed, you are ready to log into the Netmon application.

Logging Into the Netmon Application

To log in, simply type Netmon's IP address into a web browser which can access that IP address, like this:

```
http://netmon_ip_address/
```

This will display the Netmon login screen, as follows:

Figure 4 – Netmon Web Login Screen

Username and Password for Initial Login

If you are logging in for the first time, use the User ID **admin** with a password of **netmon**.

Once you log in, it is recommended that you complete the Initial Setup Tasks located in the Settings console.

Performing Basic Setup Tasks

There are 4 quick steps which should be taken immediately after logging in for the first time. These steps allow Netmon to begin discovering devices and services automatically, and also ensures that alert messages can be properly relayed.

To start the Setup Wizard, click the Settings button in Netmon's main menu at the top of the screen, and look for the Initial Setup Tasks link. Click on it, and then click each of the 4 items in turn:

1. Define your Network Range(s) (see *Managing Network Ranges* on page 92)
2. Configure SNMP Automatic Discovery (see *Using the SNMP* Automatic Discovery Service on page 41)
3. Set up Netmon User Accounts (see *Managing User Accounts* on page 86)
4. Alert Testing Utility (see *Troubleshooting Email Alerts* on page 98)

Introducing the Netmon Home Dashboard

The first screen you will see after logging into the system is the Netmon Home Dashboard. This screen is designed to provide you with a high-level, up-to-the-moment overview of your network.

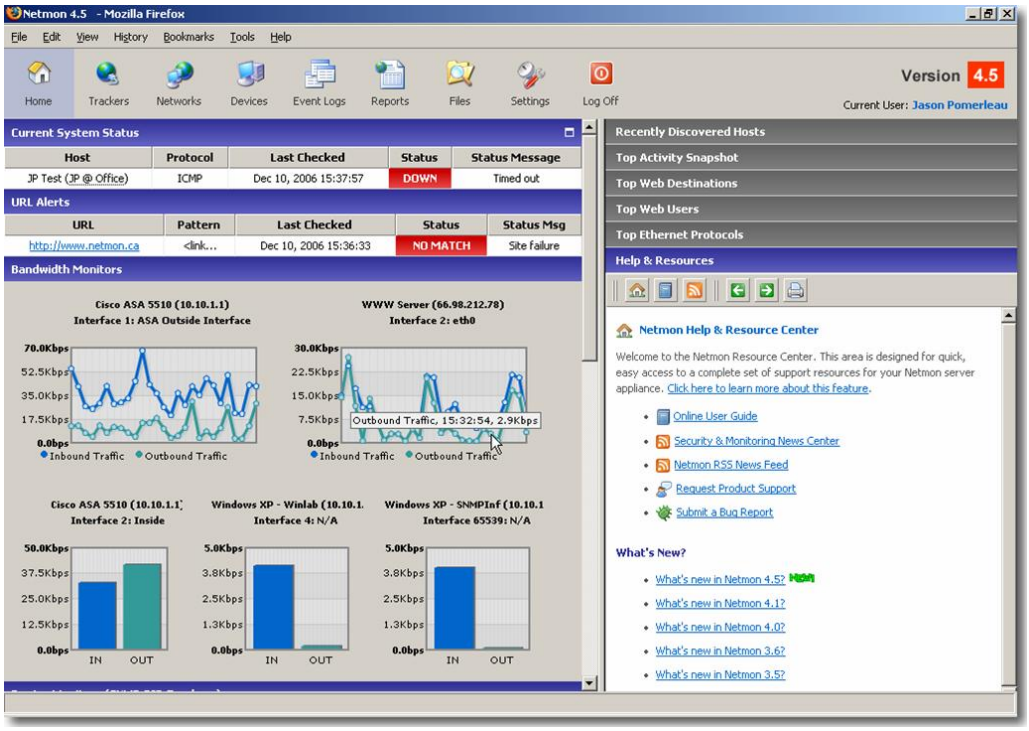


Figure 5 – Netmon Home Dashboard

Panel: Recently Discovered Hosts

The Netmon network autodiscovery service detects new MAC/IP pairs on your network, and can alert you of this situation if you wish. You can locate this panel at the top right of Netmon's Home dashboard. It displays any recently detected MAC/IP pairs. These entries remain in the panel until they are cleared.

How Network Auto-Discovery Works

Netmon uses the Address Resolution Protocol (ARP) to probe for new hosts on your local segment(s). It issues periodic ARP broadcast requests, and checks the responses it receives against its database of known MAC addresses. When a new MAC address is detected, Netmon can be configured to send an alert message.

Clearing Entries

You can remove entries from the recently discovered hosts panel by checking off the entries you wish to delete, then click the **Clear Selected** button. There are also two additional buttons provided for convenience: **Check All** and **Uncheck All** which allow you to select or deselect the entire list at once.

Configuring Alerts

To configure alert recipients for newly detected hosts, click the  button on the Recently Discovered Hosts panel. You'll be able to specify one or more alert recipients in the dialog window that follows.

Panel: Top Activity Snapshot

This panel gives you a high-level overview of the 10 most active client-server conversations over the last 60 seconds, and also shows the TDP/UDP port of each conversation. If Netmon recognizes the port being used, you'll see a friendly name instead of the actual TCP/UDP port.

To get more information for the protocol(s) which are typically used on a particular port, just click the friendly name (i.e. HTTP or FTP) and you'll be taken to a page in the Help & Resources Panel which will tell you what Netmon knows about this port. Netmon ships with a built-in dictionary for over 50 protocols. Each entry in this dictionary contains a high-level overview of the protocol, as well as links to helpful web resources for that protocol.

To get more detail for any host which is shown in this panel, simply click on it. This will take you to a page where that particular host can be explored much more thoroughly.

Panel Actions

 Print an instant Quick Report by clicking this button in the panel.

 Refresh the display with new data by clicking this button.

Panel: Top Web Destinations

This panel shows the top web destinations (based on HTTP requests), averaged over the last 20 seconds.

To get more detail for any destination which is shown in this panel, simply click on it. This will take you to the Visual Network Explorer page where that particular host can be explored in more detail.

What is a 'Web Destination'?

A web destination is simply the recipient (i.e. the server) of HTTP requests. This could be any or all of the following:

- Public websites like www.google.com or www.amazon.com
- Local intranets and web based applications
- Non-Web HTTP traffic (i.e. SOAP or XML-RPC calls)

Panel Actions

 Print an instant Quick Report by clicking this button in the panel.

 Refresh the display with new data by clicking this button.

Panel: Top Web Users

This panel displays the top local hosts which are requesting HTTP web traffic. Traffic rates (averaged over the last 20 seconds) are also provided for reference.

To get more detail for any host which is shown in this panel, simply click on it. This will take you to the Visual Network Explorer page, where that particular host can be explored in more detail.

Panel Actions

 Print an instant Quick Report by clicking this button in the panel.

 Refresh the display with new data by clicking this button.

Panel: Top Ethernet Protocols

This panel shows you the most active Layer 2 protocol usage, averaged over the last 20 seconds, and ordered by the Ethernet frame type.

This panel is extremely useful to get an idea of your overall network traffic load. It aggregates all traffic information for each major Ethernet protocol type, and displays information for each. Using this panel, you can also monitor the usage of non-TCP/IP protocols like IPX/SPX, ARP, as well as network bridging protocols like 802.1d. (Note that 802.1d is a much different protocol from the 802.11 wireless protocol suite).

On most TCP/IP networks, IPv4 (both TCP and UDP) should appear at the top of the list under normal network conditions. Address Resolution Protocol (ARP) is a MAC-to-MAC addressing protocol, is also generally present as well, though at a much lower level. (ARP poisoning attacks could be monitored through this panel.)

Panel Actions

 Print an instant Quick Report by clicking this button in the panel.

 Refresh the display with new data by clicking this button.

Using the Help & Resources Panel

The Help & Resources panel is a completely integrated, one-stop guide to your Netmon server appliance. This panel is built right into the Netmon application, and provides direct access to a rich variety of resources. Using this panel, you can:

-  Access the Netmon User Guide
-  Stay up-to-date on recent network security news with the Security & Monitoring News Center
-  Request technical support, through either the Live Chat system or by sending a message through the built in Support Request Form.
- learn more about specific parts of the Netmon application with context-sensitive buttons located throughout the Netmon user interface.

Other Panel Actions

-  As you move between different pages in the Help & Resources panel, these buttons can help you navigate.
-  All of the pages which are displayed in the Help & Resources panel are automatically printer-friendly. Just click this button for a perfect printed document.

Monitoring Network Activity

One of Netmon's core strengths is the ability to monitor and analyze different types of local and remote network traffic, at a highly detailed level.

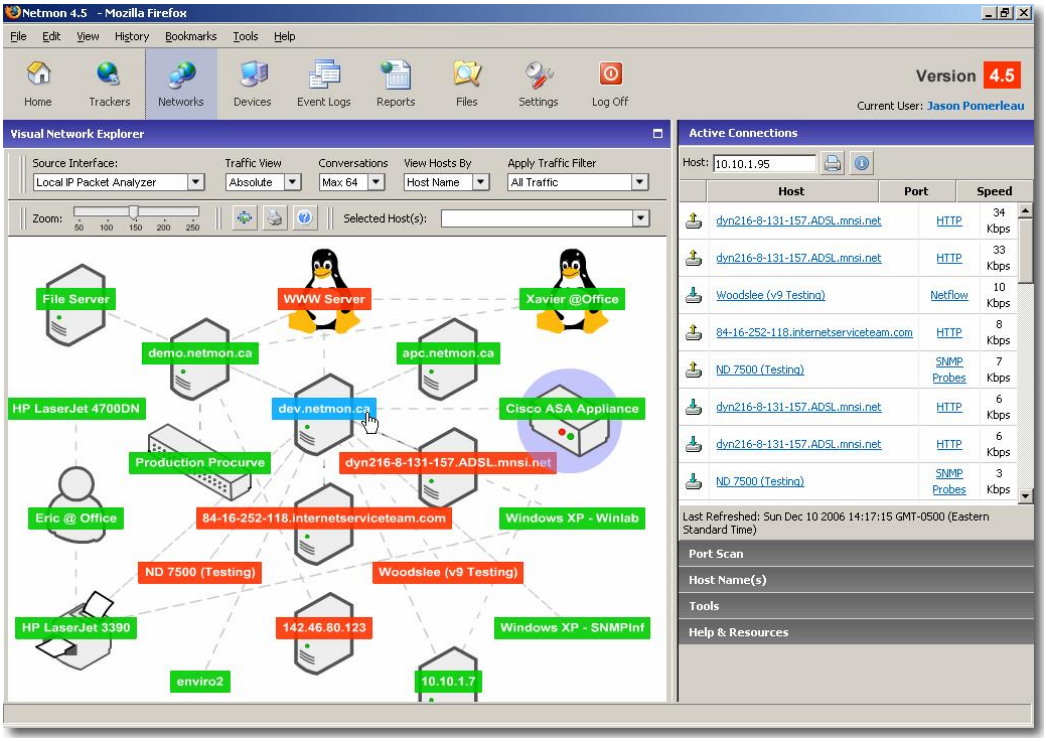


Figure 6 – Visual Network Explorer (VNE)

How Netmon Monitors Network Traffic

Netmon can monitor network activity using either (or both) of the following facilities:

Method #1 - Packet / Protocol Analyzer

The Netmon server appliance captures and analyzes all network traffic which passes across its network card(s). It is most commonly connected directly to a hub or a switch, which has been configured to forward a mirrored copy of all the frames traversing that device.

In these configurations, Netmon receives a copy of the packets traveling across the network segment which is being monitored. This is typically accomplished using a feature called port SPANning or port

mirroring, where your switch has been configured to forward all packets to a specially designated monitoring interface.

Method #2 - NetFlow Protocol

NetFlow is a perfect choice for monitoring remote networks from a centralized location. By using the NetFlow protocol, your remote devices (typically routers) perform packet inspection of all traffic going into and out of various network interfaces. Summaries of this activity are then forwarded as flow packets to a NetFlow-capable monitoring system like your Netmon server appliance.

Using Netmon's Built-In Protocol Analyzers

Netmon features several built-in protocol analyzers which are designed to gather information which passes across either of Netmon's two gigabit network interfaces.

Netmon's native protocol analyzers are generally used on networks to which the Netmon device is physically connected. See *How Netmon Monitors Traffic* above for more information.

Collecting NetFlow Data Streams from Remote Devices

You can use Netmon to monitor and record live network activity on remote networks using Cisco's NetFlow protocol suite. Netmon can accept and process NetFlow v1, v5 and v7 datagrams.

Important In order to properly process incoming NetFlow packets, you must also enable SNMPv2 GET on the device which sends NetFlow packets to Netmon. This allows your Netmon system to properly identify all of the network interfaces on the device.

Activating NetFlow

There are three steps required to monitor NetFlow data from remote devices:

1. Configure your remote device(s) to send NetFlow packets to your Netmon server appliance. Once Netmon detects incoming NetFlow data for a particular device, it will automatically add that device to your Devices Explorer tree.

2. Enable NetFlow data collection for the newly-added device by clicking the Enable NetFlow checkbox when you click on it in the Device Explorer. Once this step has been completed, you'll see a purple NetFlow icon ( ) next to the device in the **Devices Explorer**.

3. Enable NetFlow for the desired interface(s) which are sending NetFlow packets to Netmon by opening each interface and choosing the **Enable NetFlow** option.

Using the Visual Network Explorer

The Visual Network Explorer (VNE) component provides a dynamic, graphical view of your current network activity on local or remote segment(s). You can customize this view in many different ways to find information of interest.

VNE Basics

The VNE displays a live interactive graphical map of your current network activity. As your network traffic patterns change, the display is updated automatically every 20 seconds.

You can move individual hosts around on the map by clicking and dragging on them. You can also move the entire map itself: simply click and drag any empty space in the map. (This is particularly handy when you've zoomed in to view a single part of the map).

You can also use the Zoom tool to your advantage: if a particular host appears too small, or if you simply wish to zoom in for more focus, you can click and drag the Zoom slider. Zoom ranges from 50% to 250% are provided. Don't forget - you can click and drag anything (individual hosts or even the map itself) to navigate the display more easily.

To select a host and view additional details about it, simply double-click on it. Double-clicking will display the Active Connections Panel for that particular IP address, which displays all of the current network connections coming from, or arriving to, that device.

Customizing Your View

The Visual Network Explorer can also be manipulated in a number of ways to help you refine your perspective, and narrow your focus on specific host(s) and/or activities.

Traffic View Traffic view provides two distinct ways to view the network traffic itself - which is represented by a series of dotted or solid lines in between individual hosts. Each of these methods provides advantages in specific situations:

Absolute View displays all network traffic on an absolute scale. Each packet stream is displayed according to the maximum speed your infrastructure can support - usually 100 Mbps or 1 Gbps. For a reference on what each style of line represents, see the Activity Legend. Using Absolute View is usually the best way to monitor traffic if you're trying to understand your overall network load.

Relative View displays traffic according to the most active packet stream on the network. In this scenario, the most active conversation on your network is displayed with a thick, bright red line (see the Activity Legend) and all of the other conversations are scaled in a linear fashion according to this host. Relative View is the best option to use when you want to compare your network traffic to other network

traffic. It allows you to see how traffic from individual hosts compares against the traffic betweenother active hosts.

Conversations Using this feature, you can customize your view to show the Top 16, Top 32, Top 48 or Top 64 conversations. Viewing fewer conversations at once can simplify the view, while viewing many conversations at once can give you a broader perspective.

View Hosts By You can choose to view individual hosts by their IP address or by their host name. If you choose to view by Host Name, Netmon displays the host using its friendly name, if one is available. If a friendly name is not available, Netmon selects the first entry in its name database (giving preference to NetBIOS names, followed by DNS names).

Apply Traffic Filter Using this selection, you can apply any one of Netmon's traffic filters to the VNE display. Click here for more information on traffic filters.

Apply Host Filter Using this selection, you can apply any one of Netmon's host filters to the VNE display. Click here for more information on host filters.

Zoom This tool lets you change the zoom level from 50% to 250%. Simply click on any zoom level, or you can drag the Zoom handle to adjust your zoom visually.

Host Legend

- 10.10.19.47 **Internal (Non-Routable) IPs** - These hosts are displayed in green. (i.e. subnets 192.168.x.x, 10.x.x.x, 172.x.x.x, etc.)
- 63.101.150.100 **External (Routable) IPs** - These hosts are displayed in orange. (i.e. any IP address not included in above non-routable ranges)
- 192.168.1.255 **Broadcast IPs** - Broadcast hosts do not actually physically exist, and are displayed with a purple label, as well as a special icon.
- 10.10.1.10 **Highlighted** - Any host which has been highlighted with the mouse hovering over it turns blue. (Hint: Click and drag!)

Activity Legend

Line Style	Absolute View	Relative View
	32 Mbps and above	Most Active Host

	16 Mpbs and above	
	8 Mbps and above	
	4 Mbps and above	
	2 Mbps and above	
	1 Mbps and above	
	512 Kbps and above	
	256 Kbps and above	
	128 Kbps and above	
	64 Kbps and above	
	32 Kbps and above	
	16 Kbps and above	
	8 Kbps and above	
	4 Kbps and above	
	2 Kbps and above	
	Under 2 Kbps	Least Active Host

Other Panel Actions

 Print an instant Quick Report of the current VNE display by clicking this button.

 Realign Map: If you've moved the map too far, and have lost your view of the hosts and/or activity, this button will realign the display for you.

Panel: Active Connections

This panel shows you all active connections during the last 60 seconds for the selected IP address. To use this panel, you simply enter the IP address of the host you wish to explore, and then press ENTER. Alternatively, you can double-click on any host in the Visual Network Explorer window to see all Active Connections for it.

If Netmon's network sniffer detects any active connections for the selected IP address, they will be displayed in the **Active Connections Panel** window. Each data stream is separated into its own row.

Traffic Stream Direction

The direction of the traffic stream is displayed with an icon, as follows:

This data is **request** traffic. Data from the selected host is being 'uploaded' to the remote host which appears in this row.

This data is **response** traffic. Data from the remote host which appears in this row is being 'downloaded' to the selected host.

Host

The name or IP address of the destination host. The selected IP address has established a connection to this host. If the host name can be resolved, Netmon displays the name of the host here. If the IP address resolves to multiple names, Netmon displays the first hostname in its database , along with a icon, which can be clicked to expand the list.

Port

Netmon identifies the TCP or UDP port of the data stream and shows it in this column. If Netmon recognizes the port, it will apply a friendly label from its database (see Port Label Database). In addition, Netmon contains a built-in protocol dictionary which provides detailed information for a wide variety of protocols.

To learn more about these ports and protocols, you can click the label for additional information, which is displayed in the **Help & Resources Panel**.

Speed

The average speed, over the last 60 seconds, of the data stream.

Other Tips

Alternatively, you can use Active Connections Panel automatically (i.e. without having to manually enter the IP address) through the Visual Network Explorer (VNE). To do this, simply locate the host you wish to explore in the VNE, and double-click on it. This causes the [View Active Connections] IP address of the

host that was clicked to appear in the VNE toolbar. Then, simply click the View Active Connections button (see illustration at left) to automatically open the Active Connections panel for the selected host.

Panel Actions

 Print an instant Quick Report by clicking this button in the panel.

Panel: Port Scan

Using Netmon's Port Scanning Tool

With this tool, you can scan any IP address to see which TCP ports are open and accepting requests.

To scan a host, simply enter its IP address in the IP Address field of the Port Scan panel. Then, click the Scan button to begin the scanning process. (If the Port Scan Panel is not visible, click on its title bar to expand it.)

Caution: Be careful when scanning hosts that don't belong to you. Probing a remote network with a port scanning tool is often considered a form of intrusion attempt.
Types of Port Scan

You can run up to 3 different types of scan with this tool:

Standard Scan This mode scans several hundred well-known ports. This type of scan is probably the best choice for everyday audits, where an administrator's biggest concern is typically focused toward the exposure of common services like FTP, HTTP, or file and printer sharing. To run a standard scan, simply select this option in the Port Scan Panel, and click the Scan button to begin. Standard scans against non-firewalled hosts should be complete in under 10 seconds, while a scan against a firewalled host may take a minute or more.

Complete Scan This mode scans all 65,535 possible ports. It takes longer to run a complete scan (especially against a firewalled host) so generally it is best used when you suspect that a particular host may have been compromised by intruders, viruses and/or other types of malware, or if you have concerns that non-standard services may be exposed. To run a complete scan, simply select this option in the Port Scan Panel, and click the Scan button to begin. (You'll receive a warning

Custom Scan This mode scans a host for a user-specified port or port range. This type of scan is most useful when you are looking for something very specific. To scan a single port, select the Range option, which enables text to be entered in the Range text box. Enter the port number in this box, and then click the Scan button. To scan a range, simply enter a starting port, a dash, and an ending port (i.e. 1000-2000).

Scanning Firewalled Hosts

Scanning a firewalled host can be a good way to ensure that the firewall is exposing only absolutely necessary services. Keep in mind, however, that scanning a firewalled host tends to take much longer than an equivalent scan against a non-firewalled host. This is due to the fact that firewalls do not acknowledge connections on any port which is not permitted to pass through. Thus, the port scanner must wait until a specified timeout period has been reached, before it can determine that a port is truly closed.

Scanning a fully firewalled host (i.e. a host in which no ports are open, or a host which has been configured to ignore ICMP PING requests) can result in a 'Host is unresponsive or behind a firewall' message. In practice, a fully firewalled host should not appear to exist at all, so port scans against them are generally pointless. Microsoft Windows XP SP2 machines have a particularly draconian firewall, and when they have been configured for maximum security, they generally ignore inbound network requests entirely.

Port Scanner Legend

Symbol / Icon	Port Range
	Ports 0 to 25
	Ports 26 to 50
	Ports 51 to 75
	Ports 76 to 100
	Ports 101 to 150
	Ports 151 to 250
	Ports 251 to 500
	Ports 501 to 1000
	Ports 1001 to 5000
	Ports 5001 to 65535

Panel Actions

 Print an instant Quick Report by clicking this button in the Port Scan Panel.

Panel: Host Name(s)

Using this panel, you can manage Netmon's name database, which contains a variety of NetBIOS, DNS and User-Defined host names. Each of these host names maps to an IP address, and often many different host names map to the same IP address. This console allows you to manage names for any host (and even to include your own User-Defined labels) as well as search Netmon's database for host names which match a particular search criteria.

Searching for Hostnames

To search Netmon's name database, enter a search string in the Search Text/IP Address: box on the Hostname Management console. (For example, to search for all hostnames which contain the text "google", simply enter google into the Search Text/IP Address: box) Then click the Search button.

If you wish, you can customize your search, to NetBIOS names only, DNS names only, HTTP Requests only, or User-Defined Names only.

Removing A Host Name

In some cases, a host name may no longer be accurate or relevant. In these cases, you'll want to trim Netmon's name database by deleting inaccurate or outdated names.

To delete any name, simply click the **Delete** link in the **Actions** column beside the particular name which you wish to remove. You'll be prompted to confirm that you really do wish to delete this name from the database. If you're certain, click the **OK** button to proceed, and Netmon will remove the name from its database.

Adding a User Defined Host Name

You can apply your own friendly host name to any IP address. Click the Add New Host button in the Manage Hostname Database panel. An editing window will open in the Settings Editor panel on the right side of the screen.

Enter the IP address and label, then click the Add Hostname button. Your IP address will now appear as your friendly label throughout the application.

Network Tools

The Tools panel contains a variety of useful network diagnostic tools.

Capturing Raw Network Traffic with the Packet Capture Tool

Netmon features a low-level packet capture utility which can "record' network activity - payload and all - for further analysis in a protocol dissector such as Ethereal / Wireshark[8].

To use the raw packet capture tool, take the following steps:

1. Click **Network** > **Tools** > **Traffic Capture**.

2. Choose the number of packets to capture from the available drop-down box. In most cases, it's best to start with smaller captures (100 to 500 packets) and progress toward larger ones (1000 or more) as necessary.

3. Add a label, if desired, to this capture. Labels are used to differentiate between capture files in the File Manager. This step is optional.

4. Choose the network interface from which to capture packet data. You have a choice between eth0 and eth1.

5. Click the **Begin Capture** button to start the capture. Depending on the size of the capture, it may take some time to become available for download in the File Manager.

DNS Lookup Tool

The DNS lookup Tool provides a quick method to perform a DNS record lookup for a particular hostname or IP address.

Traceroute Tool

The Traceroute Tool is a handy tool that evaluates the performance of each network hop between the Netmon server appliance and a target host / IP address[9].

---

[8] Ethereal (now known as Wireshark) is a free, open-source protocol analysis package. It is the world's most popular tool for this purpose. Download a free copy of Wireshark at www.wireshark.org.

[9] Some ISPs / carriers filter the network traffic which is used to support traceroute activity. In these situations, attempts to perform a traceroute will fail at the gateway to that carrior.

Monitoring Network Devices & Services

Netmon can monitor the availability and network performance of virtually any TCP-IP connected device or service which is capable of responding to network requests.

How Netmon Monitors Devices and Services

If you simply want to determine if a host is alive or not, Netmon will use an ICMP PING request to establish the status of the target device. If a PING fails, Netmon triggers any alerts which have been attached to this tracker.

On the other hand, if you are monitoring a specific service, such as port 80 on a web server, or port 25 on an email server, Netmon uses TCP CONNECT method to determine if a service successfully responds to a basic 3-way handshake request. If the handshake fails, Netmon triggers the appropriate email and pager alerts which have been defined for the service monitor.

Introducing the Trackers Console

The Trackers console is where most of Netmon's availability tools are located. To open the Trackers console, click the Trackers button in the top toolbar.

Creating a New PING or TCP Service Tracker

To monitor a new device or service, take the following steps:

1. Click the Trackers button in the top toolbar, and then click the **TCP Service Trackers** or **Ping Trackers** button.

2. Click the **Add New Tracker** button at the top of the Trackers Explorer. This opens the Tracker Manager panel.

3. **Transport Protocol:** In the Tracker Manager panel, choose the type of monitor: TCP or ICMP. TCP is used to monitor network services, and ICMP is used to monitor devices.

4. **IP Address:** Enter the IP address of the host to be monitored.

5. **Friendly Name:** Enter a friendly name / label for the host to be monitored.

6. **Port:** If you have specified a TCP service to be monitored, enter the Port number here. A valid port number is any number between 1 an 65,535.

7. **Interval:** The monitoring interval, in seconds. Monitoring too frequently can generate unnecessary traffic, so try to balance polling intervals with your response needs. A monitoring interval of 60 seconds often a good choice for non-critical devices, and an interval of 20 seconds is optimal for mission-critical devices.

8. **Timeout:** The timeout is the amount of time Netmon will wait for an unresponsive service before queuing an alert, in minutes.

9. **Logging Threshold:** Choose the type of historical data Netmon. By default, Netmon will only log entries to the database when it detects that the device or service is DOWN. You can, however, choose various levels of logging verbosity, from Disable Logging all the way to Log Everything[10].

10. Once you have entered all of the required information, click the **Add Tracker** button to add the service or device to Netmon's monitoring database.

11. Netmon begins monitoring your new device or service within about 10 seconds after adding it.

Attaching Alerts to a PING or TCP Service Tracker

You can attach any number of email and pager alerts to a service or device tracker. To configure alerts for a particular tracker, click the Alerts link in the appropriate row in the Trackers Explorer. This opens the Alerts management panel on the right side of the screen.

When monitoring services, you have the option of being notified when the service goes down entirely, or when network latency for that service crosses a certain threshold (such as 200ms). This feature can often identify failing services before a complete stoppage has occurred.

To add an email alert, take the following steps:

1. Choose a user account from the drop-down list in the Email Alert column.

2. Choose a value for Max Latency. You can choose Service Down or a latency value from 100ms to 1500ms.

[10] If you want to be able to subsequently create a Latency analysis report for a particular device or service, choose the LOG EVERYTHING option.

3. To attach a Conditional to this alert, select the appropriate Conditional from the available drop-down list. If no Conditionals are configured, 'NONE' is the only option. Complete the action by clicking the **Add Alert** button. Click here for more information on Conditionals.

Removing an Existing Alert

To remove an alert which has already been set, click the **Delete** link next to the associated alert.

Modifying a PING or TCP Service Tracker

To modify the tracking parameters for a device or service which has already been set up, take the following steps:

1. Locate the device or service you wish to modify in the Trackers Explorer.

2. Click the Edit link which appears in the same row as the selected service. This opens the Tracker Manager window, and displays all of the configurable information for this particular service. Some items cannot be changed, such as the IP address or the Protocol / Port information.

3. Once you have made your desired changes, click the **Update Tracker** button.

Removing a PING or TCP Service Tracker

To remove an existing service monitor, take the following actions:

1. Locate the service you wish to remove in the Trackers Explorer.

2. Click the **Del** link which appears in the same row as the tracker you wish to remove.

3. A confirmation window appears, asking if you're sure you want to remove this service from the database. If you're sure, click **OK**, otherwise click the **Cancel** button.

Monitoring Devices (SNMP)

Netmon has a wealth of features for monitoring highly detailed performance metrics on network-connected devices such as routers, firewalls, switches, servers, printers, UPS systems and more.

Introduction to Simple Network Management Protocol (SNMP)

Effective network monitoring encompasses a broad range of responsibilities. You need to understand your network traffic from several vantage points, but it also becomes important to monitor the health, availability and load of many different kinds of mission-critical devices.

The solution is the Simple Network Management Protocol (SNMP): a widely supported monitoring and management protocol for network-aware devices. Managed devices, as SNMP-capable devices are otherwise known, can include things like switches, routers, multi-function printers, fax stations, firewalls, thin clients, wireless transmitters, and much more. Thousands of different devices support the SNMP protocol.

SNMP provides the ability to query and update a managed device remotely. Using this protocol, you can retrieve a potentially rich set of information about a particular device: data such as inbound and outbound traffic levels, current connections, CPU load, memory status, usage history, error messages, device status, and countless other details. This is really nice stuff to know. Furthermore, SNMP 'write' operations can even allow devices to be configured and managed remotely.

Devices can also be configured to automatically 'push' SNMP data to a remote monitoring or management system. For example, you might configure a laser printer to send information about current toner level. These UDP datagrams are known as SNMP traps, and they're generally sent to a remote monitoring system where they're collected and handled appropriately. (Netmon 3.5 will feature an SNMP trap handling engine.)
The SNMP Protocol

The SNMP protocol itself is a relatively simple request-response protocol. It works at the application layer, and typically utilizes UDP ports 161 and 162.

The choice of UDP may seem a bit unusual for a request-response protocol, but SNMP was designed from the outset to move across the network as 'non-critical' traffic. In high load situations, UDP packets that are dropped from the network are not resent by the originating host. This reduces network congestion in critical load situations. To ensure that SNMP traffic doesn't unnecessarily burden a network, its designers skipped the higher overhead of a full-blown TCP connection in favor of a more graceful failure scenario.

Every managed device keeps a hierarchical database of values, known as a Management Information Base (MIB). These MIBs are sent as numerical indexes (known as object identifiers, or OIDs) in the SNMP packet payload, and each one represents some type of configuration detail. Each MIB has an associated meaning, such as the following:

MIB: Cisco Router
OID: 1.3.6.1.4.1.9.1.1

The Good, the Bad and the Ugly

White it is certainly true that SNMP can provide you with a rich source of information for every managed device on your network(s), it also comes with a few drawbacks.

First off, while SNMP is indeed a ‘simple’ protocol, its real world implementation is not very simple at all. SNMP data is built around the idea that any kind of information can be stored and communicated by a managed device. Of course, different devices will want to communicate different kinds of data. Switches will tell you how much traffic is going in and out of each port, and so will firewalls, but printers might tell you how many pages have been printed today, or how much ink is left in each of the cartridges.

The result is that every device implements SNMP data structures in their own unique way, and there are only a handful of standard OID/MIB interfaces which are available across all types of devices. This makes the task of using SNMP data in a comprehensive monitoring or management system a non-trivial undertaking. SNMP management systems tend to be large, unwieldy and tremendously expensive systems, and their complexity can make one question the benefits of using SNMP in the first place.

SNMP and Security

The introduction of any new protocol on the network merits some attention, and SNMP deserves more scrutiny than most. Unfortunately, the most popular implementations of SNMP (known as SNMP v1 and SNMP v2) are not particularly well known for their strong security. In fact, SNMP's security record is so dismal, it has picked up a new dual meaning: Security Not My Problem (SNMP).

SNMP services and protocols are not necessarily a direct security threat themselves: attacks on SNMP are relatively uncommon. This is probably due to the fact that there are thousands of different implementations out there - any kind of attack would likely have to be narrowly focused at a single device, or class of devices.

However, a much larger security threat exists with the information that SNMP makes available to a potential intruder. SNMP data is transmitted in clear text, which could pose a problem if you're sending certain kinds of information over a non-private, unprotected network such as the Internet. In fact,

unfettered SNMP read access could allow an attacker to gather hundreds of configuration details about your network.

Many SNMP-capable devices are shipped and installed with weak (or well-known) SNMP community strings. A community string is the closest thing to a password in SNMP v2 and earlier devices, so it's incredibly important to ensure that you change these strings to strong passwords that meet modern security standards.

Fortunately, some of the most pressing security issues have been resolved with SNMP v3, the latest and greatest implementation of this protocol. Encrypted traffic is now supported, along with much stronger authentication mechanisms. However, there are still relatively few devices which support this new implementation of the protocol, despite its age - nearly 7 years at the time of writing.

In the meantime, you should review your managed devices, and evaluate their roles in your monitoring strategy. Check for the following:

1. Does the SNMP service on this device need to be active at all? Do I really need to gather performance data from this device? (In many cases the answer is *Yes*.)

2. Is the Community String set to a strong password phrase?

3. What kind of SNMP data is being polled from this device? Is it safe for this information to traverse the LAN/WAN/Internet?

4. Have SNMP write operations been disabled?

SNMP's Role in Network Monitoring

SNMP has a few warts, but can nevertheless occupy a very effective role in an overall network monitoring strategy.

Despite the rich variety of information it makes accessible, SNMP really shouldn't be used to monitor the network itself. Many monitoring and management systems use the SNMP protocol exclusively to gather information about the network, but if this is the only way you are monitoring, then you’re likely to be missing out on the big picture.

Think about it. In most cases, you will probably value the integrity of your entire network over that of any individual host. SNMP is great to gather data about devices, but in these situations you just can't beat a packet sniffer to get a real understanding of your network's actual state. Nevertheless, SNMP plays an important role in an overall network monitoring strategy.

Netmon is capable of retrieving traffic-related information from a wide variety of SNMP-capable devices, and the nice part is that it can grab data for each distinct network interface. This is especially helpful for switches, firewalls and routers, where you'll want to monitor traffic levels across each physical port. To work with this information, you'll need to take two steps.

To gather SNMP traffic data from your device, first enable SNMP on your managed device, and configure it to allow SNMP read (or "polling") operations. This process varies greatly by manufacturer. Some devices (like switches and routers) may need to be configured through a command line interface, while other devices (such as printers and other multifunction products) may provide a nice slick web interface. Be sure to specify a strong community string pass phrase wherever possible.

The second step is to add your SNMP device in Netmon's SNMP Device Explorer. You'll have to supply your device's community string to Netmon. Once you have added your device, the Netmon SNMP Service will begin polling that device for information. For additional configuration information, see the Netmon User Guide.

Once these steps are completed, you should start to see SNMP traffic data within a few minutes. Netmon's SNMP viewing tools allow you to easily spot trends and spikes for each distinct device interface, and you can historical charts and graphs as well.

Using the SNMP Automatic Discovery Service

The simplest and easiest way to add new SNMP-capable devices to your Netmon server appliance is to let Netmon do most of the work for you. In most cases, Netmon can identify a large number of SNMP-capable devices automatically in just a few minutes.

The SNMP Auto Discovery service scans your local network range(s) for SNMPv2-capable devices, and attempts to connect to them with the default community string public. If a successful connection is made, Netmon automatically adds the device to your Device Explorer collection. Devices which have been discovered in this fashion have a icon next to them in the Device Explorer tree.

Using a Different Community String?

Netmon's automatic discovery service can be configured to use any community string you wish. To make changes to the community string used by the SNMP Auto Discovery service, take the following steps:

1. Click **Settings > Netmon Services**.

2. Locate the SNMP Autodiscovery service in the list, and click the **Configure** link next to it.

3. Enter your custom community string in the **community** text box, and then click the **Update** button next to it. (You can also supply multiple community strings separated by a comma. For example: *public,community1,community2,community3*)

4. Click **Settings > Netmon Services** again.

5. Locate the SNMP Autodiscovery service in the list, then stop it using the **Stop Service** button. When the page reloads, click the **Start Service** button. This will restart the SNMP Autodiscovery Service using your new Community string[11].

Using the Devices Explorer

Netmon displays all SNMP devices in a tree format in the Device Explorer. You can reach the Devices console by clicking the **Devices** button in the top toolbar. SNMP-capable devices are identified with the following icons:

- Designates a host/device which has been automatically detected by Netmon as SNMP- or NetFlow-capable. It is then up to you to activate one (or both) of these services on the device, and assign the appropriate Device Dashboard[12].

- Designates a host/device that supports SNMP.

- Designates a host that/device supports NetFlow packet streams.

To view a high-level overview of a device and all of its interfaces, simply click the device in the SNMP Device Explorer, which displays a global view of the device, along with a summary view for each interface. Input and output is displayed on an LED-style graph.

To drill further down and view detailed information for each individual interface, simply click the port icon next to the device, and select an interface node from the tree by clicking on it. This will bring up the SNMP Interface Explorer window, which provides a detailed view of that specific interface.

---

[11] It is not strictly necessary to restart the Autodiscovery Service after changing the Community string. However, doing so will ensure that the service begins scanning using your new Community string right away. If the service is not restarted, Netmon will complete its current scan using the old community string.

[12] See *Device Dashboards* on page 48.

Adding a New SNMP Device

First, you must enable SNMP v2 GET requests (or polls, as they are sometimes known) on your managed device. This process varies from manufacturer to manufacturer, so consult the documentation for your device to determine what steps are necessary to enable this capability.

Be sure to specify, or take note of, the device's Community string. The Community string is essentially a password for retrieving SNMP data, and this string will need to be provided to Netmon.

Once you have enabled SNMP on your managed device, take the following steps in Netmon:

1. Click the **Add New Device** button at the top of the SNMP Device Explorer.
2. Enter the IP address of the device into the IP Address field.
3. In the Label field, specify a friendly name for your device, such as 'London Office Router'.
4. Choose a sampling interval and enter it into the Sample Every: text box. Netmon uses a default value of 60 seconds, but you can specify any interval you like.
5. Enter the community string that your SNMP managed device requires in order to answer SNMP v2 queries.
6. Be sure the **Enable SNMP** checkbox is checked.
7. If you anticipate receiving NetFlow data streams from this device, check the **Enable NetFlow** checkbox. Otherwise, leave it unchecked.
8. Click the **Add Device** button.

Note: Once you have added a new SNMP device, it can take Netmon several minutes or more to discover all of the interfaces and begin gathering SNMP data. In some cases, it could take as long as one hour for data to appear in Netmon's console.

Updating an Existing SNMP Device

You can update the sampling frequency, community string or friendly label of any SNMP device by doing the following:

1. Locate the device you wish to modify in the SNMP Device Explorer, and click on the main device node.

2. Update the necessary fields, and click the **Update** button or press ENTER to save your changes.

Removing an SNMP Device

To remove an SNMP device, take the following steps:

1. Locate the device you wish to remove in the SNMP Device Explorer, and click on the main device node.

2. Locate the **Remove Device** button in the detail window and press it. You'll be asked to confirm that you really want to delete this device. If you're sure, click OK to proceed with the delete operation.

Caution: Deleting an SNMP device can take a long time, because all of the historical data that was collected for it must also be deleted. Depending on the size of your database, this procedure could take anywhere from 10 seconds, to several minutes or more.

Using the Device Toolbar

The device toolbar appears at the top of all device-related pages. It corresponds to the collapsing menu which can be seen in the Device Explorer tree, so you can use whichever navigation style you prefer.

Figure 7 – Device Toolbar

To see a brief description for any toolbar button, simply hold your mouse over it.

 **Device Dashboard** Return to the home dashboard for this device.

 **Device Notes** View notes history for the selected device.

 **Network Activity** View network activity statistics for the selected device, or manage network activity monitoring preferences. (If the selected device does not have a Dashboard associated with it, this page becomes its dashboard.)

 **Events and Logs** Review Syslog and Event Log history for the selected device.

 **SNMP MIB Walk (Full)** Performs an SNMP walk on all known branches of the management tree. Depending on the amount of management information exposed by the selected device, this operation can be a resource-intensive operation. In extreme cases, it can take up to one minute for the walk to complete.

 **SNMP MIB Walk (Enterprise)** Performs an SNMP walk on the enterprise-specific branches of the management object tree. This operation is less resource intensive than a full SNMP walk.

 **SNMP Object (OID) Trackers** Browse OID object trackers for the selected device.

 **SNMP Trap Messages** View SNMP trap messages which have been sent by the selected device to your Netmon system. Click here to learn more about Netmon's SNMP Trap Handler Service.

Using the Interface Explorer

The SNMP Interface Explorer provides a detailed view of a specific device interface. For switches, routers, firewalls and other networking-oriented devices, each of these interfaces could represent a physical Ethernet network jack, or they could also be 'virtual' interfaces, such as those used for VLANs and local loopbacks.

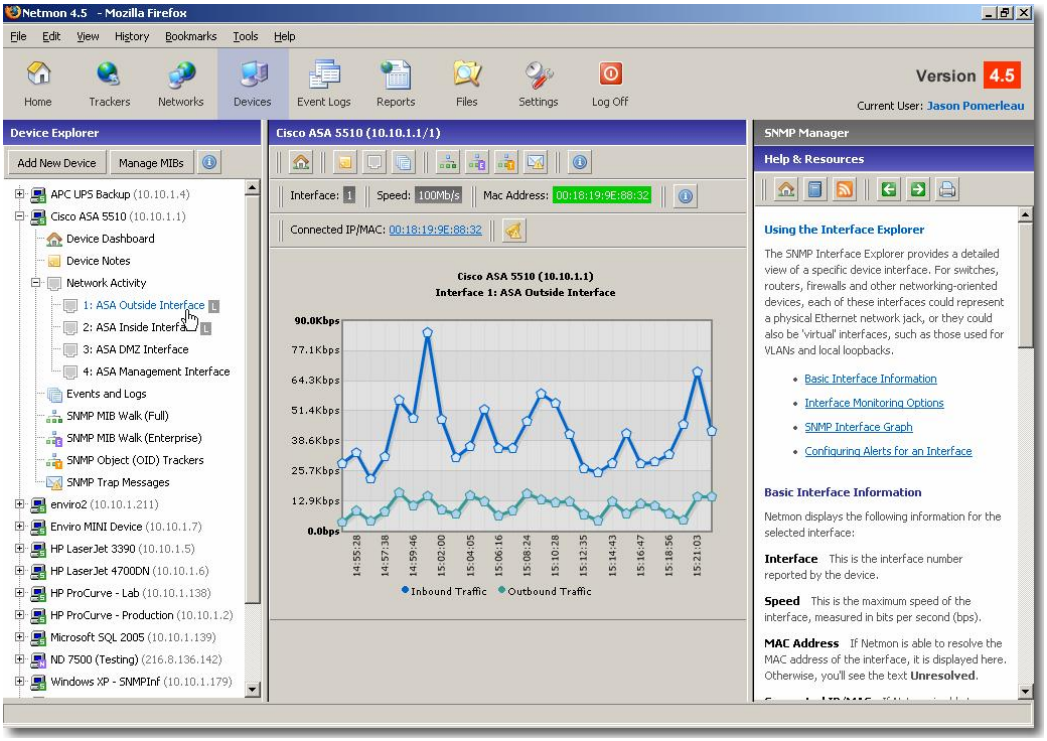


Figure 8 – SNMP Interface Explorer

Basic Interface Information

Netmon displays the following information for the selected interface:

Interface This is the interface number reported by the device.

Speed This is the maximum speed of the interface, measured in bits per second (bps).

MAC Address If Netmon is able to resolve the MAC address of the interface, it is displayed here. Otherwise, you'll see the text Unresolved.

Connected IP/MAC If Netmon is able to determine the IP or MAC address of the host that is connected to this interface, it is displayed here. Otherwise, you will see Unresolved.

Label This is the interface's friendly label. By default, Netmon displays the label provided by the SNMP host. However, you can override this label by typing your own text into the textbox, and clicking the Update button.

Display on Home Page This checkbox allows you to show recent activity for this interface on your Netmon home page. For example, you may want to display all of your outside Internet interfaces on the Home page. Simply toggle the checkbox on or off, and click the Update button to save your changes.

Interface Monitoring Options

Several different options can be set for monitoring specific interfaces. To set these options, click the desired interface in the Device Explorer, and you will see available options in the **Settings Editor** window in the top right of the screen.

Label By default, Netmon uses the *ifDesc* value in the MIB tree to label the interface. However, you can apply your own custom labels to an interface by entering a new value here.

Display on Home Dashboard This checkbox sets whether or not a graph will be shown for this interface on the Netmon home dashboard.

Enable SNMP Logging This checkbox sets whether or not to record historical bandwidth utilization data for this interface in the database. The length of time that data is kept depends on the historical data policy you set for the SNMP Interface Monitoring Service, and can range from 1 day to forever. When this checkbox is selected, you'll see a  icon next to that interface in the Device Explorer.

Enable NetFlow This checkbox sets whether or not Netmon should expect incoming NetFlow packets from this interface. When this checkbox is selected, you'll see a  icon next to that interface in the Device Explorer.

SNMP Interface Graph

The SNMP interface graph shows the input/output information for that interface. To view the interface graph, click on the interface itself in the Device Explorer (or locate it in the Network Interfaces branch of the Device Explorer tree) and you'll be brought to the Interface Explorer.

The type of graph you'll see depends on whether or not you've enabled SNMP logging for that interface. If SNMP logging is enabled for the interface, you'll see a line chart showing inbound and outbound bandwidth utilization going back 30 minutes. If SNMP logging is not enabled, you'll see a bar graph showing the last inbound/outbound traffic statistics for that interface.

Did you know? You get an exact traffic figure for each point on the graph by holding your mouse over the data point.

Configuring Alerts for an Interface

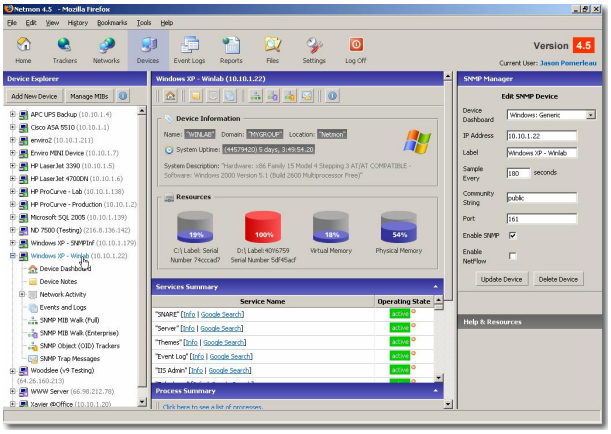
Netmon can send an email or pager alert when any specified interface goes above a user specified threshold. To add or remove email or pager alerts for a specific interface, take the following steps:

1. Click the  button for the selected interface. This will open the SNMP Manager window on the right side of the screen.
2. Enter a Label, if desired, for the alert.
3. Choose a recipient from the available list.
4. Choose an Alert media: email or pager.
5. Enter the bandwidth utilization point, as a percentage, at which the alert should be triggered. For example, to be notified when the interface reaches 90% capacity, enter **90** here.
6. Choose a traffic direction. This selector allows you to receive alerts on Inbound traffic only, Outbound traffic only, or either direction.
7. Click the **Add New Alert** button to create the alert trigger.

Your bandwidth alert has now been created.

Device Dashboards

Device dashboards allow you to view key performance metrics (such as CPU usage, RAM and much more) for several common platforms. Expensive SNMP walks are no longer required to review the most common metrics.



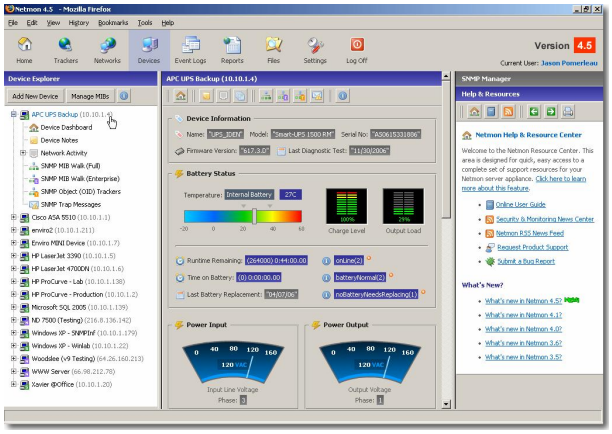


Figure 9 – Sample Device Dashboards

Assigning a Dashboard to a Device

To use a built-in dashboard for your device, take the following steps.

1. Ensure that there is a dashboard for your particular device.
2. Click the **Devices** button in the top toolbar.
3. Locate your device in the **Device Explorer** on the left side of the screen. When you find your device, click on its name. This will open the device's current dashboard.
4. Locate the **SNMP Manager** window on the top right corner of the screen.
5. Make the appropriate dashboard selection in the Device Dashboard drop-down box.
6. Click the **Update Device** button.

Troubleshooting Dashboards

- Device dashboards require appropriate SNMP support on the monitored host. If SNMP services are not enabled on your target device, you will not be able to retreive any dashboard data for that device.
- In addition to SNMP support on the target device, Netmon also requires the appropriate MIB file(s) which match the target device profile in its own MIB repository. These MIB files are, in most cases, stored in your Netmon system automatically, but it is possible to inadvertently remove them in Netmon's MIB File Browser.
- Not all metrics will necessarily be exposed by all devices which belong to a particular classification. In these cases, some metrics will be unresolved.

Browsing SNMP MIBs

How Netmon Retrieves Management Information

Netmon uses the SNMP Walk facility to explore the exposed Management Information Base (MIB) tree for a particular device.

Caution SNMP Walks can be very resource-intensive operations, and have been known to crash some older devices. You should always exercise caution when walking mission-critical devices, especially ones which are already under a heavy workload.

What is a MIB?

A Management Information Base (MIB) generally defines the set of parameters that an SNMP management station can query (or set) in in an SNMP-enabled device. It is essentially a collection (or more than one) of information that can be gathered from an SNMP-enabled device.

Supported MIB Data Types

Netmon automatically recognizes the following common MIB data types:

32 Bit - Any 32-bit value. This value is generally expressed as an integer.

Gauge - Any 32-bit value. This value is generally expressed as an integer.

Hex - A 32-bit hexadecimal number.

Integer - Any valid integer.

Host Address - An IP address.

OID - A numeric OID reference string.

String - A string value.

Timeticks - usually expressed in milliseconds or microseconds.

Managing Custom SNMP MIBs

Netmon permits the uploading of custom MIBs to its repository. Once imported, OIDs specific in the MIB definition will be replaced with the translated, human-friendly representations.

Uploading a Custom MIB

To upload a custom MIB, click the Manage Custom MIBs button at the bottom of the SNMP Device Explorer panel. This opens the MIB File Manager in the middle pane.

Click the **Upload New MIB** button, which opens the SNMP Manager window in the rightmost panel. Click the Browse button to locate the MIB file on your local system. Once you have selected a file, click the Upload button to import it into Netmon.

In order to successfully import a MIB, all of its dependent MIBs must already be present in the system. If Netmon detects that a MIB being imported is missing any of these dependencies, it may reject the upload with an error message. You must identify the missing dependent MIBs (usually by examining the *IMPORTS* declaration at the very top of the MIB definition).

Viewing a MIB Definition

To view an uploaded MIB, simply click on its name, or select the **View** link in the **Actions** column next to the MIB you wish to examine.

Using the OID Tracker Service

Netmon's SNMP OID tracker service allows you to watch a specific OID management point for changes. This is an extremely flexible service that can be used to monitor hundreds or thousands of different performance metrics from SNMP-capable devices.

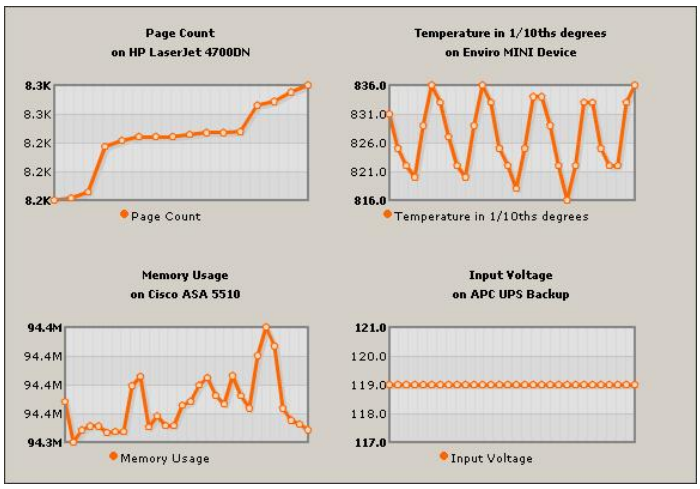


Figure 10 – Sample OID Trackers

What is an OID?

An Object Identifier (OID) represents a single piece of information about your device. OIDs belong to a much larger information repository known as a Management Information Base (MIB). A MIB is a tree-like structure (similar to the Windows Registry) which has OIDs as its branches and leaves.

Many network devices can expose hundreds, thousands, or even tens of thousands of OIDs, with each one representing some piece of data related to the configuration and operation of that device.

Browsing OIDs with the MIB Browser

You can browse different branches of the MIB tree with Netmon's built in MIB Browser. See *Browsing SNMP MIBs* on page 49 for more information.

When you find an OID of interest in the MIB Browser, you can click the **Add Tracker** link next to it to have Netmon watch that object at any desired interval.

Creating an OID Tracker

Netmon allows you to track virtually any OID management point on the MIB tree. OIDs can contain different types of data. The most common data types are:

- **Integer** [Example: 125658]
- **Counter** [Example: 40002]
- **Gauge** [Example: 55]
- **String** [Example: "HP LaserJet 4600DN"]

When tracking OIDs, Netmon renders *Integer*, *Counter* and *Gauge* data types in a similar fashion. Text data types are displayed as a small datagrid.

When you find an OID of interest in the MIB Browser, you can click the **Add Tracker** link next to it to have Netmon watch that object at any desired interval. You will then be prompted to enter the following information:

Label Apply a descriptive label to this OID Tracker. Netmon will suggest a label based on the OID you have selected, but it can often be beneficial to add additional information here. This label is the main descriptive field used for Netmon’s email and pager alerts.

Sample Every The number of seconds between successive polls. Be sure to choose an appropriate value here.

Enable Logging When this box is checked, it tells Netmon to record all historical poll results for the specified OID Tracker. If the box is left unchecked, Netmon simply records the latest result to the database.

Display on Home Dashboard If this is an important OID Tracker, you can display it on the Netmon Home Dashboard. Depending on the logging selection you have made (see above) this tracker will appear as a line chart or a single-value panel.

Attaching Alerts to OID Trackers

In addition to tracking OID values, Netmon can notify you when the value of an OID exceeds a specific threshold. For example, you may want to be notified if CPU utilization exceeds 90%, or if temperature in a rack enclosure exceeds 85 degrees, or if the operational state of a service is anything except “running”.

To attach an Alert to an OID Tracker, take the following steps:

1. Locate the desired device in the **Device Explorer** window on the left side of the **Devices** console and click on it.
2. Click the **OID Trackers** button  in the device toolbar.
3. Locate the Tracker you wish to attach alert parameters to, and then click the **Alerts** link next to it.
4. Enter the comparison value and expression in the boxes provided, and click the **Add Alert** button. Netmon will evaluate the comparison expression at each polling interval. If the comparison expression evaluates to **false** during any checkup, an alert message is relayed.

Modifying an Existing OID Tracker

To edit the tracker, click **Edit**. Do delete the alerts for a tracker, click Alerts next to the tracker and then press **Del** next to the alert you wish to delete.

Note: It is not possible to edit existing alert parameters. To modify an alert, you must delete it and create a new one.

Removing an OID Tracker

To delete your new tracker, simply press Del next to your tracker in the list of OID Trackers for that device. All associated alerts for that OID will also be removed automatically.

OID Tracking Tips

- The OID Tracker service is ideal for monitoring specific metrics that may not be exposed on a Device Dashboard. In many cases, hundreds or even thousands of data points are available, but

only a handful of the most common metrics are displayed on the dashboard.

- OID tracking is used to monitor the operating state of Windows services. See *Monitoring Windows Services* on page 56 for more information.

- Choose an appropriate monitoring interval for your OID tracking metrics. This saves processing resources and also keeps your database size optimized. For example, you may want to monitor RAM utilization on your router as frequently as every 60 seconds, while monitoring the pages printed on a network printer every 2 hours.

Processing SNMP Trap Messages

Traps are messages that are sent by managed devices automatically in response to some activity or condition taking place. Your Netmon system can process these incoming trap messages, and can (optionally) log them to the database and/or alert you when they arrive.

Sending SNMP Traps to Netmon

In order for Netmon to process SNMP trap messages, you must first configure your SNMP device to send trap messages to Netmon's IP address. Netmon expects to receive SNMP trap messages over UDP port 162, which is the most widely used port for this service.

Once you begin sending trap messages from your device, Netmon will identify unique traps that arrive, and record them in its database. Once Netmon identifies a trap, then you have the option of logging it and/or attaching an alert to it.

Logging SNMP Traps

In order to log an SNMP trap, Netmon must first recognize it. If you click the SNMP Trap Messages button, you will see a summary of all trap messages which Netmon has identified. To activate logging for a particular trap, simply locate it in the list, and click the **Enable Logging** button. Netmon will then record incoming traps from that OID to its database.

Trap Alert Services

If you'd like to be alerted when a particular type of SNMP trap message arrives, you must first enable logging for that trap (see above). Once you have enabled logging, click the **Alert**  **button** next to the trap you wish to receive alerts for. The SNMP Manager panel opens, and you can add an alert recipient to the trap.

Using the Notes Manager

Starting with Netmon 4.0, you can now associate one or more notes to specific devices. Using this facility, you can record service histories, backup configurations, and virtually any information that can be stored in a plaintext format.

Adding a New Note

To add a new note to a specific device, take the following steps:

1. Locate the device in the **Devices Explorer** and expand the selection so that its sub-items are visible.
2. Click the Notes selection in the Device tree, followed by the **Add New Note** button in the middle panel.
3. Enter a subject line (required) for the note.
4. Enter (or paste) the contents of the note into the Note textbox.
5. Click the **Save Changes** button to commit the note to the database.

Modifying an Existing Note

To modify an existing note, take the following steps:

1. Locate the note you wish to modify in the **Notes Explorer**, and click the **Edit** link.
2. Make any necessary changes to the note's subject or contents in the **SNMP Manager** window on the right side of the screen.
3. When you have finished making changes, click the **Save Changes** button to commit the updated note to the database. Netmon also automatically records the date/time that the note was modified.

Removing a Note

To remove/delete an existing note, locate the note and click the **Delete** link next to the Note title.

Monitoring Windows Services

Netmon can monitor your Windows services such as IIS, FTP, or any other program that runs as a Windows service.

This is done using SNMP, so first you must configure SNMP support on your Windows system. This can be done as follows:

Part I - Enabling SNMP support on Windows 2000/XP/2003 Hosts

If you have already enabled SNMP on your Windows system, you can skip this step.

1. Click **Start** > **Control Panel** > **Add/Remove Programs**.
2. Select the **Add/Remove Windows Components** button.
3. Ensure that the Management and Monitoring Tools option is checked.
4. Click **Start** > **Control Panel** > **Administrative Tools** > **Services**. Locate the service called *'SNMP Service*' and make sure it is running.
5. Right click the SNMP Service and select the **Properties** option.
6. Select the **Agent** tab and make sure all the services are checked.
7. Select the **Security** tab, where you can configure the community string, and which hosts SNMP will accept requests from. (Be sure to make a note of this community string. You'll need to provide it to Netmon later.)
8. Click the **OK** button.
9. Restart the SNMP service, by right clicking on it and choosing **Restart Service**.

Part II - Monitoring a Windows Service in Netmon

Now that SNMP is running on your Windows server, we can now configure Netmon to monitor Windows services. This is done through the Devices section, as follows:

1. Click the **Devices** button in the Netmon top toolbar.

2. Add the Windows device to your SNMP device list, if it is not already present. (See *Adding a New SNMP* Device on page 43 for more information). Be sure you specify an appropriate Windows dashboard.

3. In the Device Explorer, click on the Windows device. This will bring up its dashboard, where you will be able to see various pieces of information for the target system. You will also see a section called **Services Summary**. Click on the link below the header to see a list of Windows services[13].

4. Locate the service you wish to monitor, and click the Add Tracker button: ( )

5. Enter the Label you wish to use for the tracker. Netmon will pre-fill the OID value here (svSvcOperatingState) but it is a good idea to over-write this label with the name of the service you are monitoring.

6. Choose how often you want it to sample (Sample Every), whether you want this tracker logged or not, and check off Display on Home Dashboard if you would like this tracker to appear as a Dashboard on your home screen.

7. Click **Add Tracker** to finish.

8. Now that the tracker is added, we can attach an alert onto it to send us emails when the tracker value changes. To do this, select OID Trackers under the device in Device Explorer and click Alerts next to the tracker we just created. Windows uses the following values for service status:

   -1 = not present or not running
   1 = running
   2 = continue pending
   3 = pause pending
   4 = paused

9. Here you can set up your alert. Enter a Label for this alert and select a Recipient and the Media Type by which to send the alert. Enter a Value Threshold of **1**, and select Comparison Expression to be **'Not Equal'**.

10. Click **Add Tracker** to finish.

11. Your alert is now set up. You should receive an alert when a Windows Service stops running.

---

[13] Don't see this header on your device dashboard? It is most likely that you have not associated the correct Windows dashboard to the device. See *Device Dashboards* on page 48 for more information on assigning a dashboard to your device.

Modifying an Existing Windows Service Tracker

To edit the tracker, click the Edit link next to your tracker in the list of OID Trackers for that device.

Note: It is not possible to edit existing alert parameters. To modify an alert, you must delete it and create a new one.

Monitoring SYSLOG and Event Logs

Using the Event Log Explorer

Netmon's built-in SYSLOG server allows you to manage SYSLOG and event log data from a variety of hosts in a single, integrated console.

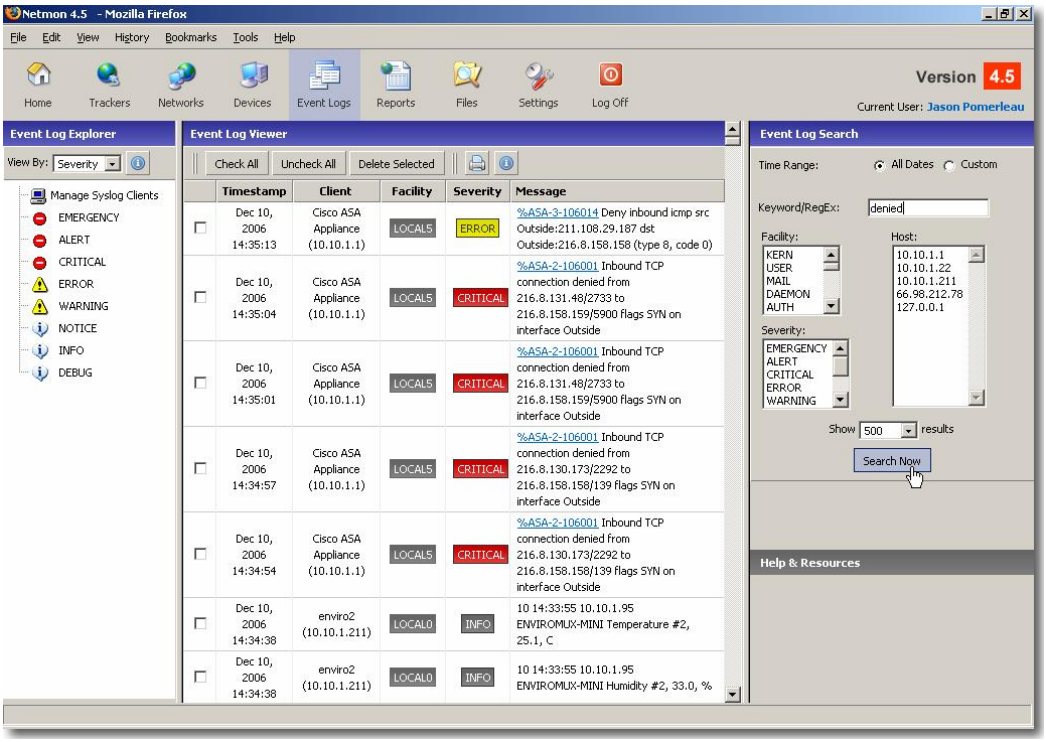


Figure 11 – Netmon Event Logs Console

Setting Up SYSLOG Clients

In order to manage event log data in Netmon, you must first configure your SYSLOG-capable clients to send log messages to Netmon's IP address.

Important: Netmon expects to receive log data over UDP port 514. Most SYSLOG message systems should be configured by default to send messages over this port. However, if you're not seeing expected SYSLOG data in Netmon, you may want to ensure that your client software is configured to use this protocol/port combination.

Once you have configured your client device(s), take the following steps in Netmon:

1. Click the **Manage SYSLOG Clients** option in the **SYSLOG Explorer** window.
2. Click the **Add New SYSLOG Client** button in the **Manage SYSLOG Clients** window.
3. Enter the necessary information in each field (as detailed below) and then click the **Add Now** button.

Netmon requires the following information:

IP The IP address of the SYSLOG client.

Facility The message facility to collect. This option defaults to any (or all) facilities.

Min. Severity The minimum message severity level that Netmon should collect. Netmon will ignore all SYSLOG messages which fall beneath this severity threshold.

Browsing SYSLOG Data in Netmon

You can look for specific kinds of log messages easily with Netmon's Event Log Explorer. You can choose any of these three options:

Browse by Client Using this option, you can browse log messages sorted by each SYSLOG client device.

Browse by Severity With this option, you browse SYSLOG data from any one of 8 different severity levels: INFO, DEBUG, NOTICE, WARNING, ERROR, ALERT, CRITICAL, EMERGENCY.

Browse by Facility This option allows you to search by a wide variety of message facilities, including: KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, FTP, NTP, LOGAUDIT, LOGALERT, and LOCAL0 through LOCAL7.

Monitoring Windows Event Logs

Netmon can monitor Event Logs on Windows systems, and collect these logs in the same way that SYSLOG messages are handled. The same alerting and reporting facilities are also available. A software agent is required to facilitate this task.

Considerations for Event Log Monitoring

SYSLOG is a 'push' oriented format, so most systems that support it are capable of sending log data to a monitoring system with a few small configuration changes.

Windows Event Logs, on the other hand, were not designed to be forwarded to other systems, but are instead are stored only locally in the file system. An agent is therefore required to retrieve these logs and perform the task of sending them to a remote system.

Using the SNARE Windows Agent

Netmon recommends (and distributes with all Netmon products on CD-ROM) the SNARE for Windows Agent, which gathers Event Log data and sends it in a SYSLOG-compatible format to your Netmon system.

The SNARE Windows Agent is highly respected open-source package, which has no licensing costs (so you can deploy it on as many systems as you desire) and is also supported by Netmon technical staff.

Netmon can provide you with a copy of SNARE Agent for Windows at no charge[14]. Contact technical support for more information.

Searching the Log Repository

Netmon provides several quick-search options in the **Event Log Explorer**, but there are times when you want to perform more finely-grained searches of your log repository.

Using the **Event Log Search** panel, located on the rightmost side of the Event Log console, you can search the log repository by any (or all) of the following parameters:

- A specific time range (to a granularity of 1 minute);
- A specific facility (or group of facilities);
- A specific severity (or group of severities);
- A specific host (or group of hosts);
- A specific text pattern (or regular expression pattern);

Configuring Log Alerts

Netmon can alert you when a particular type of log message is collected by the system. You can be notified when specific types, severities or payloads appear in a log entry. Netmon can even perform

[14] Per the License Agreement, we can also supply you with a copy of the source code.

sophisticated pattern matches on incoming log messages through built-in support for regular expressions[15].

To set up an Event Log Alert, take the following steps:

1. Click the **Manage Syslog Clients** link in the Event Log Explorer window.

2. Locate the client you wish to monitor for incoming alerts, and click the **Alerts** link next to it.

3. Choose the appropriate matches to associate with the incoming alert. In the **Text / Regex** field, you can enter a text string (for basic patter matches) or a regular expression (for advanced matching).

4. Click the **Add New Alert** button.

[15] Regular expressions are creating using a powerful expression language which is capable of performing very sophisticated text pattern search matching. A discussion of regular expressions is unfortunately outside the scope of this text. For an introduction to regular expressions, visit www.regular-expressions.info.

Monitoring Disks and Partitions

Netmon provides system administrators with the ability to monitor the amount of free space on network-connected disks and partitions. Netmon can keep track of disks on Windows® NT/2000/XP/2003 systems, as well as Unix or Unix-like hosts.

It can alert you when occupied space exceeds your defined threshold, and can also help you monitor volume growth over time, which helps in capacity planning. Custom alert thresholds and notification parameters can be set for each share, along with custom monitoring intervals and timeout periods.

How does Netmon monitor disks and partitions?

On Windows® NT-based systems, Netmon uses the Server Message Block (SMB) protocol to connect to your shared folders. The SMB protocol returns information to Netmon about the amount of free space on the disk.

On Linux and Unix type systems, Netmon uses the df utility to work with inetd or xinetd super servers. Netmon connects to the specified port number, parses the df output, and extracts the necessary disk information.

Monitoring Windows Volumes

Netmon can monitor public or administrative shares on Windows servers and workstations.

Adding a New Windows Share

To monitor Windows shared folders and drives, do the following:

1. If you have not already done so, create a shared folder on your Windows machine according to the security considerations listed below.

2. Open the Disk Trackers console by clicking on **Trackers > Disk Trackers**.

3. Click the **Add New Disk** button on the Disk monitoring panel, and choose Windows for disk type.

4. Fill in the following fields, and then click the **Add Disk** button:

Domain Name This is the name of the domain (or workgroup) to which the host belongs.

IP Address This is the IP address of the Windows host.

Username This is the login or account name which has permission to access the share.

Password This is the password for the account which has permission to access the share.

Share Name If you have entered a valid domain, IP address, username and password, this field will automatically display a list of available shares. If the information supplied is invalid, an error message will appear here.

Timeout Specify how long, in minutes, Netmon should spend trying to connect to the remote host. The default timeout period is 5 minutes, but this can be set to any interval you choose.

Interval Specify how frequently, in seconds, Netmon should check the remote share. The default interval is 300 seconds (5 minutes) but this can be set to any interval you choose.

Threshold When this percentage of space is exceeded, Netmon will trigger an alert. You can enter any value between 1 and 100.

Modifying Disk Parameters

To modify the monitoring parameters for a disk, take the following steps:

1. Open the Disk Trackers panel by clicking **Trackers > Disk Trackers**.
2. Click the **Edit** link next to the Disk you wish you modify.
3. Make the necessary adjustments to your Tracker parameters, and click the **Update Disk** button.

Removing a Monitored Disk

To remove a monitored disk, open the **Disk Trackers** panel, and click the **Delete** link next to it. You will be prompted to confirm deletion. If you're sure, click **OK** and the tracker will be deleted from your system.

Configuring Alerts for a Monitored Disk

To configure email and/or pager alerts for a disk, open the Disk Trackers panel, and click the **Alerts** link next to the desired Disk. This opens the Alerts window for that particular disk, where email / pager alerts can be added or removed from the disk.

Security Considerations for Monitoring Windows Shares

Monitoring a shared Windows® folder requires that Netmon log in to the remote system with a valid username and password.

Since the transmission of a non-encrypted user-name and password across the network is a security risk, use the following technique to ensure that Netmon can monitor remote Windows® shares safely:

1. Create a new, empty share on the drive or partition you wish to monitor, and set the access privileges for this share to read-only. Do not place any data in this folder.

2. Create a separate user account on the target machine with the minimum access privileges required to access the monitoring share.

Monitoring Linux and Unix Partitions

On Unix type systems, Netmon uses the df utility to work with inetd or xinetd super servers. Netmon connects to the specified port number, parses the df output, and extracts the necessary disk information.

Adding a New Unix Partition (inetd Method)

Use this method if your system uses inetd. Monitoring a Unix partition requires a minor change to two configuration files on the remote system. These files are called **/etc/services** and **/etc/inetd.conf**.

1. Insert the following line into /etc/services:

```
df 5001/tcp #DF
```

(We have specified port 5001 here, but you can actually choose any port number you wish. However, you'll have to remember to specify the same port number when adding this information to Netmon.)

2. Insert the following line into /etc/inetd.conf:

```
df stream tcp nowait root /usr/bin/df
```

3. Restart inetd with the following command:

```
killall – HUP inetd
```

Alternatively, you can use the following command:

```
kill-HUP <inetd PID>
```

4. Open the Disk Trackers panel, located in the Trackers console.

5. Click the Add New Disk button on the Disk Monitoring panel, and choose UNIX for disk type.

6. Fill in the following fields, then click the **Add Disk** button:

IP Address This is the IP address of the UNIX host.

Port Specify the port number to which NetMon must connect. This should be the same port number as entered in Step 1 above.

Partition Enter the device name of the partition (i.e. /dev/sda1 or /dev/hda1).

Timeout Specify how long, in minutes, NetMon should spend trying to connect to the remote host. The default timeout period is 5 minutes, but this can be set to any interval you choose.

Interval Specify how frequently, in seconds, NetMon should check the remote partition. The default interval is 300 seconds (5 minutes) but this can be set to any interval you choose.

Threshold When this amount of space is ex-ceeded, NetMon will trigger an alert. The default threshold is 90%, but this can be set to any amount you choose.

Adding a New UNIX Partition (xinetd Method)

Use this method if your system uses xinetd. Monitoring a Unix partition requires a minor change to two configuration files on the remote system. These files are called **/etc/services** and **/etc/inetd.conf**.

1. Insert the following line into /etc/services:

```
df      5001/tcp      #DF
```

(We have specified port 5001 here, but you can actually choose any port number you wish. However, you'll have to remember to specify the same port number when adding this information to Netmon.)

2. Create the 'df' script in **/etc/xinetd.d** with the following content:

```
service df
{
disable = no
flags = REUSE
socket_type = stream
wait = no
user = root
server = /bin/df
}
```

3. Restart xinetd with the following command:

```
killall – HUP inetd
```

Alternatively, you can use the following command:

```
kill-HUP <inetd PID>
```

4. Open the **Disk Trackers** panel, located in the **Trackers** console.

5. Click the **Add New Disk** button on the Disk Monitoring panel, and choose UNIX for disk type.

6. Fill in the following fields, then click the **Add Disk** button:

IP Address This is the IP address of the UNIX host.

Port Specify the port number to which Netmon must connect. This should be the same port number as entered in Step 1 above.

Partition Enter the device name of the partition (i.e. /dev/sda1 or /dev/hda1).

Timeout Specify how long, in minutes, Netmon should spend trying to connect to the remote host. The default timeout period is 5 minutes, but this can be set to any interval you choose.

Interval Specify how frequently, in seconds, Netmon should check the remote partition. The default interval is 300 seconds (5 minutes) but this can be set to any interval you choose.

Threshold When this amount of space is exceeded, Netmon will trigger an alert. The default threshold is 90%, but this can be set to any amount you choose.

Modifying Disk Parameters

To modify the monitoring parameters for a disk, take the following steps:

1. Open the Disk Trackers panel by clicking **Trackers > Disk Trackers**.
2. Click the **Edit** link next to the Disk you wish you modify.
3. Make the necessary adjustments to your Tracker parameters, and click the **Update Disk** button.

Removing a Monitored Disk

To remove a monitored disk, open the **Disk Trackers** panel, and click the **Delete** link next to it. You will be prompted to confirm deletion. If you're sure, click **OK** and the tracker will be deleted from your system.

Configuring Email or Pager Alerts for a Monitored Disk

To configure email and/or pager alerts for a disk, open the Disk Monitoring panel, and enter the IP address of the device.

Click the **Alerts** link next to the disk which is to be configured with alerts. This opens the Alerts window for that particular disk, where email / pager alerts can be added or removed from the disk.

Monitoring Websites and Web Applications

Netmon can monitor websites and web applications by analyzing the results of an HTTP request. You can use this service to monitor your corporate website, company intranet, or any other web-based system.

Introducing the URL Tracking Service

Netmon requests a user-specified URL at user-configurable intervals. It receives the resulting HTML web page (or XML, or any other HTTP payload) and inspects the contents for a user-specified text pattern.

If Netmon finds a matching copy of the text pattern or phrase in the response, it assumes the website (or web application) is functioning normally. If Netmon does not find a matching string in the response content, it can be configured to queue an alert message.

Creating a New URL Tracker

To create a new URL Tracker, take the following steps.

1. Click the Trackers button in the top toolbar, followed by the URL Trackers button.
2. Click the **Add New URL Tracker** button.
3. Specify the desired URL in the URL text box. If you wish to include additional GET parameters, append them to the end of the URL in the usual querystring format (i.e. http://www.someweb.com/somescript.php?var1=true&var2=text)
4. Specify a text Pattern to use when matching the incoming HTTP response. You can specify a simple text string, or use a Regular Expression (PCRE) for more sophisticated matching capabilities.
5. Choose a monitoring interval, in seconds. In most cases, the 5 minute (300 second) interval is suitable.
6. Click the **Create Tracker** button.

Attaching Alerts to a URL Tracker

Netmon can alert you by email or pager when it detects an invalid response from your website(s) or web application(s). To attach an email or pager alert recipient to an URL Tracker, take the following steps:

1. Click the **Trackers** button in the top toolbar, followed by the **URL Trackers** button.
2. Locate the URL Tracker you wish to attach an alert to, and click the **Alerts** link next to it.
3. Assign the alert a Label, if desired. This step is optional.
4. Specify a Netmon user account to be the alert recipient.
5. Specify the **Alert Media** to be used (email or pager).
6. Specify one or more **Alert Command**(s) to associate with the alert condition, if desired and if available.
7. Click the **Add Alert** button.

Modifying a URL Tracker

To modify an existing URL Tracker, take the following steps:

1. Locate the URL Tracker in the URL Tracker Explorer, and click the **Edit** link next to it.
2. Make the desired changes to the URL Tracker paramters.
3. Click the **Update Tracker** button.

Removing a URL Tracker

To remove an existing URL Tracker, take the following steps:

1. Locate the URL Tracker in the URL Tracker Explorer, and click the **Del** link next to it.
2. You will be prompted to confirm deletion. If you are sure, click **OK**.
3. The URL Tracker will be deleted.

Netmon Reports

To access the Netmon Reports console, click the **Reports** button in the top toolbar. Netmon ships with selection of built-in reports, which can be customized and saved depending on your needs.

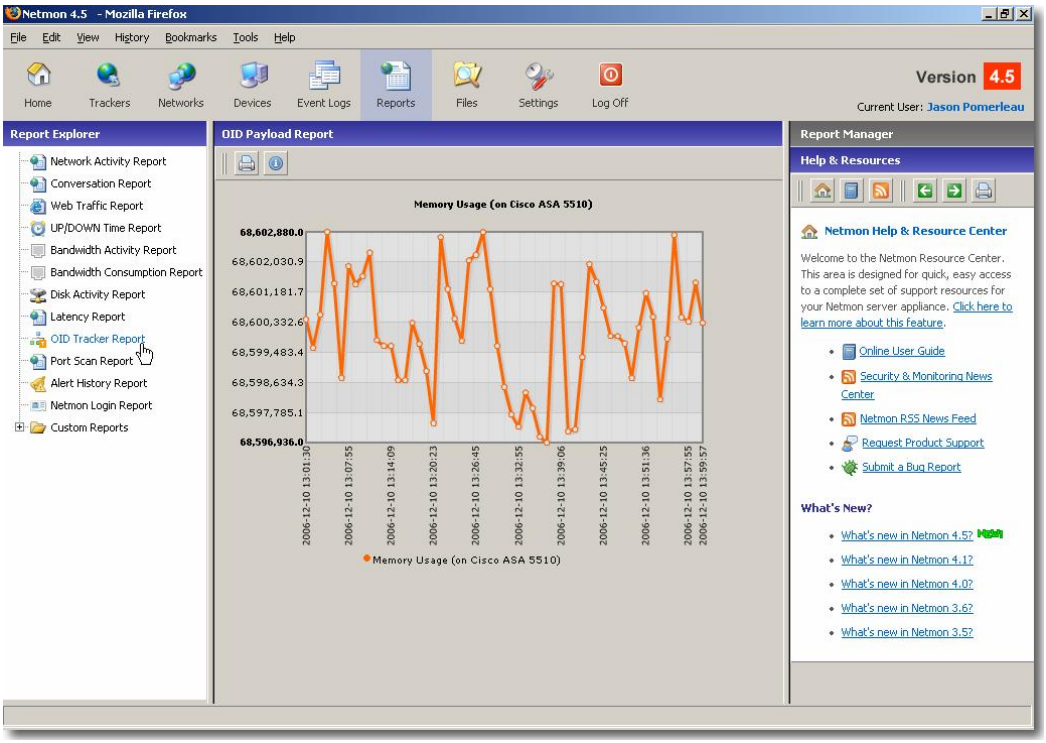


Figure 12 – Sample Netmon Report

Creating and Saving Custom Reports

You can save any of Netmon's core reports as a custom report, for later retrieval.

To save a report, simply provide a friendly Report Name in the text box which appears under the **Run Report Now** button in the Report Builder panel. Then, click the **Save Report Now** button to save the parameters you have entered.

When saving a report, Netmon retains all of the information you enter. You may then edit the report at any time by clicking on the "Saved & Scheduled Reports" entry in the "Report Explorer" tree of the "Reports" section, and clicking on the report you just saved.

Report Scheduling & Background Reports

As of Netmon 4.6, it is possible for you to schedule daily, weekly, monthly and yearly reports in Netmon. Once a report has been completed, Netmon will send you a notification email informing you of the time it took to generate the report and how to access the generated report.

Scheduling a report is a simple procedure and you can always go back and change the scheduling behaviour of a particular report.

In order to schedule a report, load the report builder for the report you would like to schedule by clicking on the report name in the "Report Explorer" tree of the "Reports" section. Once the report builder has been loaded in your browser, follow the following instructions to schedule your report:

1. Enter the appropriate selections in the report builder for the report you would like to run.

   Note: It usually makes a lot of sense to select a 'relative' reporting period, such as 'yesterday', 'today', rather than a custom date/time range, as the relative periods will always be based on when the report is being executed.

2. Enter a short descriptive name for your report in the "Saved Report Name" field of the builder.

3. Check the "Schedule This Report to Run Automatically" checkbox in the report builder. A new section will be appended to the builder.

4. Select the time-of-day at which the report should be executed in the "Start Time" drop-down (default: 12:00 AM)

5. Select the scheduling frequency. Available options are Daily, Weekly, Monthly or Yearly.

   - If you selected Weekly, the builder will now ask you for the weekday that should be used for scheduling.
   - If you selected Monthly, the builder will now ask you for the day of the month to use for scheduling.
   - If you selected Yearly, the builder will now ask you for the day of the year to schedule the report.

6. Select the user account that should receive email notifications when the report has been completed in the "Notify on Completion" drop-down entry.

Click on the **Save Report Now** button above the scheduling portion of the builder.

Your report has now been scheduled and saved. You may edit the report or scheduling settings at any time by clicking on the "Completed Reports" entry in the "Report Explorer" tree and clicking on the name you just entered while scheduling your report.

What are Background / Asynchronous Reports?

As of version 4.6, Netmon allows you to trigger a report to run immediately in the background, allowing you to continue using the web interface to run other reports or monitor the status of your network.
In order to run a background report, simply enter the required information in the report builder if your choice, and check the "Run Asynchronously" checkbox in the builder.

The Report Builder will display a new text-box titled "Filename", with a randomly selected default name pre-filled in the box. You may change this file-name if you wish to use a specific name for your report output, and proceed to click on the "Run Report Now" button.

At this point, instead of making you wait while Netmon is generating your report, Netmon will simply display a confirmation message indicating that the report is currently running and that it will be available in the "Completed Reports" entry in the "Reports" section once the report has completed.

Network Activity Report

The Network Activity Report allows you to query Netmon's network traffic database for any type of activity, for any host.

To run a Network Activity Report, simply click the **Network Activity Report** icon in the Netmon Report Explorer, and take the following steps:

1. Choose a source interface from the available drop-down box. You can select Netmon's built-in Local IP Packet Analyzer, or any NetFlow-enabled interface.

2. Choose a host (or group of hosts) to include in your query, and make the selection in the Host Selection: selection boxes . You can run a Network Activity report against All Hosts in the database, or you can narrow your search by applying a host filter or specifying an individual host to scan. You can even look for hosts which have a specific text pattern in their DNS names.

3. Choose the type of TCP/IP traffic to scan. You can scan for All Activity, or you can narrow your search by applying a traffic filter, or specifying an individual protocol/port combination.

4. Specify how many records to return and how to order the results by selecting the appropriate entries in the "Limit Results" and "Order Results By" drop-down entries.

5. Finally, select a reporting period. Available choices are *Last Hour*, *Custom Range*, *Today*, *This Week*, *This Month*, *Last Week*, and *Last Month*. If you decide to select the "Custom Range" entry, you will need to enter a valid date and time range by selecting the dates in the calendars, and the time of days to report against in drop-down entries.

6. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the Network Activity Report window.

Conversation Report

The Conversation Report allows you to examine network activity between two hosts, or two groups of hosts.

To run a Conversation Report, simply click the Conversation Report icon in the Netmon Report Explorer, and take the following steps:

1. Choose a source host (or group of hosts) to include in your query, and make the selection in the Source Host(s): selection boxes . You can run a Conversation Report against All Hosts in the database, or you can narrow your search by applying a host filter or specifying an individual source host.

2. Choose a destination host (or group of hosts) to include in your query, and make the selection in the Destination Host(s): selection boxes . You can run a Conversation report against All Hosts in the database, or you can narrow your search by applying a host filter or specifying an individual destination host to scan.

3. Choose a reporting period. Available choices are Today, Yesterday, Last 7 Days and Custom. If you choose Custom, you will need to enter a valid date and time range.

4. Choose the type of TCP/IP traffic to scan. You can scan for All Activity, or you can narrow your search by applying a traffic filter, or specifying an individual protocol/port combination.

5. Finally, you can limit your result set and choose the ordering of the information with the Limit Results To: and Order Results By: selection boxes.

6. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the Conversation Report window.

Web Traffic Report

The Web Traffic Report allows you to query Netmon's HTTP Request Plugin, which keeps track of URLs which have been requested from your network.

To run a Web Traffic Report, simply click the **Web Traffic Report** icon in the Netmon Report Explorer, and take the following steps:

1. Choose a host (or group of hosts) to include in your query, and make the selection in the Hosts: selection boxes. You can run a Web Traffic report against All Hosts in the database, or you can narrow your search by applying a host filter or specifying an individual host to scan.

2. Choose a reporting period. Available choices are Today, Yesterday, Last 7 Days and Custom. If you choose Custom, you will need to enter a valid date and time range.

3. Enter a keyword or partial text string to narrow your search, if desired. This field is optional.

4. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the Web Traffic Report window.

UP / DOWN Time Report

This report provides a summary of the availability of each of your monitored services and disks, for the time interval specified.

To run an UP/DOWN Time Report, simply click the **UP/DOWN Time Report** icon in the Netmon Report Explorer, and take the following steps:

1. Choose a reporting period. Available choices are Today, Yesterday, Last 7 Days and Custom. If you choose Custom, you will need to enter a valid date and time range.

2. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the UP/DOWN Report window.

Bandwidth Activity Report

A Bandwidth Activity Report plots bandwidth utilization for SNMP device interfaces (such as those found on routers, firewalls, switches and servers) for a given time interval.

Note You can only run a Bandwidth Activity Report if you have enabled historical logging for an interface.

To run a Bandwidth Activity Report, simply click the **Bandwidth Activity Report** icon in the Netmon Report Explorer, and take the following steps:

1. Choose a device from the SNMP Device drop-down menu.
2. Choose an interface for the selected device from the Interface drop-down menu.
3. Choose a reporting period. Available choices are Today, Yesterday, Last 7 Days and Custom. If you choose Custom, you will need to enter a valid date and time range.
4. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the Bandwidth Activity Report window.

Bandwidth Consumption Report

The Bandwidth Consumption Report allows you to measure total network activity for particular subnet(s) or IP range(s). This report is useful to identify the largest bandwidth consumers (and providers) on a particular monitored network. Before you run a Bandwidth Consumption Report, familiarize yourself with the following report parameters:

Source Network(s) This is the subnet or IP range you wish to measure. Every IP address in the selected range will be accounted for in the resulting report (assuming there is network activity for that address).

Network(s) to Exclude Any activity between the source network(s) and the network(s) specified here is excluded from the reporting result. This feature is useful, for example, if you want to measure Internet-

bound bandwidth for a subnet, while filtering out any local activities (i.e. activity which is switched internally, inside the network border). Or, you may wish to filter out traffic which is destined to a particular branch office.

Traffic Filter You can use traffic filters to limit the report result to a specific protocol or group of protocols by making a selection here. The default selection includes all network activity, regardless of protocol.

Order Results By You choose to produce a report for each individual IP address selected as Source Network(s), or you can produce a report which summarizes the data for each network subnet/range.

Running a Bandwidth Consumption Report

To run a Bandwidth Consumption Report, click the Bandwidth Consumption Report icon in the Netmon Report Explorer, and take the following steps:

1. Choose Source Network(s) from the available drop-down selection.
2. Choose Network(s) to Exclude from the available drop-down selection.
3. Select a reporting period. You can choose from any one of several pre-defined values, or specify a custom time interval by choosing the Custom option.
4. Choose a Traffic Filter, if desired, to limit the protocols which are included in the reporting results.
5. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the Bandwidth Consumption Report window.

Disk Activity Report

The Disk Activity Report allows you to plot disk utilization over a specified time interval.

To run a Disk Activity Report, simply click the **Disk Activity Report** icon in the Netmon Report Explorer, and take the following steps:

1. Choose a disk, share or partition to include in your query, and make the selection in the Disk/Share/Partition selection box.

2. Choose a reporting period. Available choices are Today, Yesterday, Last 7 Days and Custom. If you choose Custom, you will need to enter a valid date and time range.

3. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the Disk Activity Report window.

Latency Report

The Latency Report analyzes all of the TCP Service Trackers, PING Service Trackers and Disks which have been configured in the Netmon Trackers console, and provides an average latency (in milliseconds) for each service, for the time interval specified.

Please note that in order to run a Latency Report for a specific device/service, you first need to enable full historical logging for that device/service. By default, Netmon does not keep historical data for devices or services, for performance reasons.

To run a Latency Report, simply click the Latency Report icon in the Netmon Report Explorer, and take the following steps:

1. Choose a reporting period. Available choices are Today, Yesterday, Last 7 Days and Custom. If you choose Custom, you will need to enter a valid date and time range.

2. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the Latency Report window.

OID Tracker Report

An OID Tracker Report allows you to examine historical values for any SNMP management object (OID) through Netmon's OID Tracker Service. Though this is a very simple report, it is extremely flexible and useful for a variety of tasks.

Note: In order to run a report for any OID Tracker, you must first ensure that the Enable Logging selection has been checked in the OID Tracker Manager.

To run an OID Tracker Report, take the following steps:

1. Choose **OID Tracker Report** from the **Reports Explorer**.
2. Select a Device from the available list. (If no Devices are visible, see Note above)
3. Choose an OID Tracker from the available list.
4. Choose a reporting period. Available choices are Today, Yesterday, Last 7 Days and Custom. If you choose Custom, you will need to enter a valid date and time range.
5. If desired, check the Delta Report option by clicking the checkbox. When this option is checked, Netmon plots the rate of change of the management object over the desired time interval, as opposed to absolute values.
6. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the OID Tracker Report window.

URL Tracker Report

A URL Tracker Report allows you to evaluate the performance of websites and web applications. You can monitor the performance (latency) of URL request delivery, as well as accuracy (expected results returned) through the same report.

Note: In order to run a report for any URL Tracker, you must first ensure that the Enable Logging selection has been checked in the URL Tracker Manager.

To run a URL Tracker Report, take the following steps:

1. Choose **URL Tracker Report** from the **Reports Explorer**.
2. Select a URL from the available list. (If no URLs are visible, see Note above)

3. Choose a reporting period. Available choices are Today, Yesterday, Last 7 Days and Custom. If you choose Custom, you will need to enter a valid date and time range.

4. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the URL Tracker Report window.

Port Scan Report

A Port Scan Report summarized the results of Netmon's background port scanning service, which probes hosts on your various network range(s) for open ports.

Netmon scans each host on your network range(s) every 2 hours, and records the results of its scan to the database. A port scan report shows all scanned hosts, along with the open ports for each host.

To get more detail on a particular port/protocol, just click on it.

Configuring Network Service Alerts

Netmon can notify you when it detects a new network service (i.e. open port) that was not identified on a previous scan. To configure alerting options for this service, click the **Configure Alerts button** at the top of the Port Scan Report output window.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the Port Scan Report window.

Alert History Report

The Alert History Report displays a list of all email and pager alerts which have been generated across the entire Netmon system for the specified period of time.

To run an Alert History Report, simply click the **Alert History Report** link in the **Netmon Report Explorer**, and take the following steps:

1. Choose a reporting period. Available choices are Today, Yesterday, Last 7 Days and Custom. If you choose Custom, you will need to enter a date and time range.

2. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the Alert History Report window.

Netmon Login Report

The Netmon Login Report displays a list of all Netmon login activity for the specified period of time.

To run a Netmon Login Report, simply click the **Netmon Login Report** icon in the Netmon **Report Explorer**, and take the following steps:

1. Choose a reporting period. Available choices are Today, Yesterday, Last 7 Days and Custom. If you choose Custom, you will need to enter a valid date and time range.

2. Click the **Generate Report** button.

Panel Actions

 Print an instant printer-friendly report by clicking this button in the Netmon Login Report window.

File Management

The Netmon Files Manager console provides a central location for managing various kinds of files, including data backups, traffic captures, proprietary SNMP MIBs and more. Here, you can view, download or delete files as needed.

To use the files manager, simply click the **Files** button in the top toolbar, and then make the appropriate selection from the Folder Explorer on the left side of the window.

Managing the Backups Folder

The Backups folder contains your Netmon data backups as well as various system-level backup files (including package repositories). This is the location where you can view, download or delete these items, by clicking the appropriate link next to each item.

If you see a  icon next to any file, it means that Netmon does not recognize the file type. The default action for these file types is **Download**.

Managing the Enterprise MIBs Folder

The Enterprise MIB folder contains proprietary, enterprise-specific MIB files which have been uploaded through Netmon's Custom MIBs feature[16]. You can view these files, download them, or print them.

If you see a  icon next to any file, it means that Netmon does not recognize the file type. The default action for these file types is **Download**.

Managing Netmon Log Files

The Netmon Logs folder contains logging output for each of Netmon's background services, such as the IP Protocol Analyzer or Syslog Server. You may be directed to review these logs, or send them via email to Netmon Technical Support personnel.

The size and contents of these log files depends on the level of logging verbosity you have specified in **Settings** > **Netmon Services**.

If you see a  icon next to any file, it means that Netmon does not recognize the file type. The default action for these file types is **Download**.

[16] See *Managing Custom SNMP MIBs* on page 50 for more information.

Managing Traffic Capture Files

The Netmon Traffic Captures folder contains .cap files which have been created using Netmon's low level packet capture utility. These files are prepared in a format which can be read and understood by Ethereal / Wireshark client software.

Traffic capture files need to be downloaded to your local system for analysis. They cannot be used from within Netmon itself.

If you see a  icon next to any file, it means that Netmon does not recognize the file type. The default action for these file types is **Download**.

Administration and Management

Using the Settings Console

The Netmon Settings console is where most administrative tasks are performed. To open this console, click the Settings button in Netmon's main toolbar, and choose from a number of maintenance and administrative snap-ins, including:

- Basic Setup Tasks
- Define Alert Conditionals
- Customize Alert Templates and Alert Commands
- Use Data Management Tools which can help you perform data backups
- Manage Traffic and Host Filters
- Manage Netmon's Host Name Database
- Define Local Networks for reporting and display purposes
- Manage Netmon System Services
- Manage the Port Label Database
- Manage Netmon User Accounts

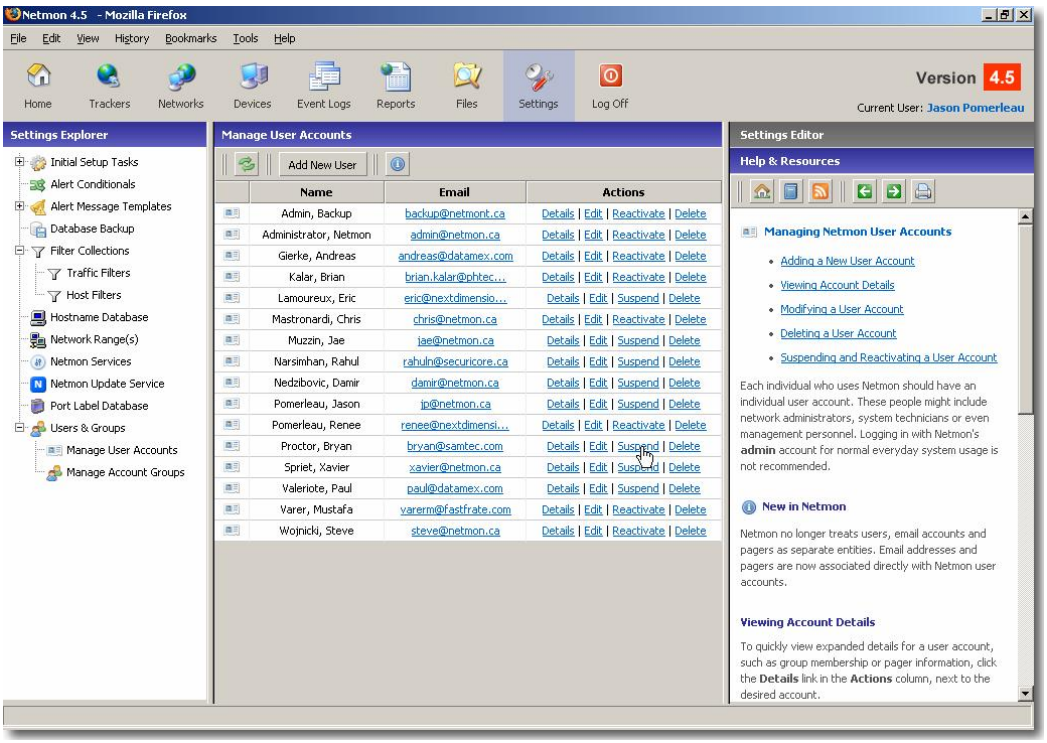


Figure 13 – Netmon Settings Console

Managing Alert Conditionals

What is an Alert Conditional?

An Alert Conditional provides fault tolerance for false alert situations. Imagine what might happen if the Netmon server itself were to become disconnected from the rest of the network. Since it would be unable to reach any of the services and devices it is monitoring, it might (incorrectly) assume that all of those services and devices were down - and trigger the appropriate email and pager alerts. Nobody wants to receive an avalanche of alert emails and/or pager beeps.

False alerts can be prevented with the use of a Conditional, which is simply an IP address that Netmon checks in order to ensure that an alert situation is genuine.

If the IP address specified in the Conditional is determined to be alive (through a simple ICMP PING/echo request) Netmon knows that the alert situation is real. On the other hand, if the IP address specified in your Conditional is unresponsive, Netmon withholds the alert, since this would indicate that Netmon itself had a connectivity problem.

Are Conditionals Mandatory?

No. Conditionals are optional, and you do not have to specify any. Their use is recommended only to prevent unwanted false alarm situations.

Using Conditionals Effectively

In most cases, you only need to set up two conditionals: one which tests internal connectivity (such as the IP address of a domain controller or other high-uptime device) and another which tests external connectivity. For external connectivity tests, choose the IP address of a highly-available web destination (such as Google.com).

Adding an Alert Conditional

To add a new conditional, select **Alert Conditionals** from the **Settings Explorer**, and click the **Add New Conditional** button. A dialog window opens in the **Settings Editor** panel on the right side of the screen.

Enter the IP address of the conditional in the IP Address, and specify a friendly name in the Conditional Name field. To add this conditional to the database, press the **Add Conditional** button when you have finished entering the preceding information.

Removing an Alert Conditional

To remove an alert conditional from Netmon's database, select **Alert Conditionals** from the **Settings Explorer,** and click the **Delete** link next to the conditional you wish to remove. You'll be prompted to confirm your decision: click **OK** to proceed with removal of the selected conditional, or **Cancel** to abort the operation.

If you remove a conditional, you will also remove that conditional from any previously configured alerts. Other previously configured conditionals for existing alerts will remain unchanged.

Managing User Accounts

Each individual who uses Netmon should have an individual user account. These people might include network administrators, system technicians or even management / administrative personnel. Logging in with Netmon's admin account for normal everyday system usage is not recommended.

Viewing Account Details

To quickly view expanded details for a user account, such as group membership or pager information, click the **Details** link in the **Actions** column, next to the desired account.

Adding a New User Account

To add a new user account, click the **Add New User** button in the middle panel. This will cause the **Settings Editor** panel to open on the right side of the screen, displaying a form for the entry of new user information. To read more about each of these , see Editing User Account Properties.

Modifying a User Account

To update group membership, an email address or other user details, click the **Edit** link in the **Actions** column next to the account to be modified.

Deleting a User Account

To remove a Netmon user account, simply click the **Delete** link in the **Actions** column next to the account to be deleted. You'll be asked to confirm if this is what you really want to do. If you confirm, the selected user account will be removed from the system, and logins under that account will no longer be permitted.

Suspending a User Account

Suspending a user account has almost the same effect as deleting the account: future logins for that account are disabled. However, when you suspend a user account, you have the later option to re-

activate it. This can be a useful option in cases where access should be temporarily disabled, but not permanently revoked. For example, you may wish to temporarily disable the user accounts of technicians or administrators who are away on vacation.

To suspend an active account, click **Suspend** in the **Actions** column. To reactivate an account which has been previously suspended, click **Reactivate** in the **Actions** column.

Managing Account Groups

Account groups allow you to logically group individual Netmon user accounts, and bind them to a specific set of permissions that is common between them. For example, you may want to prevent network technicians from deleting data or making changes to Netmon's configuration, while providing senior administrators with more control.

Netmon ships with four built-in account groups. You can modify the individual permission settings in each of these groups, create your own groups, or even remove groups that are not required in your environment.

Administrators By default, this group has full control over the Netmon software application. It is strongly recommended that you do not change the permission structure of this group, nor should it be removed.

Backup Users This group is only permitted to perform backup operations, such as configuration backups, database compact operations, and complete data backups.

Standard Users This is the 'normal' account group that should be used for most of your Netmon user accounts. It grants access to the entire Netmon application, but prevents members from deleting data or performing administration functions.

Report Users By default, this group has read-only access to the entire Netmon application, but is prevented from altering data or performing system administration or maintenance functions. You can customize the individual permissions in this group to allow/disallow access to specific areas of Netmon.

Understanding Permission Inheritance

A user account can belong to one or more groups. When a user account belongs to two groups or more, the user inherits all available permissions from both groups.

Group A has permissions X and Y. Group B has permissions Z. A user who is a member of both groups inherits permissions X, Y and Z.

Viewing Group Details

To quickly view expanded details for an account group, click the **Details** link in the **Actions** column, next to the desired group.

Adding a New Group

To add a new user account, click the **Add New Group** button in the middle panel. This will cause the **Settings Editor** panel to open on the right side of the screen, displaying a form for the entry of new group information. To read more about each of these, see Editing Group Properties.

Modifying a Group

To update permission assignments for an existing group, click the **Edit** link in the **Actions** column next to the group to be modified. Check/uncheck the desired values, and click the **Update** button in the Settings Editor panel.

Deleting a Group

To remove a Netmon account group, simply click the **Delete** link in the **Actions** column next to the group to be deleted. You'll be asked to confirm if this is what you really want to do. If you confirm, the selected group will be removed from the system.

You should not remove the Administrators group, nor should you delete all groups. Doing so could result in an unexpected lockout from administrative functions.

Managing Alert Message Templates

Netmon allows you to customize the alert messages which are sent from various monitoring facilities through the use of simple templates. Simply navigate to **Settings** > **Alert Message Templates**, and expand the tree to see a complete list of available templates.

Customizing an Alert Message Template

To customize any template, select it from the available list in the **Settings Explorer**. An editing window will appear, showing the current alert text.

In any alert message, special information is inserted (such as the name and IP address of a service which has failed, for example) via specially tagged keys into the template. These keys look like **{$host}** or **{$ip_address}**, and they help Netmon to understand where to place important alert information.

You can insert these tags anywhere in your template using the specially provided buttons. Simply position the cursor where you'd like to place the data, and then click the desired button on the right side of the editing window. You can also use standard cut & paste tools to move tags around your message.

You must click the **Save Template** button to permanently commit any changes you make to a template.

Restoring Default Templates

To restore any template to its factory default settings, select it from the template list, and click the **Restore Default Template** button. The window contents will be immediately populated with the factory default alert message for that particular alert. You must then click the **Save Template** button to commit any changes to Netmon's database.

Managing Alert Response Commands

Netmon can run special scripts or commands in response to an alert event. For example, you may wish to run a port scan against a newly-discovered host, or receive a list of large files when a disk capacity alert is issued. Using this facility, you can also issue a restart to an unresponsive Windows service.

Alert commands are associated with alert events, and they are managed on the same screen as alert templates (see above). Once a command has been associated to a particular alert event, you then have the option to run that command for any alerts of that type.

Note that alert commands do not run automatically in response to alert events. You must still associate any desired commands you wish to run with each new alert you create. This area simply allows you configure which commands *are available* for a specified alert type.

Creating a New Alert Command

To create a new alert command, take the following steps:

1. Click **Settings > Alert Message Templates** and locate the alert condition to which you wish to attach a new command.
2. Fill out the appropriate fields (outlined below) and click the **Create Command** button.

Label A friendly name or label for this command.

Command The actual command syntax. The text specified here is run as a shell command on the Netmon server. You can use the **Insert Variable** buttons on the top of the Alert Template window to insert dynamically changing values (i.e. the device IP address, hostname, etc.) into your command string. Netmon will substitute these values for each individual alert.

Timeout The number of seconds Netmon should wait to run the command before giving up.

Process Asynchronously / Add Output To Alert You can choose to process the command before the alert message is sent by selecting the *Add Output to Alert* radio box. In this case, Netmon will append the results of the command to the alert message you receive. Alternatively, you can run the command separately from the alert message by selecting the *Process Asynchronously* radio box, so that the command and alert message are both processed separately from one another.

Modifying an Existing Alert Command

Any existing commands will be listed in the Alert Template editing window. To modify an existing command, simply click the **Edit** link next to it. Make any necessary adjustments, and then click the **Update Command** button.

Removing an Alert Command

To remove a command from the available selections, simply click the **Del** link next to it. You'll be prompted to confirm deletion. Once a command has been deleted from this area, any existing alerts which may have called that command will continue to function, however, they will no longer run that command.

Managing Host Names

Using this console, you can manage Netmon's name database, which contains a variety of NetBIOS, DNS and user-defined host names. Each of these host names maps to an IP address, and often many different host names map to the same IP address. This console allows you to manage names for any host (and even to include your own user-defined labels) as well as search Netmon's database for host names which match a particular search criteria.

Searching for Hostnames

To search Netmon's name database, enter a search string in the Search Text/IP Address: box on the Hostname Management console. (For example, to search for all hostnames which contain the text "google", simply enter google into the Search Text/IP Address: box) Then click the **Search** button.

If you wish, you can customize your search, to NetBIOS names only, DNS names only, HTTP Requests only, or user-defined names only.

Removing a Host Name

In some cases, a host name may no longer be accurate or relevant. In these cases, you'll want to trim Netmon's name database by deleting inaccurate or outdated names.

To delete any name, simply click the **Delete** link in the **Actions** column beside the particular name which you wish to remove. You'll be prompted to confirm that you really do wish to delete this name from the database. If you're certain, click the **OK** button to proceed, and Netmon will remove the name from its database.

Adding a User Defined Host Name

You can apply your own friendly host name to any IP address. Click the **Add New Host** button in the Manage Hostname Database panel. An editing window will open in the **Settings Editor** panel on the right side of the screen.

Enter the IP address and label, and then click the **Add Hostname** button. Your IP address will now appear as your friendly label throughout the Netmon application.

Managing Filter Collections

One of the most powerful features in Netmon is the use of filters. Filters allow you to look for specific kinds of traffic, or narrow your view to a certain set of IP addresses - or both! You can use filters in the Visual Network Explorer (VNE) and they can also be used when creating reports. Netmon uses two kinds of filters:

Traffic Filters

Traffic filters allow you to refine your view (or a report) to look for specific TCP or UDP ports or protocols. You can look for an individual protocol/port combination (i.e. UDP 514) or you can include a wide range of different ports into a single filter.

Netmon ships with a series of built-in traffic filters, but you can also create your own traffic filters in the **Settings > Filter Collections > Traffic Filters** console.

Host Filters

Host filters permit you to create logical groups of hosts, and narrow your search to a specific IP address, or a group of related IP addresses. You can assign a friendly name to this group.

Netmon does not ship with any predefined host filters, as these are dependent on the IP addresses which are important to you. You can create your own host filters in the **Settings > Filter Collections > Host Filters** console.

Managing Network Ranges

For reporting and automatic discovery services, Netmon needs to know the IP range(s) that belong to you. In many cases, your network range(s) will be LAN addresses which use non-routable IP ranges (such as 192.168.xxx.xxx or 10.xxx.xxx.xxx) - however this does not necessarily have to be the case. (When monitoring a WAN, for example, remote IP ranges could be listed here).

Each range should consist of a block of addresses, such as:

* 10.10.1.1 to 10.10.1.255 or
* 10.10.2.1 to 10.10.3.100

Adding a New Network Range

To add a new IP range to Netmon's database, press the Add New Network Range button, which makes an editing window visible. Enter the following values in the boxes provided:

Starting Address The starting IP address of a contiguous block.

Ending Address The ending IP address of a contiguous block.

Enable SNMP AutoDiscovery A checkbox indicating whether Netmon should attempt to scan this range for SNMP-capable devices. If you do not want Netmon to perform automatic device discovery on this range, uncheck this box.

Enable Background Port Scans A checkbox indicating whether Netmon should attempt to perform background port scans against devices in this range. If you do not want Netmon to perform automatic port scans on this range, uncheck this box.

Once the correct information has been entered, press the **Add Network** button.

Modifying an IP Range

To make changes to an existing IP Range, locate it in the **Manage Network Range(s)** panel, and click the **Edit** link next to the range you wish to modify.

Make the necessary changes to your IP Range in the **Settings Editor** window, and then click the **Update Network Range** button.

Removing an IP Range from the Database

To remove an IP range from the Netmon database, simply locate it in the **Manage Network Range(s)** panel, and click the **Delete** link next to the range you wish to delete.

Using the Netmon Update Service

The Netmon Update Service is a background service that checks for new patches or updates for your Netmon product automatically, every 24 hours. This service is capable of updating any component of your Netmon system, including:

- Operating System / Security Updates
- Background Services / Netmon Engine
- Application / Middleware
- User Interface and Documentation

The Netmon Update Service uses the RSYNC protocol to communicate with the update server at Netmon headquarters. It therefore requires your Netmon server appliance to establish outbound connections on TCP Port 873. If your firewall rules do not permit this type of connection, you'll need to install updates manually from CD-ROM.

Checking for Updates Manually

You can also force Netmon to check for new updates anytime outside of its normal 24 hour interval. For example, you may be instructed by Netmon Technical Support personnel to request an update, or you may wish to apply a new update ahead of schedule. To manually trigger an update request, take the following steps:

1. Click the **Settings** button in the top toolbar.
2. Choose **Netmon Update Service** from the Settings Explorer tree.
3. Click the **Check for New Updates Now** button.

Installing Updates from CD-ROM

If your network does not permit outbound connections on TCP Port 873, you will need to apply patches and updates manually from a CD-ROM image, which is available at the following location:

Link: http://www.netmon.ca/support/downloads/

Managing the Port Label Database

When Netmon recognizes a particular port (i.e. TCP port 80) it applies a friendly label (i.e. HTTP) from this table. Netmon ships with nearly 2,000 built-in port labels.

To manage the port label database, click **Settings > Port Label Database**.

Adding a New Port Label

To add a new port label to Netmon's database, press the **Add New Port Label** button, which makes an editing window visible. Enter the following values in the boxes provided:

Transport Layer Choose between TCP and UDP.

Port Number Provide a valid port number, from 1 to 65535.

Label Enter a brief (36 character maximum) friendly label to apply to this protocol/port combination.

Once the correct information has been entered, press the **Create Port Label** button.

Modifying a Port Label

To change an existing port label, click the **Edit** link next to the label you wish to modify. An edit window will appear in the **Settings Editor** on the right side of the screen. Made the desired changes to the transport protocol, port number or label, and click the **Update Port Label** button to save your changes.

Removing a Port Label from the Database

To remove a port label from the Netmon database, simply click the **Delete** link next to the particular label you wish to delete. You'll be prompted to confirm each delete operation.

Built-In Protocol Dictionary

If an entry for a particular protocol exists in Netmon's protocol dictionary, Netmon displays it when you click the protocol's friendly label. If Netmon does not recognize the protocol, a generalized entry is displayed.

Managing Netmon System Services

Netmon uses a variety of background services (known as 'daemons' in the UNIX world) to perform its many monitoring tasks. The Netmon Services Manager lets you monitor and manage each of these services for your Netmon server appliance.

Starting and Stopping Services

Each of Netmon's background services can be started or stopped using this console. Under normal operating conditions, it is generally not be necessary to start or stop any of these services. However, if you wish to customize various services for different deployment scenarios, or if your Netmon server appliance is behaving unexpectedly, this panel can be a quick way to tell if Netmon's core services are alive and running.

Services that are running are denoted with a  icon, and services which are off have a  icon.

To change the start/stop status of any service, simply click the **Start Service** or **Stop Service** button next to the service you wish to modify. Note that changes made in this panel are not preserved after reboot, so they will need to be made again if you need to restart your Netmon server appliance.

Overview of Individual Services

ARP Probe Service Analyzes ARP packets and records MAC/IP pairs. This service is used to support new host detection in the Recently Discovered Hosts panel, on the Netmon Home Dashboard.

Background Port Scanning Service With this service enabled, Netmon performs regular port scans all of the IP address ranges defined in your Local Network range(s).

Email Alert Service This service supports the forwarding of email alerts to your mail server.

IP Packet Analyzer (Master Process) This is Netmon's primary network traffic inspection and protocol analysis service. The "IP" is a misnomer – this service is responsible for analyzing network activity at many different OSI layers. This service coordinates each instance of a packet analyzer plugin (see below) allowing incoming data from each interface to be properly managed.

Packet Analyzer Plugins (Interfaces 0 to 3) These plugins examine particular types of network traffic. For example, the *mod_eth* plugin examines Layer 2 frame activity, while the *mod_http* plugin looks specifically for HTTP requests at Layer 7. Simply start the desired plugin for each physical interface which is to be monitored for that type of activity.

Name Resolution Service Responsible for resolving DNS and NetBIOS names for hosts which appear in Netmon's protocol analyzers. This service is generally best left active, unless you have specific reasons for not resolving DNS names.

NetFlow Collector This service analyzes incoming NetFlow datagrams and processes them according to the rules and policies set forth in the Devices section and the service configuration settings.

Pager Alert Service This service manages Netmon pager alert system. If you are not using pager alerts, you can safely stop this service.

Service Monitor This service handles ICMP and TCP Trackers in the Netmon Trackers console. In most cases, this service should be left running.

SNMP AutoDiscovery Service This service scans your Local Network range(s) for SNMP-capable devices, and tries to connect to those devices. If Netmon discovers an SNMP-capable device, it adds it to a list of discovered hosts in the SNMP console.

SNMP Interface Monitor This service monitors and records bandwidth utilization for network interfaces on SNMP-capable devices.

SNMP OID Tracker Service This service is responsible for monitoring user-defined management points on SNMP-capable devices. If you are not monitoring custom Object IDentifiers (OIDs), you can disable this service.

SNMP Trap Handler This service processes and stores SNMP trap messages, and optionally hooks into Netmon's email and pager alert system.

SYSLOG Server Starts and stops Netmon's built-in SYSLOG server. If you are not using the SYSLOG server console, you can safely stop this service.

UNIX Partition Monitoring Service This service is responsible for monitoring Linux/UNIX disks and partitions. If you are not monitoring Linux or UNIX partitions, you can disable this service.

URL Monitoring Service This service is responsible for monitoring websites and web applications. If you are not monitoring these systems, you can disable this service.

Windows Share Monitoring Service This service is responsible for monitoring Windows NT/2000/XP shared folders and disks. If you are not monitoring Windows disks with Netmon, you can safely turn this service off.

Configuring Individual Services

Many Netmon Services have customizable settings. For example, the Email Alert Service allows you to specify SMTP settings for outbound mail alert messages, and the Packet Analyzer Service allows you to adjust your historical data retention policy for that service.

To configure custom parameters for specific services, click the **Configure** link next to the associated service. You'll be brought to a page where you can configure all available items for that service.

Changing Service Startup Behavior

By default, Netmon is configured to start most background services when the appliance is booted. However, you may want to configure your system to start additional services (or services on additional network interfaces) upon a system boot. You may also wish to turn certain services off at boot time.

To change the startup behavior for a particular service (or plugin) you change the **Automatic** / **Manual** flag next to it. Setting a service/plugin to Automatic will tell your Netmon server to start that service/plugin upon system boot. Choosing **Manual** will tell your system to leave that service off at system boot.

Shutting Down and Restarting the Netmon Server Appliance

To properly shut down or reboot the Netmon server appliance properly, you'll need to log into the operating system console[17], and issue one of the following commands:

Restarting the Server

To restart the server appliance, issue the following console command, and press Enter when complete:

```
shutdown -r now
```

Shutting Down the Server

To restart the server appliance, issue the following console command, and press Enter when complete:

```
shutdown -h now
```

[17] See *Logging into the Netmon System Console* on page 15 for more information.

Troubleshooting Guide

Finding Help

Need help with your Netmon server appliance? We're here to help. For Registered Product Subscribers, assistance is just a call or click away.

- Visit the online User Guide at www.netmon.ca/support/manuals/
- Use the Live Chat feature on the Netmon website: www.netmon.ca/support/
- Use the Live Chat feature in your Netmon Help & Resources panel[18].
- Email us at support@netmon.ca
- Call us toll-free at **1-800-944-4511**

Troubleshooting the Packet Analyzer

Here are a series of tips for troubleshooting Netmon's packet analyzer:

No Visible Traffic

- Ensure that one or both network cards are plugged into a port on the switch which is receiving a copy of all of the network traffic through port forwarding, SPAN, port mirroring or a similar mechanism.

- Ensure there is a valid network link by verifying that the network jack itself displays a flashing or solid green light for both network cable connections.

- Be sure you have not applied a traffic filter or host filter in the Visual Network Explorer which is not present on your network, causing no devices and traffic to be shown in the VNE.

Seeing Partial Traffic

- If you're seeing mostly broadcast traffic (directed to x.x.x.255 addresses) and only a few instances of other types of activity, chances are that port forwarding is not configured correctly your switch. Netmon's secondary network card operates in promiscuous mode, which means that it will capture all broadcast traffic for the entire network segment being monitored, regardless of whether or not port monitoring is correctly configured.

Troubleshooting Email Alerts

Here are some tips for troubleshooting Netmon's email alerts:

[18] See *Using the Help & Resources Panel* on page 23 for more information.

1. Click **Settings** > **Initial Setup Tasks** > **Alert Testing Utility**.

2. Choose an appropriate **Recipient** from the available list.

3. Click the **Send** button.

Netmon will attempt to send a test alert message to the specified recipient. You will see the output provided by your mail server in the window. If the alert was relayed successfully, you'll receive it by email, along with an **OK** message in the output window.

If the alert was not relayed successfully, you will see the error message returned by your mail server in the output window. The most common problem seen here is that the mail server is not configured to permit the Netmon server appliance to relay email messages.

Troubleshooting Pager Alerts

Here are some tips for troubleshooting Netmon's pager alerts:

- Be sure the modem on your Netmon server appliance is connected to a dial tone via the supplied telephone cable. This line should be a plain analog line, similar to what would be required for a FAX machine. Certain phone systems do not provide a dial tone that is usable by the Netmon server.

- It’s important to distinguish between the **Pager Terminal Number** and the **Pager Number**. The Pager Number is usually the number that people dial when they wish to send you a page. The Pager Terminal Number is a special access line provided by your paging company. Instead of a voice prompt, it provides a TAP-compliant handshake to facilitate electronic communications with a system like Netmon for automated paging. In most cases, you’ll need to contact your paging service provider to acquire this number.