6.4

Management & Administration Guide

Contents

Contents 2
Introduction 5
Settings Explorer 5
Initial Setup 6
Network Interfaces 6
(Re)configuring a Network Interface 6
Network Ranges 7
Adding a New Network Range 7
Modifying a Network Range 8
Removing a Network Range from the Database 8
SMTP Configuration 8
Testing SMTP 8
Activation and Licenses 10
Registration & Activation Panel 10
Device Slot Usage Panel 10
Managing Alerts and Alert Conditionals 11
Central Alert Management 11
Modifying Alert Parameters 12
Maintenance / Blackout Windows 12
Removing a Maintenance / Blackout Window 12
Removing an Alert 12
Alert Templates 12

Reducing False Alerts with Alert Conditionals 12
Are Conditionals Mandatory? 13
Using Conditionals Effectively 13
Adding an Alert Conditional 13
Removing an Alert Conditional 13
Backup Tools 14
Netmon Backups 14
Creating a New Backup 14
Downloading a Backup 14
Restoring a Backup 15
File Management 16
Using the Files Manager 16
Backups 16
Enterprise MIBs 16
Netmon Logs 17
Saved Reports 17
Traffic Captures 17
Filter Collections 18
Traffic Filters 18
Host Filters 18
Hostname Database 19
Managing Host Names 19
Searching for Hostnames 19
Removing a Host Name 19
Adding a User Defined Host Name 20
Host Groups 21
Managing Host Groups 21
Adding a New Host Group 21
Modify an Existing Host Group 21
Removing a Host Group 21
Services & Plugins Console 22

Overview of Individual Services 22
Configuring Individual Services 23
Starting and Stopping Services 24
Data Retention Policies 24
Features and Their Associated Background Service 24
Changing Service Startup Behavior 25
Port Labels 26
Managing Port Labels 26
Adding a New Port Label 26
Modifying a Port Label 26
Removing a Port Label from the Database 27
Built-In Protocol Dictionary 27
Software Updates 28
Checking for Updates 28
User and Group Management 29
Managing User Accounts 29
Adding a New User Account 29
Viewing Account Details 30
Modifying a User Account 30
Deleting a User Account 30
Suspending and Unsuspending a User Account 30
Managing Account Groups 30
Understanding Group Permission Inheritance 31
Viewing Group Details 31
Adding a New Group 31
Modifying a Group 31
Deleting a Group 32

Introduction

Settings Explorer

The Netmon Settings Explorer 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:

- Initial Setup
- Activation and Licenses
- Alert Conditionals
- Alert Management
- Backup Tools
- File Management
- Filter Collections
- Hostname Database
- Host Groups
- Services & Plugins
- Port Labels
- Software Update
- Users & Groups

Initial Setup

The initial setup console consists of 3 panels:

- Network Interfaces
- Monitored Network Ranges
- SMTP Configuration

Network Interfaces

Netmon appliances ship with multiple physical network interfaces. At least one of these interfaces should be used to interact with the Netmon user interface itself. The other interfaces are available to monitor other networks, or to work as traffic analyzers for port mirroring configurations.

By default, all network interfaces which have a physical connection to a network will attempt to configure themselves by requesting an IP address through DHCP.

It's recommended to configure at least one interface with a static IP address, so that you can reach Netmon at a predictable network location.

(Re)configuring a Network Interface

To (re)configure a network interface, first locate the **Network Interfaces** toolbar in the Initial Setup console.

You'll see a list of interfaces in this panel. The interface name, current IP address (or DHCP if the address is dynamically-allocated) as well as the configuration type (static or DHCP). Click on any interface label to open its detail window, where you can make the following selections:

1. Choose the type of address allocation in the **IP Address** field. Possible options here are *Dynamic IP Address via DHCP* or *Static IP Address*.

2. If *Static IP Address* is selected, additional fields will appear. You can enter the desired IP address, network mask and default gateway address in the appropriate fields.
3. To save your changes and apply the new configuration to the network interface, click the **Save Changes** button.

Important Note: If you reconfigure the network interface to which your user session is attached, you may lose your connection to the Netmon application. Enter the new IP address or DNS hostname in your browser to reconnect.

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, under Settings > Define Network Range(s), which makes an editing window visible. Enter the following values in the boxes provided:

Label: A friendly identifier for this range. For example, "Cincinnati Office"

Starting Address: The starting IP address of a contiguous block.

Ending Address: The ending IP address of a contiguous block.

SNMP Auto Discovery: An Enable/Disabled choice indicating whether Netmon should attempt to scan hosts in this range for SNMP-capable devices. If you do not want Netmon to perform automatic device discovery on this range, uncheck this box.

TCP Service Auto Discovery: An Enable/Disabled choice indicating whether Netmon should attempt to scan hosts in this range for TCP services.

Once the correct information has been entered, press the **Save Changes** button.

Modifying a Network Range

To make changes to an existing Network Range, locate it in the Monitored Network Ranges panel and click on its label.

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

Removing a Network Range from the Database

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

SMTP Configuration

Netmon can use its own internal SMTP server to deliver email alerts, and this is the default configuration. You can, however, specify that Netmon use your own SMTP server to deliver mail.

To specify custom SMTP server settings, locate the **SMTP Configuration** panel in the Initial Setup console. You'll see a list of settings; clicking any one of them will open a window which allows you to edit all of them:

> **SMTP Server:** Enter the IP address of the SMTP server here. Default is 127.0.0.1 for the local SMTP server.
>
> **SMTP Account:** The email address which messages will appear to be originating from. This could be *netmon@yourdomain.com*.
>
> **SMTP Timeout:** The interval, in seconds, to wait for a response from the SMTP server when delivering a message. Netmon will attempt to deliver a message 10 times before giving up.

Testing SMTP

To ensure that email alerts will be delivered, it's important to test your SMTP configuration. Netmon has a built-in tool which will generate a test email message. To use this tool, click on the **Test SMTP** button in the SMTP Configuration toolbar.

A window will appear where you can select a recipient, enter a message subject and message body. Make the appropriate updates or edits here, and click the **Send Test Message** button.

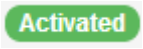
Netmon will attempt to deliver the test message immediately. If you don’t receive it after about a minute, you may want to inspect your configuration to ensure that these settings point to a valid SMTP server which will allow Netmon to relay email.

Activation and Licenses

Your Netmon appliance is licensed allow monitoring up to a specific number of devices. It also requires activation. The **Activation and Licenses** console allows you to see your licensing and activation information. To reach this console, click the **Settings** button in the top toolbar, followed by the **Activation and Licenses** link in the navigation menu.

Registration & Activation Panel

To update your registration information or re-activate your appliance, see the **Registration & Activation Panel**, which is located in **Settings > Activation and Licenses**.

1. Enter your **Registration Key** in the available text box.
2. Update your Company Name, Address information, and contact details in the available text boxes.
3. Click the **Activate Now** button. Netmon will attempt to activate your appliance using the information provided. If activation is successful, you will see the Activation Status change to 

.

Device Slot Usage Panel

This panel provides a summarized list of the device licenses you're currently using, along with indicators of which monitoring services are being utilized for each device. Next to each IP address are checkboxes for UNIX disk trackers, Windows disk trackers, TCP Service or Ping trackers, and Syslog services.

If you're running out of licenses, this panel will help you understand which hosts are consuming device licenses.

Managing Alerts and Alert Conditionals

Central Alert Management

Netmon has a central facility for managing alerts from all sections of the application. To see a list of all configured alerts across the entire system, navigate to **Settings** > **Alert Management**. Alerts are listed in a table format, with the following columns:

Status: This will either be Active or Inactive, depending on whether or not this alert is currently under a maintenance / blackout window.

Type: The type of alert. Available options here include *ICMP/TCP Tracker, SNMP OID Tracker, SNMP Trap, Windows Share Tracker, UNIX Share Tracker, Syslog*.

Label: The friendly label that has been applied to this alert.

Trigger: The set of conditions which will activate the alert.

Alert Recipient: The Netmon user who will receive the alert messages.

Maintenance Schedule: If a maintenance or blackout window has been configured for this alert, details for it will appear here.

Actions: Action buttons to permit editing, scheduling or deletion of specific alerts.

Along the top of the Alert Management interface are three buttons: **Pause Selected**, **Resume Selected**, and **Delete Selected**. These buttons work in conjunction with the checkboxes next to each listed alert. Using the checkboxes, select the alerts you would like to take immediate action on and click the appropriate button.

Modifying Alert Parameters

To modify parameters for an existing alert, click the **Edit** button to open the Settings Editor for this alert. Here you can modify the alert's conditions, descriptions, or recipients. When finished, click the **Save Changes** button.

Maintenance / Blackout Windows

To create a maintenance window for a specific alert, click the **Schedule** button next to the associated alert in the Manage Alerts console.

The Settings Editor will now show the Maintenance Scheduler. Use this interface to schedule a maintenance window, during which the alert will not be triggered. You can set a time to begin the blackout window, a duration (in hours), and even specify a recurring window (to occur during nightly backup jobs, for example).

Once a maintenance window has been created, it will be listed in the **Maintenance Schedule** column of the Alert Management console.

Removing a Maintenance / Blackout Window

A maintenance window can be removed by clicking the **Schedule** button next to the associated alert. This will open a dialog window. Click the **Reset Scheduler** button at the bottom of this window to reset blackout windows.

Removing an Alert

To remove an alert, locate it in the Alert Management console, and click the **Delete** button.

Alert 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.

Reducing False Alerts with Alert Conditionals

An alert conditional reduces false alert messages. 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 alerts. Nobody wants to receive an avalanche of alert emails.

False alerts can be reduced considerably with the use of an Alert 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** 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** field, and specify a friendly name in the **Label** field. To add this conditional to the database, press the **Save Changes** button when you have finished.

Removing an Alert Conditional

To remove an alert conditional from Netmon's database, select **Alert Conditionals** from the Settings Explorer, and click the **Delete** button next to the conditional you wish to remove. You'll be prompted to confirm your decision.

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.

Backup Tools

To manage Netmon backups, click the **Backup Tools** link in the Settings Explorer.

Netmon Backups

Creating a New Backup

To create a new backup, click the **Create Backup** button in the Backup Tools toolbar. This will open the Create Backup window with the following options / parameters:

Backup Type: You can create the backup file on the local Netmon device, for later download via the Files Manager.

Label: You can supply an optional label for your backup.

Notify User: Select a user to be notified by email when the backup operation completes.

Remove Backed Up Data When Complete: Checking this box will remove the backed up data from Netmon's live database. This is recommended to ensure that your database doesn't grow too large, which can cause performance issues.

When you have made the appropriate selections, click the **Run Backup Now** button, or click **Cancel Backup** to return to the Backup Tools console without completing the activity.

Downloading a Backup

When a backup job completes, the user that was specified (if any) in the backup notification will receive an email message confirming the completion of the job. Netmon will also add the backup file to the Files Manager and Backup Tools console.

To download a backup to your local computer, first locate the backup file in the Backup Tools console. Backup files are listed on the right side of this screen. You can also see backup files in Netmon's File Manager under the Backups tab.

Restoring a Backup

Restoring a backup to your Netmon system should be performed by Netmon Support. Please contact us for assistance.

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.

Using the Files Manager

To use the Files Manager, click the **File Management** link in the **Settings Explorer**. You can view different file types by clicking the tabs at the top of the File Manager content window.

To download a file to your local computer, click the **Download** button next to the associated file.

To delete a file from Netmon, click the **Delete** button next to the associated file.

Backups

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 button next to each item.

Enterprise MIBs

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

Netmon Logs

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** > **Services & Plugins**.

Saved Reports

While saved reports can also be viewed in the **Report Explorer**, they can also be managed from within the Settings console.

Traffic Captures

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

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

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.

Hostname Database

To open the Hostname Database console, click the **Settings** button in the top toolbar, followed by the **Hostname Database** link in the navigation menu.

Managing Host Names

Using the Hostname Database 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 string in the search box on the Hostname Database toolbar. 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. To filter on these items, make the appropriate selection from the drop-down menu beside the search box.

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** button in the Hostname Database toolbar. This will open an editing window.

1. Enter the hostname (or even just a friendly label) that you wish to use in the **Hostname** field.
2. Enter the **IP Address** of the host that will have this name or label.
3. Choose a **Node Type** from the available drop-down menu. The Node Type helps Netmon to classify a particular host, and is used to determine which device dashboard to display.
4. When you've finished entering the above information, click the **Save Changes** button. Your IP address will now appear as your friendly label throughout the Netmon application, and its device dashboard will reflect the Node Type selection you made.

Host Groups

Host Groups allow you to view a set of hosts as a collection. For example, you may want to have a host group for “New York Office” and a separate one for “Houston Datacenter”. Host Groups are managed via their own console in the Settings Explorer.

Managing Host Groups

Adding a New Host Group

To add a new Host Group, click the **Add New** button in the Host Group toolbar, which will open an editing window. Enter a group name in the text box provided, and click the **Save Changes** button.

Modify an Existing Host Group

To make changes to an existing Host Group, locate it in the list in the Host Groups console and click on it, which will open an editing window. Update your group name in the text box provided, and click the **Save Changes** button.

Removing a Host Group

To remove a Host Group, locate it in the list in the Host Groups console and click the **Delete** button next to it. You’ll be prompted to confirm your choice. If you confirm, the Host Group will be removed from Netmon’s database.

Services & Plugins Console

Overview of Individual Services

ARP Probe Service: Analyzes ARP packets and identifies MAC/IP pairs. This service is used to support new host detection.

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 Packet Analyzer Plugin below) allowing incoming data from each interface to be properly managed.

Packet Analyzer Plugins: There is one plugin instance for each physical network interface. These plugins examine particular types of network traffic. For example, the eth plugin examines Layer 2 frame activity, while the 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/SFlow Collector Daemon: 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 Auto Discovery 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 Packet Analyzer Service allows you to adjust your historical data retention policy for that service.

To configure custom parameters for specific services, click the name of the service. A window will appear where you can adjust all available configuration details for that service.

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 labeled as such with a green Running badge, and services which are off have red Stopped badge.

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.

Data Retention Policies

Netmon stores data for a specified period of time. This ensures the disk will not get filled up with data as the services continue to log network traffic and other information over long periods of time.

Netmon allows you to configure how long data will be stored in the system for each background service. This is configured under Settings > Netmon Services > configure > data archival. The data archival setting is specified as weeks. A data archival setting set to 6 weeks will mean that data will be deleted a month and a half after it is recorded.

Below is a reference to point you towards which background service you will want to edit the data retention policy for. In the below list, find the feature you want to limit data retention for, find the service name above it, and click 'configure' next to that service name in under Settings > Services & Plugins.

Features and Their Associated Background Service

Some reports depend on Netmon services. If you're having problems getting data out of some lists, reports or other views, ensure that you've correctly configured the services they depend on. Below is a list of services, and the views they enable:

- SNMP Interface Monitor
    - Bandwidth Activity Report
    - Bandwidth Graphs
    - OID Tracker Report
- IP plugin

    - Network Activity Report
    - Conversation Report
    - Bandwidth Consumption Report
    - Visual Network Explorer Traffic
- http plugin
    - Web Traffic report
- Syslog Server
    - Events and Logs

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.

Port Labels

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 the **Settings** button in the top toolbar, followed by the **Port Labels** link in the navigation menu.

Managing Port Labels

Adding a New Port Label

To add a new port label to Netmon's database, press the **Add New** button in the Port Label console, 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 **Save Changes** button.

Modifying a Port Label

To change an existing port label, click the port label itself. An editing window will appear. Made the desired changes to the transport protocol, port number or label, and click the **Save Changes** button to apply your changes.

Removing a Port Label from the Database

To remove a port label from the Netmon database, simply click the **Delete** button 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.

Software Updates

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

Important Note: The Netmon Update Service uses the RSYNC protocol to communicate with the Netmon update network. It therefore requires your Netmon server appliance to establish outbound connections on TCP Port 873.

Checking for Updates

You can 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 to open the Settings Explorer.
2. Choose **Software Update** from the navigation menu.
3. Click the **Check for New Updates button** in the Software Update toolbar.

Netmon will reach out to the update network to see if any new updates are available. If there are, you'll be prompted to confirm whether or not you'd like to apply them. If there are none, you'll receive a message indicating so and will be returned to the Software Update console.

User and Group Management

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.

To manage user accounts, click the **Users & Groups** link in the Settings Explorer.

Adding a New User Account

To add a new user account, click the **Add New** button in the Users toolbar. This will open a new user window.

User Name: A user identifier for the user. This name will be supplied by the user when logging into Netmon.

Password: A password for the user account. For best security, this password should follow length and complexity standards.

First Name: The first name of the user.

Last Name: The last name of the user.

Email Address: The email address to associate with this user account. This could be an individual email address, or it could be an alias that is associated with multiple recipients on your mail server.

Viewing Account Details

To quickly view expanded details for a user account, such as group membership, click on the **User Name**. The account details window will appear.

Modifying a User Account

To update group membership, change a password, email address or other user details, click on the account name to open the account details window. Make the desired changes, and click the **Save Changes** button.

Deleting a User Account

To remove a Netmon user account, simply click the **Delete** button 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 and Unsuspending 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 option to re-activate it later.

Suspending a user account 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, or on extended leave.

To suspend or unsuspend a user account:

1. Click on the account name to open the user details window.
2. Click the **Suspend User** or **Unsuspend User** button.
3. Click the **Save Changes** button. This will apply your updates and close the user details window.

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. The built-in groups are as follows:

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 Group 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 group, 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 Modifying 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.

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