6.4

Getting Started Guide

Contents

Appliance Installation

Appliance installation follows the standard “rack it, power it and connect it to the network” steps of any new server installation. For the smoothest installation process, keep the following factors in mind:

- To make physical network connections easier, the Netmon appliance should be close in proximity to networking equipment, particularly your core switch(es).
- Always ensure that the server is connected to UPS power. Sudden fluctuations in power can cause significant problems for your Netmon system.

Once you have installed your Netmon appliance, power it on. The appliance will boot to a Linux desktop environment. Use the following credentials to log into this environment.

User: netmon
Password: netmon

IP Address Assignment (Optional)

The Netmon installer will attempt to configure your network interface card with DHCP, for the purpose of downloading required software packages. Once Netmon is fully installed, you may manually configure the network using the graphical desktop environment.

If you do not have DHCP in your environment, or if your DHCP server takes too long to respond, the automated Debian Linux installer will display an error message, and you will have the option to retry network autoconfiguration, or to enter network settings manually.

On the Netmon desktop you will find a number of icons, including one labeled “Network Admin”. To configure your network card with a static IP address, double-click this icon. You will immediately be prompted to enter the root password, which is “netmon”.

Once in the network administration tool itself, on the tab labeled “Connections”, select the network interface you would like to use with Netmon and click the “Properties” button. You can

now choose between DHCP and static settings, and fill in the appropriate settings for your network. You can also use Network Admin to configure your DNS settings. Click the “OK” button in the “interface properties” window, then click “OK” in the “Network settings” window.

Logging In For the First Time

To log into your Netmon appliance, open a web browser and type the IP address (or DNS name) of your Netmon server in the address bar.

The default username and password for logging into the web interface is:

User: **admin**

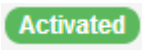
Password: **netmon**

Once you have logged in successfully, click the **Settings** button in the top toolbar, followed by the **Initial Setup** link in the navigation list on the left side of the page.

Initial Setup

License Activation

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 

.

Network Configuration

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 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.

Configuring Automatic Discovery

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.

Configuring Packet Analyzers and Port Mirroring

In order for Netmon's packet analyzers to work properly, it must receive a copy of the packets going across your network. This is accomplished using port monitoring (also known as port mirroring or port spanning) on your switch. Most business-class switches support this feature. In essence, the switch mirrors the traffic on one (or more) interfaces and forwards a copy to the destination (monitoring/mirroring/span) port.

The steps to enable port monitoring vary from manufacturer to manufacturer, so consult the product documentation for your switch to determine the necessary steps. For Cisco devices, the manufacturer has provided an excellent resource to get you up to speed on the SPAN capabilities of Cisco devices and the configuration steps that are required, in this document.

Once you have traffic forwarding working on your switch, you must plug your Netmon device into the forwarding port on your switch. The recommended configuration is to have NIC #1 (which the operating system calls eth0) configured as the Management Interface and NIC #2, 3 or 4 (which the operating system calls eth1, eth2 and eth3, respectively) as the interface for packet analysis.

This means that the Management Interface will be connected to a normal port on your switch for normal network access, and the Sniffing Interface(s) will be plugged into the mirrored port(s) on your switch so it can monitor network traffic.

Once you've made the physical connection and configured your switch, you'll need to activate Netmon's packet analyzer for each interface which will be monitoring traffic. To do this, go to **Settings** > **Services & Plugins**. Ensure that the IP Packet Analyzer (Master Process) is running in the **Services** panel. If it's not running, click the **Start Service** button. Then review the **Plugins** panel to the right. These plugins represent different types of packet analyzers:

eth plugin: Analyzes layer 2 (i.e. Ethernet-level) frames.

http plugin: Performs deep packet inspection on HTTP traffic

IMAP plugin: Performs deep packet inspection of IMAP email traffic

IP plugin: Monitors layer 3 IPv4 traffic

netflow emitter plugin:

POP3 plugin: Performs deep packet inspection of POP3 email traffic

SMTP plugin: Performs deep packet inspection of SMTP email traffic

You can start or stop any plugin on any configured network interfaces. Changing the start/stop status of any service or plugin is preserved across system reboots, so your preferences will be saved.

Note: If you are unable to start packet analyzers on a particular interface, there may be a configuration problem with that interface.

Note: It is not recommended to run packet analyzers on eth0 interface. This interface is recommended for management/web access.