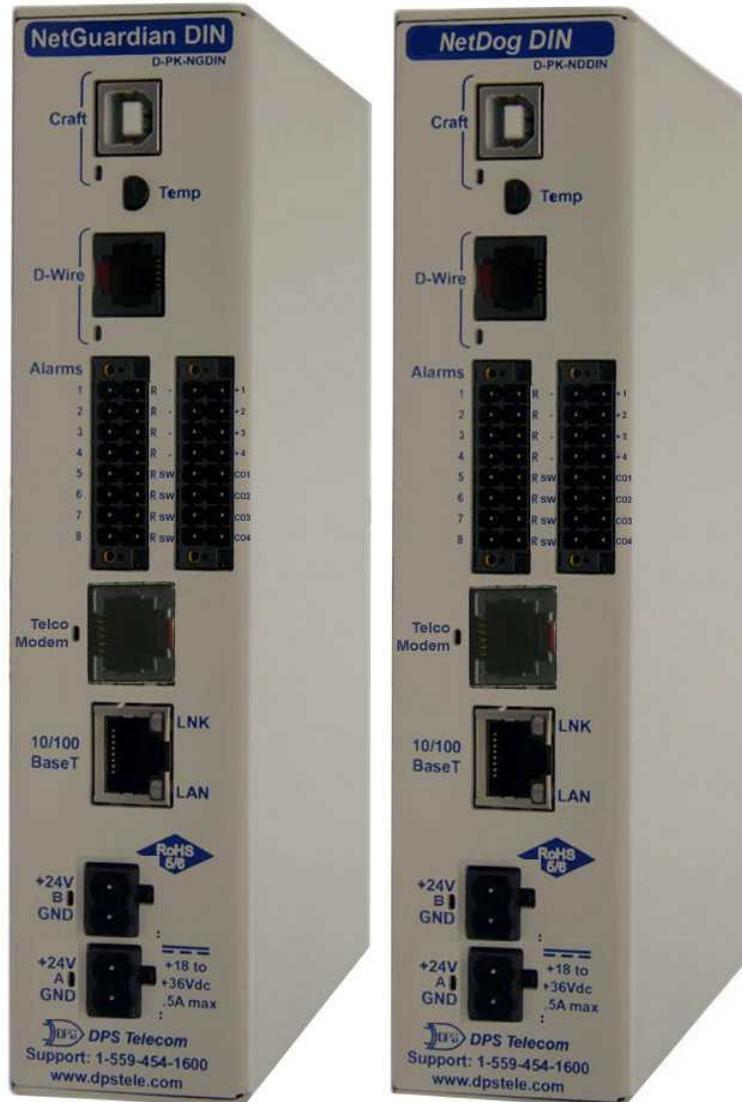# *NetGuardian DIN/ NetDog DIN*

USER MANUAL

D-PK-NGDIN

Visit our website at www.dpstelecom.com for the latest PDF manual and FAQs.

Revision History

August 27, 2020	Added Alarm Echo section
November 13, 2019	Updated RADIUS feature
August 23, 2019	Added Auto Sync Request feature
April 19, 2019	Expanded Modbus configuration options
July 2, 2018	Added support for Persistent Alarm Counter
January 18, 2018	Added support for Modbus and HVAC monitoring
October 20, 2017	Added D-PK-DNPAN to optional accessories list
September 13, 2017	Timed Tick added to Timers
March 23, 2017	Added History Log Format and Operation Section
November 19, 2015	Serial Ports section added to Provisioning
October 14, 2015	Updated Display Mapping section
July 8, 2015	Added Data Port Section
May 15, 2015	Multi-Purpose Analog Inputs Added
February 6, 2015	NetDog DIN Added
January 14, 2015	Updates to Control Screenshots
February 13, 2014	Initial Release

Contents

1 NetGuardian DIN Overview

Do you need a **compact** way to protect your IT server room or data center? Have you estimated how much your network uptime is **worth to you**? These questions are important when considering how to monitor and protect your vital IT equipment. The **NetGuardian DIN** is a compact, simple and reliable device that easily fits on a DIN rack and monitors basic environmental conditions (like temperature, humidity, smoke...) around your valuable equipment. Without this environmental visibility, your server room is at risk of serious damages that could lead to major outages and system failure.

The NetGuardian DIN features:

- **Up to 8 Discrete Alarm Inputs (Build Option)**
- **Up to 8 Analogs (Build option)**
- **1 D-Wire sensor input jack (Build option), supporting up to 32 sensors (sold separately)**
- **6 Control Relay Outputs (Build option)**
- **Fast, integrated web browser**
- **32 ping targets to monitor other devices on the network**

Fig. 1.1 *How to access HyperTerminal.The NetGuardian DIN.*

NOTE: The NetGuardian DIN also refers to the NetDog DIN.

The NetGuardian DIN will help you monitor all the environmental levels that affect your servers, phone closets, data centers, and other equipment locations. The 8 discrete alarms on the front panel are used to monitor dry contacts, such as motion sensors, UPS, smoke detectors, flood sensors, AC and room entry. All of this information can be monitored from the easy-to-use web interface using any of your network computers.

Don't wait until the day your cooling fans wear out and your server closet **overheats** to start protecting your system. The compact NetGuardian DIN alerts you of changing conditions 24 hours a day, 7 days a week, either to your cell or SNMP manager. The NetGuardian DIN is the cost-effective way to stay proactive in your monitoring.

The NetGuardian DIN reports alarms as SNMP traps over LAN and supports DCP polling over LAN. The NetGuardian DIN supports simultaneous SNMP and DCP operation.

NetGuardian DIN has the option of up to 8 Analogs, 8 or 6 Discrete alarms and 2 control relays, all form A, user defined NO/NC with shunt. The control relays allow network administrators to respond remotely to threats to system integrity. Using the control relays, network administrators can turn on backup generators, open doors and gates for emergency access, reboot equipment, or perform other functions. The NetGuardian DIN also allows you to reverse the logic state of the alarm on a point by point basis for discrete alarms. The single D-Wire port gives access to the "DPS Sensor Network" for measuring environmental conditions by daisy-chaining multiple sensors together. Up to 8 notifications can be

created and sent via email/txt and can include TRIP protocol.

Another feature of the NetGuardian DIN is user-defined alarm qualification times. This will allow you to clearly distinguish momentary status changes from serious problems.

2   Specifications

Discrete Alarm Inputs:	8 (Optional build with 6 alarms and 2 controls) Up to 8 dry 5V alarms (optional)
Control Relays:	6 (Form A) user defined NO/NC (Optional)
Analog Inputs	8 (Optional)
Analog Input Range:	-90 to +90 VDC (or 4-20mA)
Analog Accuracy:	+/- 1% of Analog Range (See analog step sizes)
Ping Targets:	32
Protocols:	SNMPv1, SNMPv2c, SNMPv3, DCPx, TELNET, HTTP, HTTPS, Email, TRIP
Dimensions:	2.1" H x 7.250" W x 5.150" D
Weight:	1.13 lbs (.513 kg)
Mounting:	DIN mount, Wall mount option (brackets sold separately)
Power Input:	–48 VDC nominal (–36 to –72 VDC) (Optional) –24 VDC nominal (–18 to –36 VDC) (Optional) Wide Range –24/–48 VDC (–18 to –58 VDC) (Optional) +24VDC (+18 to +36 VDC) (Optional) +12VDC (+11 to +18 VDC) (Optional) Power Over Ethernet (POE) (POE has priority when built with POE and standard power inputs)
Fuse:	Internal Resetable
Current Draw:	140 mA @ 24VDC
Interfaces:	1 RJ45 10/100BaseT full-duplex Ethernet port 1 USB front-panel craft port 1-4 RJ11 connector for D-Wire sensor network (Optional) 1 RJ11 Connector for Telco
Visual Interface:	7 Front Panel LEDs
Operating Temperature:	32° - 140° F (0° - 60° C)
Industrial Temperature Option:	-22° to 158° F (-30° to 70° C)
Operating Humidity:	0% - 95% non-condensing
MTBF:	60 years
Windows Compatibility:	XP, Vista, 7 (32 or 64 bit)
RoHS	5/6
Sensors:	Up to 15 dwire sensors

1 built-in temp sensor (Optional)

3   Shipping List

Please make sure all of the following items are included with your NetGuardian DIN. If parts are missing, or if you ever need to order new parts, please refer to the part numbers listed and call DPS Telecom at **1-800-622-3314**.

NetGuardian DIN
D-PK-NGDIN

NetGuardian DIN Resource CD
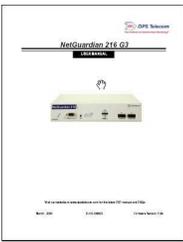
NetGuardian DIN User Manual
D-UM-NGDIN

6 ft. USB Download Cable
D-PR-046-10A-06

 x 1

Lg. Power Connector (Main Power)
2-820-00862-02

14ft. Ethernet Cable
D-PR-932-10B-14
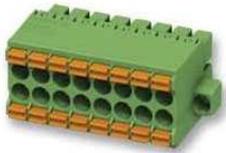
 x 1

8-Pin Alarm Connector
2-821-20835-00
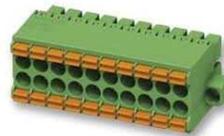
 x 1

10-Pin Alarm Connector
2-821-21035-00

3.1   Optional Shipping Items - Available by Request

Temp Sensor Node
D-PK-DSNSR-12001

Temp/Humidity Sensor Node
D-PK-DSNSR-12002

Din-Mount Pluggable Panel
D-PK-DNPAN-12001

Din-mount pluggable panel that allows for convenient termination access to discrete alarms, controls, and analogs.

NOTE: Not compatible with all NetGuardian DIN builds. Please call DPS for more information.

4   Installation

4.1   Mounting

Below are two simple steps needed to mount the NetGuardian DIN on a standard DIN rail.
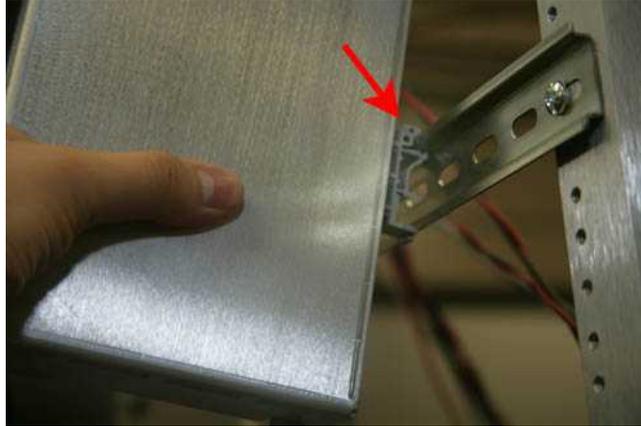
Fig. 4.1 *First connect the top of the DIN clip to the rack.*
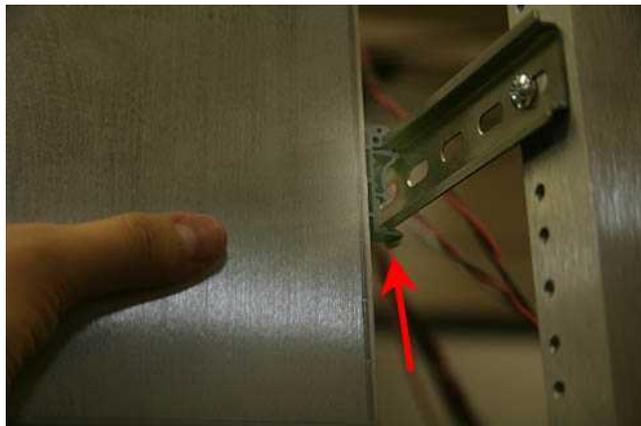
Fig. 4.2 *Then snap the bottom of the DIN clip to the bottom of the rack.*

Note: The NetGuardian DIN has a wall mounting option. The brackets are sold separately.

4.2   Power Connection

The NetGuardian DIN uses single or dual (Optional) power inputs, powered through two barrier plug power connectors.

Fig. 4.3 *NetGuardian DIN Power Terminal*

To connect the NetGuardian DIN to a power supply:

1. Locate the metal grounding lug next to the symbol ⏚. Use the grounding lug to connect the unit to earth ground.
2. Insert the eyelet of the earth ground cable between the two nuts on the grounding lug (Ground cable not included).
3. Choose a barrier plug power connector to attach your power cable to. The plug's right terminal is Ground and its left terminal is Battery Lead.
4. Insert a battery ground into the power connector plug's right terminal (GND) and tighten the screw.
5. Insert a battery lead to the plug's left terminal and tighten its screw.
6. Insert fuse into the fuse distribution panel.
7. Check the power status LED.
8. Measure voltage. Connect the black cable onto the ground connector of your Digital Voltage Meter (DVM) and red cable onto the other connector of your DVM. The voltmeter should read between the values listed on the silk screen next to the power connector.
9. The power plug can be inserted into the power connector only one way to ensure the correct polarity.

Note: The battery terminal is on the left and the GND terminal is on the right.

10. Verify that the ☼ LED is lit. To confirm that power is correctly connected, the front panel status LED will flash RED and GREEN, indicating that the firmware is booting up.

4.3   Configuration

To configure the NetGuardian DIN, you'll need a PC with terminal emulator, such as HyperTerminal.

5   NetGuardian DIN Front Panel
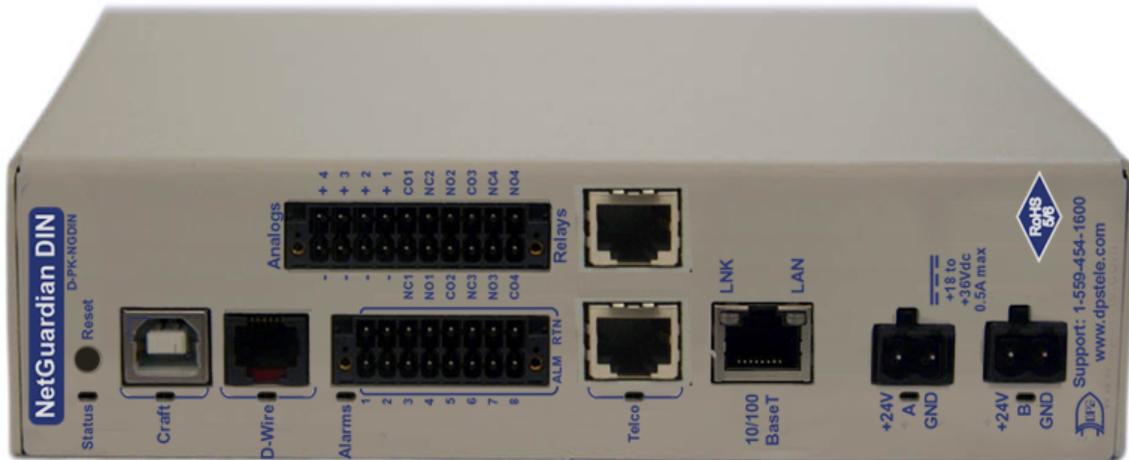
Fig. 5.1 *NetGuardian DIN Front Panel*

LED	Status	Description
Status	Flashing Green	Application Running
	Flashing Red	Bootloader Running
Craft	Flashing Green	Transmit over craft port
	Flashing Red	Recieve over craft port
D-Wire	Solid Green	At least 1 D-Wire enabled, no alarm
	Solid Red	New Alarm
	Off	No D-Wire Sensors attached.
Alarms	Flashing Red	New Alarm
	Solid Red	Standing Alarm Acknowledged via DCP poll
	Off	No Alarms
Power (A or B)	Solid Green	Has power
	Off	Does not have power or polarity reversed.
Reset		Reserved for future use. To reset the unit, see the *TTY Interface* section of this manual.

Front Panel LED Descriptions

5.1   Multi-Purpose Analog Inputs
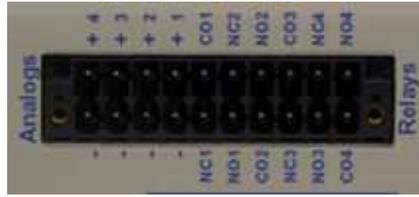
Fig. 5.2 *Analog Connectors*
(Note: Analog Channel Polarity does not match label on units shipped prior to 09/27/14)

The NetGuardian's six multi-purpose analog inputs measure continuous ranges of voltage or current. Analog alarms are typically used to monitor battery voltage, charging current, temperature, humidity, wind speed, or other continuously changing conditions. The measurement range of the analog channels is –90 to +90 VDC or 4 to 20 mA. To configure the analogs for current sensing (4 - 20mA) please review the section "Switching Analog Alarms to Current Operation" for info on jumper position.

To connect analog inputs, remove the connector plug, connect the leads to the appropriate terminals and reinsert the barrier plug. Note that the plug can be inserted into its socket only one way, so make sure it can only be reinserted with the alarm inputs aligned correctly.

By default, the analog inputs are configured to measure voltage. You can switch the analog inputs to measure current by resetting jumpers on the NetGuardian's circuit board.

Analog Step Sizes:
Your Analogs are accurate to within +/- 1% of the analog range.

Analog Step Sizes and Accuracy		
Input Voltage Range	**Resolution (Step Size)**	**Accuracy**
0-5 V	.0015 V	+/- .05V
5-14 V	.0038 V	+/- .14V
14-30 V	.0081 V	+/- .30V
30-70 V	.0182 V	+/-.70V
70-90 V	.0231 V	+/-.90V

5.1.1   Switching Analog Alarms to Current Operation
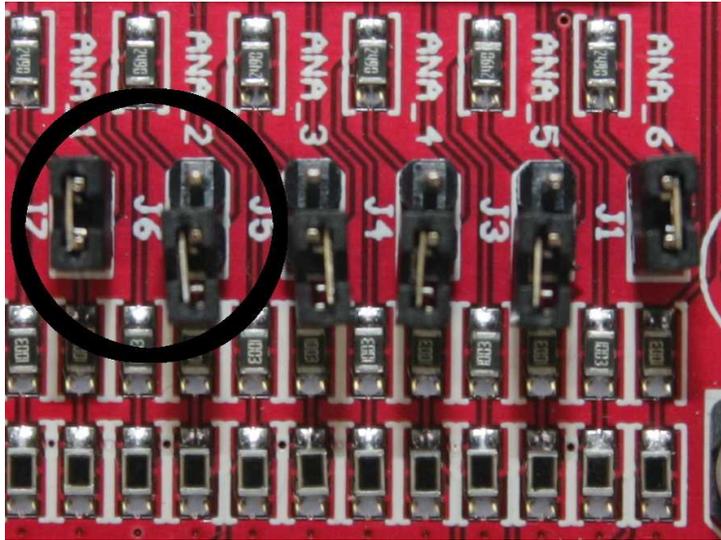
Fig. 5.3 *Adjustable jumpers on the NetGuardian circuit board*

To test the analog alarm voltage/current jumpers, follow these steps:

1. Make sure the NetGuardian is powered down and disconnected from all network connections.
2. Remove the screws from the sides of the NetGuardian case.
3. Slide the top cover of the case off to expose the circuit board.
4. The adjustable jumpers are shown in the above diagram. All alarm inputs can be individually configured for current or voltage operation. Remember that the default jumper position is OPEN for measuring voltage. **Note:** Each jumper inserts a 250-ohm shunt resistor across the input. This must be taken into account when defining the analog input reference scale.
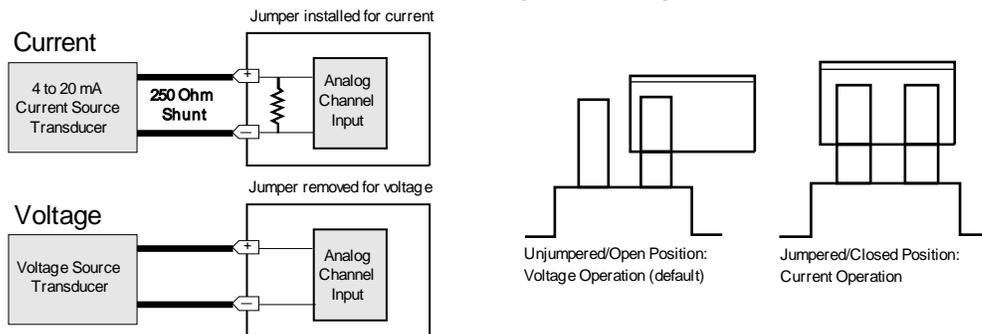
5. Slide the top cover of the case back into position and replace the screws.
6. Reconnect and power up the NetGuardian.

6   Quick Start: How to Connect to the NetGuardian DIN

Most NetGuardian DIN users find it easiest to give the unit an IP address, subnet and gateway through the front craft port (TTY interface) to start. Once these settings are saved and you reboot the unit, you can access it over LAN to do the rest of your databasing via the Web Browser interface.

Alternative option: You can skip the TTY interface by using a LAN crossover cable directly from your PC to the NetGuardian DIN and access its Web Browser.

6.1   ...via LAN

Fig. 6.1 *NetGuardian DIN Ethernet Port*

To connect to the NetGuardian DIN via LAN, all you need is the unit's IP address (Default IP address is 192.168.1.100).

If you DON'T have LAN, but DO have physical access to the NetGuardian DIN, connect using a LAN crossover cable. **NOTE:** Newer PCs should be able to use a standard straight-through LAN cable and handle the crossover for you. To do this, you will temporarily change your PC's IP address and subnet mask to match the NetGuardian DIN's factory default IP settings. Follow these steps:

1. Get a LAN crossover cable and plug it directly into the NetGuardian DIN's LAN port.
2. Look up your PC's current IP address and subnet mask, and write this information down.
3. Reset your PC's IP address to **192.168.1.200**. Contact your IT department if you are unsure how to do this.
4. Reset your PC's subnet mask to **255.255.0.0**. You may have to reboot your PC to apply your changes.
5. Once the IP address and subnet mask of your computer coincide with the unit, you can access the unit via a Telnet session or via Web browser by using the unit's default IP address of **192.168.1.100**.
6. Provision the NetGuardian DIN with the appropriate information, then **change your computer's IP address and subnet mask back to their original settings.**

Now you're ready to do the rest of your configuration via LAN. Plug your LAN cable into the NetGuardian DIN and enter your username and password.
NOTE: Default username is **admin** and password is **dpstelecom**.

6.2   ...via Craft Port (using TTY Interface)

Fig. 6.2 *NetGuardian DIN Craft Port*

Use the front panel craft port to connect the NetGuardian DIN to a PC for onsite unit configuration. To
use the craft port, connect the included DB9 download cable from your PC's COM port to the craft port.

Note: The following images display the setup process done in Windows XP.

The following steps will occur the first time any DPS USB equipment is used on this PC. If you've used a different DPS USB device before and have installed the DPS USB drivers, then **skip to Step 9**.

When you first connect the NetGuardian DIN to your PC via USB, a "Found New Hardware" message will appear:

1. Click the "Found New Hardware" message/icon to launch the "Found New Hardware Wizard".

2. Select "Install from a list or specific location (Advanced)"
3. Click "Next >"
4. Select "Search for the best driver in these locations."
5. Insert NetGuardian DIN Resource Disc (CD) into your PC.
6. Click "Browse"
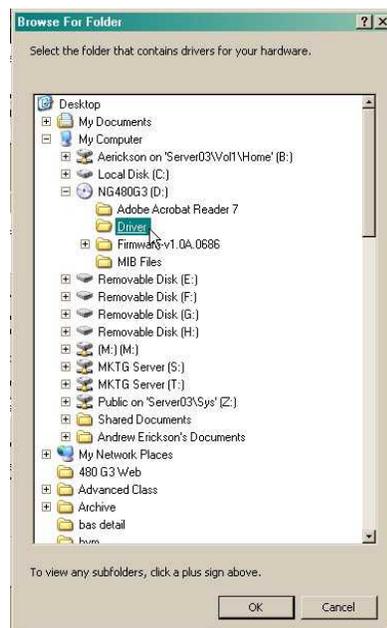
7. Select the "Driver" folder of your NetGuardian DIN Resource Disc Disc (CD) and click "OK"

The following message will confirm installation of a new "USB Communications Port"

8. Click "Finish" to close the Wizard.

Now that the driver has been installed, a new COM port is being emulated on your PC. Before using hyperterminal, you must confirm the identity of that new COM port (COM1, COM2, COM3...) in the Windows Device Manager.

9. Right-click the "My Computer" icon on your desktop, then click "Manage"
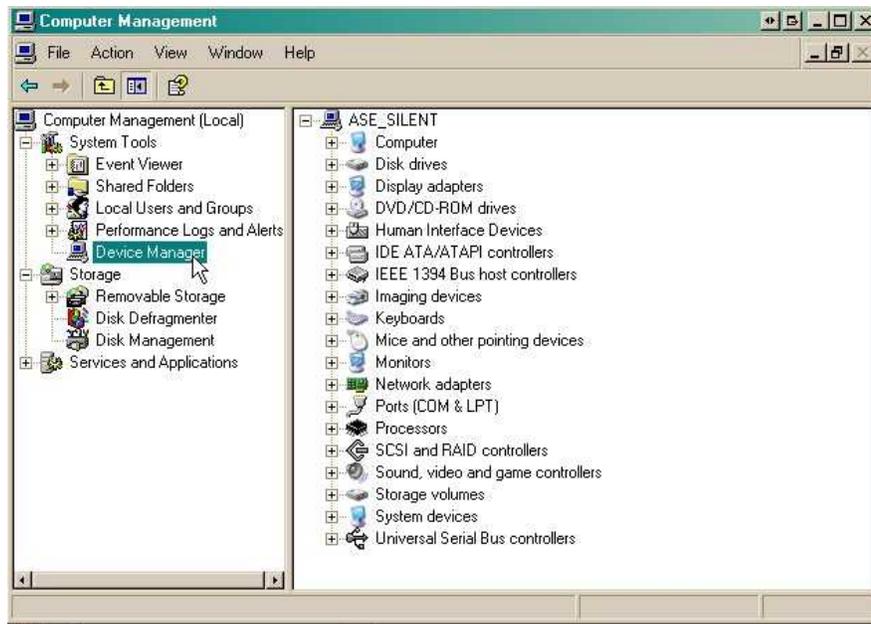
10. Click "Device Manager" in the left pane.
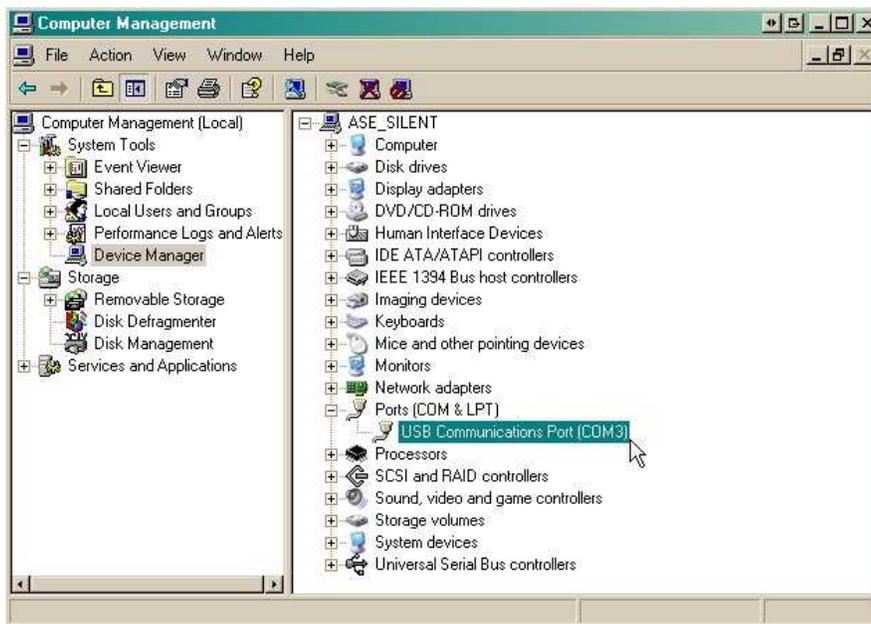
11. Expand the "Ports (COM & LPT)" section in the right pane. Look for "USB Communications Port (COMx)". Note the number of the COM port ("COM3" in the example above).

12. Click on the **Start** menu **>** select **Programs** > **Accessories** > **Communications** > **HyperTerminal.**

13. At the Connection Description screen, enter a name for this connection. You may also select an icon. The name and icon do <u>not</u> affect your ability to connect to the unit.
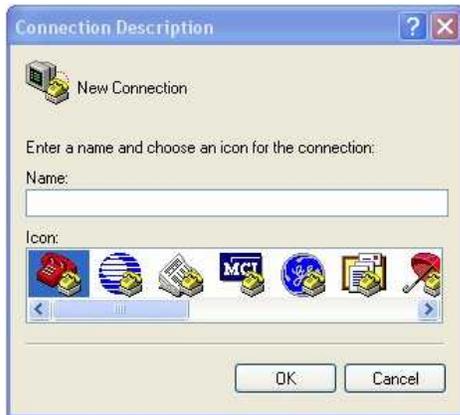
14. At the Connect To screen, use the drop-down menu to select the COM port you found earlier in the Device Manager.

15. Select the following COM port options:
   • Bits per second: 9600
   • Data bits: 8
   • Parity: None
   • Stop bits: 1
   • Flow control: **None**

 Once connected, you will see a blank, white HyperTerminal screen. Press Enter to activate the configuration menu.

16. When prompted, enter the default user name **admin** and password **dpstelecom**. <u>NOTE</u>**:** If you don't receive a prompt for your user name and password, check the Com port you are using on your PC and make sure you are using the cable provided. Additional cables can be ordered from DPS Telecom.
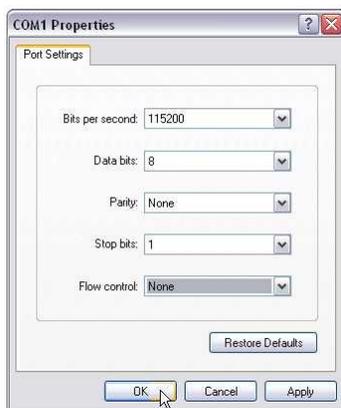
17. The NetGuardian DIN's main menu will

18. ESC to the main menu. When asked if

appear. Type C for C)onfig, then E for E)thernet. Configure the unit's IP address, subnet mask, and default gateway.
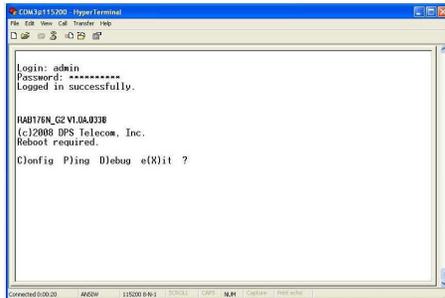
you'd like to save your changes, type Y for Y)es. Reboot the NetGuardian DIN to save its new configuration.

```
COM3p115200 - HyperTerminal
File  Edit  View  Call  Transfer  Help

Login: admin
Password: **********
Logged in successfully.

RAB176N_G2 V1.0A.0330
(c)2008 DPS Telecom, Inc.
Reboot required.

C)onfig  P)ing  D)ebug  e(X)it  ?

Connected 0:00:20    ANSIW    115200 8-N-1    SCROLL    CAPS    NUM    Capture    Print echo
```

```
Linked       : No
DHCP         : Disabled
Host Name    :
Unit IP      : 126.10.230.127    (126.10.230.127)
Subnet Mask  : 255.255.192.0     (255.255.192.0)
Gateway      : 126.10.255.23     (255.255.255.255
Unit MAC     : 00.10.81.00.53.33 (00.10.81.00.53.

U)nit Addr  S)ubnet  G)ateway  D)HCP  H)ost  (ESC

E)thernet  S)tats  n(V)ram  re(B)oot  (ESC) ?

Do you want to save changes (y/N) : _
```

Now you're ready to do the rest of your configuration via LAN. Please refer to the next section "...via LAN" for instructions on setting up your LAN connection.

7   TTY Interface

The TTY interface is the NetGuardian DIN's built-in interface for basic configuration. From the TTY interface, you can:

- Edit the IPA, subnet, and gateway
- Configure primary port
- Set unit back to factory defaults
- Set DCP info for T/Mon polling
- Ping other devices on the network
- Debug and troubleshoot

  For more advanced configuration tools, please use the Web Browser Interface.

For Telnet, connect to the IP address at port 2002 to access the configuration menus after initial LAN/WAN setup. **Telnet sessions are established at port 2002, not the standard Telnet port** as an added security measure.

If you're using Windows 7, then you'll need to install telnet before you can use the TTY interface. To install telnet, open up your command line (type "cmd" into the search bar in the **Start Menu**). Select **cmd.exe** to run the command line.
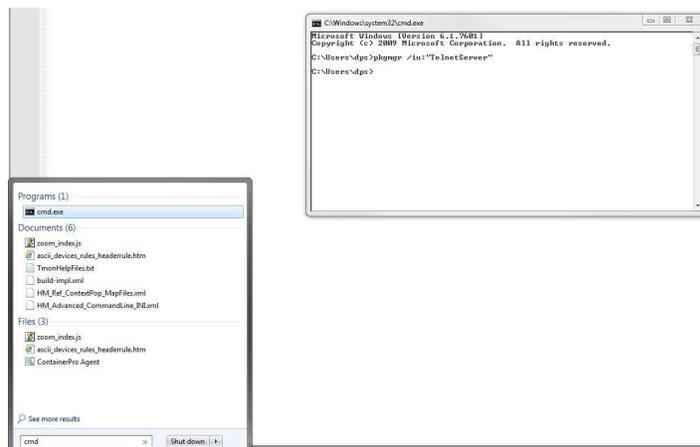
Fig. 7.1

From the command line, type in **pkgmgr /iu:"TelnetClient"** then press **enter**. When the command prompt appears again, the installation is complete.

Menu Shortcut Keys
The letters before or enclosed in parentheses () are menu shortcut keys. Press the shortcut key to access that option. Pressing the ESC key will always bring you back to the previous level. Entries are not case sensitive.

To reset unit to factory default settings:

Connect to the craft port to login to the unit. The user prompt will pop up

Use command options to initialize:
     User: init
     Password: Init!999

Press (C)onfig > n(V)ram > (I)nitialize > (Y)es

8 Quick Turn Up

The next sections of this manual will walk you through some of the most common tasks for using the NetGuardian DIN. You will learn how to send email notifications, and send SNMP traps to your alarm master - all using the Web browser. For details on entering your settings into each Web browser menu, the section "Provisioning Menu Field Descriptions" section.

8.1 How to Send Email Notifications

1. Click on the **Notifications** button in the **Provisioning** menu. You can setup as many as 8 different notifications. Begin the setup "wizard" by clicking **Edit** for a notification number. In this example, we'll setup Notification 1 to send emails.

Fig. 8.1

2. At the **Notification Setting** screen, use the drop down box to set what events to use for this notification. Now, select the **Send Email Notification** button and click **Save and Next**.

Fig. 8.2

3. At the **Email Notification** screen, you'll enter your email server settings. Enter the **IP address** or **Host Name** of your email server. Enter the **Port Number** (usually 25) and the **"To" Email Address** of the technician that will receive these emails. If authentication is required, chose the type and fill in the necessary fields. Click **Next**.

Notification 1 (Email)

SMTP Server IP or Host Name	
Port (Usually Use 25)	0
"From" E-mail Address (Global)	xxxxxxx@dpstele.net
"To" E-mail Address	

How to authenticate

◉ No authentication
○ POP before SMTP authentication
○ SMTP authentication

POP Server IP or Host Name	
POP Port (Usually Use 110)	0
User name	
Password	

[Back] [Save and Next]

Fig. 8.3

4. At the **Schedule** screen, you'll select the exact days/times you want to receive email notifications. You can set 2 schedules per notification. For example, you may want to receive notifications at certain times during the week, and at different hours on the weekend. Use the check boxes to select the days of the week, and select the time from the drop down menus. Click **Finish.** To try a test notification, click the **Test** button (See next step.)

Fig. 8.4

5. If you chose to test the email notification you've just setup, you will prompted with a pop up . Click **OK** to send a test email alarm notification. Confirm all your settings by checking your email to see if you've received it. **NOTE:** This test only means that your notification settings are correct, but you still need to assign the notification to an alarm point. See the next step.

6. Now you will associate this notification to an alarm (system, base, analog, etc.) You have 8 notification devices available to use. In the image below, you might assign **Notification Device 1** to **Alarm 1**. This means that you would receive an email notification when an alarm for **Alarm 1** (SERVER ROOM**)** occurs.

Fig. 8.5

8.2   How to Send SNMP Traps

1. Click on the **SNMP** button in the **Provisioning** menu. Enter the **SNMP GET** and **SNMP SET** community strings for your network, then click **Save**. The typical SNMP SET and GET community strings for network devices is "public". As an added security measure, we've made our default "dps_public".

2.

Fig. 8.6

2. Click on the **Notifications** button in the **Provisioning** menu. You can setup as many as 8 different notifications. Begin the setup "wizard" by clicking **Edit** for a notification number. In this example, we'll setup Notification 1 to send SNMP traps to your alarm master.

Fig. 8.7

3. At the **Notification Setting** screen, use the drop down box to set what events to use for this notification. Now, select the **Send SNMP Notification** button and click Next.

Notification 1

Status	Notify on both Alarms and Clears ▾
Type	○ Send Email ⦿ Send SNMP

[Back] [Save and Next]

Fig. 8.8

4. At the **SNMP Notification** screen, you'll enter your network's SNMP settings. Enter the **IP address** of your SNMP Trap Server. Enter the **Trap Port Number** (usually 162) and the **Trap Community** password. Click **Save and Next**.

Notification 1 (SNMP)

SNMP Trap Server IP	
Trap Port No. (Usually Use 162)	0
Trap Community	
Trap Type	SNMPv1
SNMPv3 user (see SNMP menu)	User 1 ()

Back | Save and Next

Fig. 8.9

5. At the **Schedule** screen, you'll select the exact days/times you want to receive SNMP notifications. You can set 2 schedules per notification. For example, you may want to receive notifications at certain times during the week, and at different hours on the weekend. Use the check boxes to select the days of the week, and select the time from the drop down menus. Click **Save and Finish.** To try a test notification, click the **Test** button (See next step.)

Notification 1 (Schedule)

Id	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Notification Time	
1	✔	✔	✔	✔	✔	✔	✔	○ Any Time	⊙ 12 h 0 min AM to 11 h 59 min PM
2	✔	✔	✔	✔	✔	✔	✔	○ Any Time	⊙ 12 h 0 min AM to 11 h 59 min PM

Back | Save and Finish

Fig. 8.10

6. If you chose to test the email notification you've just setup, you will prompted with a pop up . Click **OK** to send a test SNMP alarm notification. Confirm all your settings by checking your alarm master to see if the SNMP trap was received.

NOTE: This test only means that your notification settings are correct, but you still need to assign the notification to an alarm point. See Step 6 in "How to Send Email Notifications" for more detail.

8.3   How to Send TRIP Notifications

1. Click on the **Notifications** button in the **Provisioning** menu. You can setup as many as 8 different notifications. Begin the setup "wizard" by clicking on **Edit** for a notification number. In this example, we'll setup Notification 8 to send an voice alert.

2. At the **Notification Setting** screen, select the conditions you want to be notified of from the drop down: **Notify on both Alarms and Clears, Notify on Alarms only, Notify on Clears only.** (Selecting Notification Disabled means you will not receive any type of alerts.) Select **Trip Dialup (T/Mon)** and click Next.

Fig. 8.11

3. At the next screen, you'll select the phone number the NetGuardian should call when this particular alarm is triggered. Enter the T/Mon's phone number and chose if you want the NetGuardian to dial only if the DCP poller inactive is selected. Then click **Save and Next**.

Fig. 8.12

5. At the **Schedule** screen, you'll select the exact days/times you want to receive notifications. You can set 2 schedules per notification. For example, you may want to send after hours or at certain times during the week, and at different hours on the weekend. Use the check boxes to select the days of the week, and select the time from the drop down menus. Click **Save and Finish.** To try a test notification, click the **Test** button (See next step.)

Fig. 8.13

6. Click **Test** to send a test voice notification. **NOTE:** This test only means that your notification

settings are correct, but you still need to assign the notification to an alarm point (See step 6 of the "How to Send Email Notifications" section).

9   LAN Security

The Telnet interface is available on TCP port 2002. It is enabled by default per section *9.1 LAN Lockdown*.

The web interface is available on the HTTP port 80 and HTTPS (SSLv3) port 443. Both are enabled by default. HTTP can be disabled per section *9.1*, but HTTPS is always active.

All file transfers take place over HTTP/HTTPS; scp, sftp, ftp are not supported.

9.1   LAN Lockdown

Telnet and HTTP can be disabled via the TTY interface. HTTP can be disabled via either Telnet or USB sessions, but Telnet can only be disabled via a USB session.

To lockdown, browse to C)onfig, L)ockdown. This will display the port each service is running on or "LOCKDOWN" if it is locked down. Press T)elnet or H)TTP to toggle lockdown for that service. Note that services are locked down immediately, but changes must be saved by escaping to the top menu to persist a reboot.
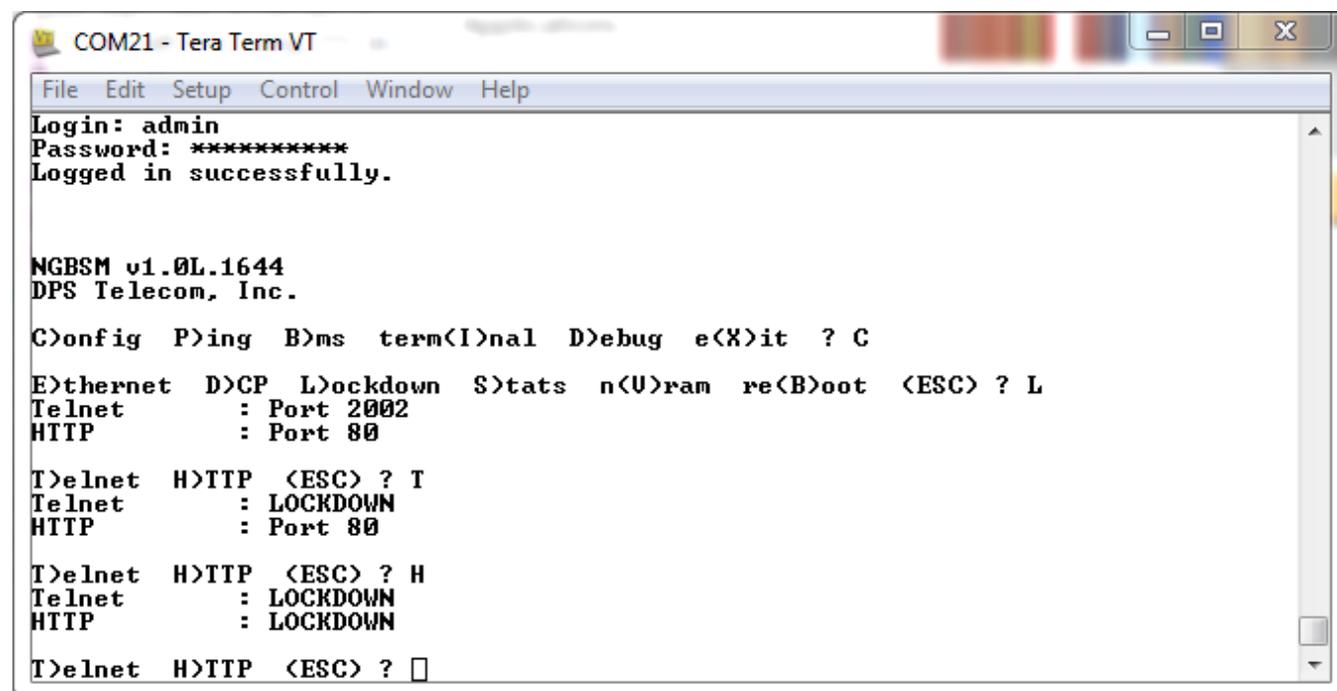
Fig. 9.1

10 Provisioning Menu Field Descriptions

NetGuardian DIN configuration is performed from the **Provisioning** menus, the menu options in green on the left-side of the web interface. The following pages provide a brief description of the options available in each menu.

Saving Configuration Changes to the NetGuardian DIN:
At the bottom of each screen you access from the **Provisioning** Menu, you will see a **Save** button. Clicking Save will cache your changes locally. The web interface will then prompt you to either **Write** your changes to the unit or **Reboot** the unit for changes to take effect in the top-left corner of your browser. The relevant options will be highlighted in the **Device Access** options**.**

Note: If the unit prompts you to both Write changes to the unit **and** Reboot, you will Write your changes first. Rebooting without writing to the unit (if a Write is required) will cause you to lose your configuration changes.

Please **WRITE** to the unit after you are finished with your changes!
Please **REBOOT** the unit for changes to take effect!

Status messages on the NetGuardian DIN Device Access menu, inform you how to implement your changes

Device Access			Device Access
Backup Config			Backup Config
Read			Read
Write			**Write (required)**
Initialize			Initialize
Get Log			Get Log
Purge Log			Purge Log
Reboot			Reboot
Fig. 10.1			*Fig. 10.2*

The control menu highlights items that must be completed for your changes to take effect

10.1 System

From the **Provisioning** > **System** menu, you will configure and edit the global system, call, T/Mon and control settings for the NetGuardian DIN.

Fig. 10.3
The Provisioning > System menu

Global System Settings	
Name	A name for this NetGuardian DIN unit. {Optional field}
Location	The location of this NetGuardian DIN unit. {Optional field}
Contact	Contact telephone number for the person responsible for this NetGuardian DIN unit. {Optional field}
TRIP Unit ID	Site number used when communicating over dialup with T/Mon.
Auto sync request on every Timed Tick alarm.	Periodically resend notifications on every Timed Tick. NOTE: Timed Tick must be enabled for this feature to work.
DCP Responder Settings *(For use with T/Mon)*	
DCP Unit ID	User-definable ID number for the target unit (DCP Address)

DCP Unit Protocol	Drop-down menu of available protocols for use with DCP Address
DCP over LAN port	Enter the DCP port for the target unit (UDP/TCP port)
LAN Protocol	Drop-down menu of available protocols for use over LAN
Alarm Echo Settings	
Alarm Echo	Enable DCP interrogator to gather 16 alarms and 10 control relays of other device and display them in the alarm echo tab.
Sensors History	
Get History	Download a log of all configured analog and sensor values.
Erase History	Erase the log of all configured analog and sensor values.

10.1.1 History Log Format and Operation

GET parameters can be used with the history.csv or the eventlog.csv request to filter the returned data. When no GET parameters are supplied, all data will be returned in CSV format.

To add GET parameters:
❑Right-click the **history.csv** link on the *Provisioning > Systems* page.
❑Depending on your browser, select either "Copy link address", "Create link shortcut", or similar option.
❑Paste the link in a new tab on your chosen web browser.
❑Add the desired parameters to the link.
  - The string must start with a "?" after the **.csv**
  - Enter the parameter, then "=", followed by desired value (described in description in the table below).
  - To enter multiple parameters, each should be separated by "&".
  - **Example:** http://10.0.6.45/history.csv?st=1397669439&et=1397671119&uk1=userkey1&uk2=userkey2
❑Press enter to return results.

Example Output:
```
systime,utime,chan,romid,description,average,minimum,maximum,units,ukey1,ukey2,ukey3
2011-02-03 11:13:27,1296731607,9,28E5644407000046,test,75.750,75.750,75.750,F,,,
2011-02-03 11:12:27,1296731547,9,28E5644407000046,test,75.750,75.750,75.750,F,,,
2011-02-03 11:11:27,1296731487,9,28E5644407000046,test,75.750,75.750,75.750,F,,,
2011-02-03 11:10:27,1296731427,9,28E5644407000046,test,75.688,75.625,75.750,F,,,
2011-02-03 11:09:27,1296731367,9,28E5644407000046,test,75.625,75.625,75.750,F,,,
```

Parameter	Description	Works With
ch	Channel number 1-40. If present, filters for a particular channel. Analogs are mapped to channels 1-8, sensors are mapped to channels 9-40.	history.csv
cnt	If present, device will return "cnt" latest lines.	history.csv or eventlog.*
st	Start time in unix time format. This will limit number of lines returned.	history.csv or eventlog.*
et	End time in unix time format. This will imit number of lines returned.	history.csv or eventlog.*
uk1	User Key 1. Up to 32 characters. This key will be returned ukey1 column.	history.csv
uk2	User Key 2. Up to 32 characters. This key will be returned ukey2 column.	history.csv
uk3	User Key 3. Up to 32 characters. This key will be returned ukey3 column.	history.csv

Note: Total GET parameters string cannot be longer then 100 characters.

10.2   User Profiles

Clicking **User Profiles** gives you access to modify the default username and password, and to edit the administrator profile and create up to 9 additional unique user profiles, each with different access rights to the NetGuardian DIN's web interface.

Fig. 10.4 *Configure access privileges for users in the User Profile screen*

To create or edit any of the 10 user profiles (including the Admin), click the **Edit** button. From there, you can change all configurable settings for a user profile.

	User Profile
Suspend this Profile	If this box is checked, the profile will not be able to access the NetGuardian DIN.
Username	Enter a username or a user description
Password	Enter a unique user password **Note:** All passwords are AES 128 encrypted.
Confirm Password	Re-enter the password.
	Access Rights
Check all	Enables all Access Rights
Edit logon profiles	Enables the user to add/modify user profiles and password information.
Write Config (change unit configuration)	Enables the user to change the unit config by accessing the **Write** feature in the control menu.
View monitor pages	Allows the user to access Monitor menu options.
Send relay commands	Allows the user to send commands to operate the device's control relays.
TTY access (access via Craft port or via Telnet)	Grants the user access to the unit via TTY interface (via craft or telnet).
Initialize config to factory defaults	Allows the user to use the **Initialize** option in the **Device Access** menu, resetting the NetGuardian DIN to factory default settings. All user settings will be lost. **Note:** If you want to initialize, but preserve the Ethernet settings only, check the "Preserve Ethernet Settings" box.
Upload new firmware, or config	Allows the user to upload firmware or backed-up configuration files.
Get audit log	Allows the user to access the Audit Log (**Get Log** command).
Purge (delete) audit	Allows the user to deletes the existing audit log.

User Profile	
log	
Get (backup) config	Backs-up all user profile configuration settings.
Get and delete analog history	Allows the user to access and delete the analog and sensor history.

User profile field descriptions

10.3   Ethernet

The **Edit** > **Ethernet** menu allows you to define and configure Ethernet settings.

Fig. 10.5 *The Provisioning > Ethernet menu*

Ethernet Settings	
MAC Address	Hardware address of the NetGuardian DIN. (Not editable - For reference only.)
Host Name	Used only for web browsing. Example: If you don't want to remember this NetGuardian DIN's IP address, you can type in a name is this field, such as "MyNetGuardian DIN". Once you save and reboot the unit, you can now browse to it locally by simply typing in "MyNetGuardian DIN" in the address bar. (no "http://" needed).
Enable DHCP	Used to turn on Dynamic Host Connection Protocol. NOT recommended, because the unit is assigned an IP address from your DHCP server. The IP you've already assigned to the unit becomes inactive. Using DHCP means the unit will NOT operate in a T/Mon environment.
Unit IP	IP address of the NetGuardian DIN.
Subnet Mask	A road sign to the NetGuardian DIN, telling it whether your packets should stay on your local network or be forwarded somewhere else on a wide-area network.
Gateway	An important parameter if you are connected to a wide-area network. It tells the NetGuardian DIN which machine is the gateway out of your local network. Set to 255.255.255.255 if not using. Contact your network administrator for this info.
DNS Server 1	Primary IP address of the domain name server. Set to 255.255.255.255 if not using.
DNS Server 2	Secondary IP address of the domain name server. Set to 255.255.255.255 is not using.

Advanced TCP Settings	
Force Max TCP Window Size	The defined TCP window size is used.
Maximum TCP Window Size	Sets the TCP receive window size.

Note: DNS Server settings are required if a hostname is being used for ping targets.

10.4   Serial Port

The **Provisioning > Serial Port** menu allows you to change settings depending on the port type of your NetGuardian DIN. From this menu, you can select a mode of operation and enable reach-through serial port functionality.

Fig. 10.6 *The Provisioning > Serial Ports menu*

Location	
A reminder that your primary serial port is located on the back of the NetGuardian DIN chassis.	
Port Configuration	
Port Type	Select the serial port for your build of the NetGuardian DIN. Choose from 232, 485...
Baud, Parity, and Stop Bits	Select the appropriate settings from the drop-down menu.
RTS Head	Only used if your NetGuardian DIN was built with a 202 modem. The most commonly used value is 30.
RTS Tail	Only used if your NetGuardian DIN was built with a 202 modem. The most commonly used value is 10.
Reach-Through	
Enable Reach-through	Checking this box enables the port to be used as a terminal server. Most commonly used to Telnet through the port over LAN to a hub, switch, or router. From a command prompt, type the following *(note the spaces between each entry)*: telnet [IP address] [port] **Example**: telnet 192.168.1.100 3000
Port	Port number used for reach-through to a serial device.
Type	Select TCP or UDP traffic to be passed through to a serial device.

10.5   SNMP

The **Provisioning** > **SNMP** menu allows you to define and configure the SNMP settings.

SNMP

Global Settings	
Get Community	dps_public
Set Community	dps_public
Read and Write Access	Access disabled
SNMPv3 Engine ID	80000a7a03001081008d5e

SNMPv3 Users					
Id	**SNMPv3 Username**	**Auth Type**	**Auth Pass**	**Priv Type**	**Priv Pass**
1		No Auth		No Priv	
2		No Auth		No Priv	
3		No Auth		No Priv	

Save

Fig. 10.8 *SNMP Menu*

Global Settings	
Get Community	Community name for SNMP requests.
Set Community	Community name for SNMP SET requests.
Read and Write Access	This field defines how the NetGuardian DIN unit may be accessed via SNMP. This can be set to the following: • Access Disabled- Restricts all access to unit via SNMP • SNMPv2c only- Allows SNMPv2c access only • SNMPv2c and SNMPv1-Only- Allows SNMPv1 and SNMPv2c access • SNMPv3, SNMPv2c and SNMPv1- Allows SNMPv3, SNMPv2c and SNMPv1 access
SNMPv3 Engine ID	Specifies the v3 Engine ID for your NetGuardian device. DPS recommends using the default ID for the unit, which is automatically generated by the unit.The default ID is generated according to RFC3411 and is based on the unit's unique MAC address and DPS Telecom's SNMP enterprise number. **Note:** To have the unit generate a unique Engine ID, clear the **v3 Engine ID** field and press the **Submit** key.

Fields in the Provisioning > SNMP settings

10.5.1 RADIUS

RADIUS (Remote Authentication Dial In User Service) is an industry-standard way to manage logins to many different types of equipment in one central location. The NetGuardian DIN connects to your central RADIUS server. Every time a device receives a login attempt (usually a username & password), it requests an authentication from the RADIUS server. If the username & password combination is found in the server's database, an affirmative "access granted" reply is sent back to the unit device, allowing the user to connect.

Fig. 10.9 *RADIUS configuration screen*

Fig. 10.10 *RADIUS server prompt for Username **and** Password.*

Global Settings	
Retry	Enter the number of times the RADIUS server should retry a logon attempt
Time-out	Enter in the number of seconds before a logon request is timed out
Servers 1 / 2	
IPA	Enter the IP address of the RADIUS server
Port	Port 1812 is an industry-standard port for using RADIUS
Secret	Enter the RADIUS secret in this field

After successfully entering the settings for the RADIUS server, the NetGuardian Web Browser will prompt users for both a Username and Password, which will be verified using the information and access rights stored in the RADIUS database.

RADIUS logons **are** case-sensitive. If the RADIUS server is unavailable, local login will be used. Also, the "dictionary.dps" files (included on the Resource Disk) needs to be loaded on the RADIUS server for access-right definition. If RADIUS is enabled on the NetGuardian, the local authentication will not be valid unless the RADIUS server is unreachable.

10.6   Notifications

From the initial **Provisioning** > **Notifications** menu, you will see which of the 8 notifications are enabled, their server, and schedule. Click on the **Edit** link for one of the notifications to begin configuration.

Once you've chosen which notification you want to setup, check the **Enable Notification** to turn it "on." Then choose a notification method, either email, SNMP, voice call, or TRIP Dialup (T/Mon).

10.6.1 Notification Settings

1. Email Notification Fields

Fig. 10.11 *Editing Email Notification Settings*

Email Notification	
SMTP Server IP or Host Name	The IP address of your email server.
Port Number	The port used by your email server to receive emails, usually set to 25.
Use SSL	Check this box to use SSL encryption. Currently this feature has been tested with Gmail. To send with Gmail SMTP server, do the following: • SMTP Server IP or Host Name should be set to "smtp.gmail.com" • Port number must be set to 465. • SMTP authentication radio button must be selected. • User name and password (below under "How to Authenticate") are the user name and password for the Gmail account in use.
"From" E-mail Address	Displays the email address (defined in the Edit menu > System) that the NetGuardian DIN will send emails from. Not editable from this screen.
"To" E-mail Address	The email address of the person responsible for this NetGuardian DIN, who will receive email alarm notifications.
User Name	User name for the Gmail account being used.
Password	Password for the Gmail account being used.

Note: If you want to send authenticated emails, click the appropriate radio button. If you enable POP authentication, you will have to enter the relevant authentication information the fields below.

2. SNMP Notification Fields

Fig. 10.12 *Editing SNMP notification settings*

SNMP Notification	
SNMP Trap Server IP	The SNMP trap manager's IP address.
Trap Port No.	The SNMP port (UDP port) set by the SNMP trap manager to receive traps, usually set to 162.
Trap Community	Community name for SNMP TRAP requests.
Trap Type	Indicate whether you would like to send SNMP v1, v2c or v3 traps.

3. TRIP Dialup (T/Mon) Notification Fields

Fig. 10.13 *Editing Call notification settings*

Call Notification	
T/Mon Phone Number	Enter the phone number for your T/Mon unit
Only dial if DCP poller inactive alarm is set	Check this box if you want the Netguardian to only dial if the DCP poller inactive alarm is set

Note: T/Mon will need to have a "^" at the begining of the dialing string for data calls to function properly (i.e.. ^15594541600).

4. Syslog Notification Fields

Fig. 10.14 Editing Syslog Notification Settings

Syslog Notification	
Syslog Server IP or Host Name	The IP address of your Syslog Server
Port	The port used by your Syslog Server to receive Syslog notifications, usually set to 514
Priority Code	**Facility**: Used to determine the type of program that is logging the message
	Severity: Used to determine the severity of the message being logged.

5. rCell SMS Notification Fields

Fig. 10.15 Editing rCell SMS Notification Settings

rCell SMS Notification	
rCell IP Address	The IP address of your rCell Unit
Port	The HTTP port on your rCell (usually 80, login to your rCell as below to verify)
SMS Destination Number	The phone number to send the SMS to
rCell User Name	The user name you use to login to the rCell
rCell Password	The password you use to login to the rCell
Confirm Password	Retype the above password

Important: For the notification method to work, you must login to the rCell and enable HTTP via LAN (shown below)

Fig. 10.16 *Enabling rCell HTTP access for NetGuardian*

6. Breakdown of Example SMS Notification

Site Name (truncated to 20 characters)

Site Location (truncated to 20 characters)

NetGuardian_DIN, Fresno, CA

Desc: MjU: Analog 0-60V — *Alarm Description* (truncated to 25 characters)
Status: Alarm — *Alarm Status*
Reading: 0.138 VDC — *Analog Reading* that triggered threshhold.
Time: Dec 13, 2016 17:02:47

Ref: 7.35 — *Time event* occured.

Display and *Point Reference*. This alarm is **Display 7**, **Point 35**.

Note: The NetGuardian will consider the SMS sent when it has been relayed to the rCell. If the rCell fails to send the message (for example, if there is no signal or SIM card), the failure will appear on the rCell's

interface; see *Fig. 10.17*.

Fig. 10.17 *Example of rCell SMS fail due to no cell signal.*

10.6.2 Schedule

The notifications scheduling menu is where you will tell the NetGuardian DIN exactly which days and times you want to receive alarm notifications. You set 2 different schedules for each.

Fig. 10.18 *The Schedule creation screen*

Notification Scheduling	
Days of the week	From either Schedule 1 or 2, check which days you want to receive notifications.
Any Time	Select this is if you want to receive alarm notifications at any time for the day(s) you've selected.
Notification Time	Tells the unit to only send notifications during certain hours on the day(s) you've selected.

10.7   Alarms

Discrete alarms are configured from the **Provisioning** > **Alarms** menu. Descriptions for the alarm points, polarity (normal or reversed) and notification type(s) are defined from this menu. You also have the option to use **Basic** or **Advanced** configuration methods, explained in this section.

Fig. 10.19 *The Provisioning > Alarms menu*

Basic Alarm Configuration	
ID	Alarm ID number.
Description	User-definable description for the discrete alarm point.
Rev (Reverse)	Reverse: Check this box to reverse the polarity of the alarm point. Leaving this option un-checked means a normally open contact closure is an alarm. When polarity is reversed, a normally closed alarm point is clear when closed.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for that alarm point.
Advanced Alarm Configuration (Advanced>>)	
On Set	User-definable description (condition) that will appear for the discrete alarm input on Set. Example: "Alarm".
On Clear	User-definable description (condition) that will appear for the discrete alarm input on Clear: "Example: "Alarm Cleared".
Qual. Time (Qualification Time)	The length of time that must pass, without interruption, in order for the condition to be considered an Alarm or a Clear.
Qual. Type (Qualification Type)	Allows you to choose whether you want to apply the Qualification Time to the alarm Set, Clear, or Both.

10.8   Alarm Echo

Echo alarms are the first 16 alarms and 10 controls information of other unit.
For example, if a unit 1 has alarm 1 active, the unit 2 echo alarm 1 will be active.

Alarms Echo

Alarms Echo			Rev.	1	2	3	4	5	6	7	8
Id	**Description Display Map**		☐	☐	☐	☐	☐	☐	☐	☐	☐
1	Echo - Fresno office AC Fail	Advanced<<	☐	☐	☐	☐	☐	☐	☐	☐	☐

On Set:	Qual. Time: 0sec	Message: Alarm
On Clear:	Qual. Time: 0sec	Message: Clear

Id	Description		Rev.	1	2	3	4	5	6	7	8
2	Echo - Push Button - Gun Hill Door Strike	Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
3		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
4		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
5		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
6		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
7		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
8		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
9		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
10		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
11		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
12		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
13		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
14		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
15		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
16		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
17	Echo - AC Loss or Low Battery, Fresno office	Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
18	Echo - System Summary Alarm, Fresno office	Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
19	Echo - AC Loss or Low Battery, Airport	Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
20	Echo - System Summary Alarm, Airport	Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
21		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
22		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
23		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
24		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
25		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐
26		Advanced>>	☐	☐	☐	☐	☐	☐	☐	☐	☐

Save

Alarm Echo in the Provisioning menu.

10.9   Persistent Alarm Counters

You can configure your NetGuardian DIN to count how many times a discrete alarm or control relay input turns on. Persistent alarm counters can be provisioned under the **Provisioning > Persistent Alarm Counters** menu. This can be used, for example, if you have a sensor which detects lighting strikes, and you would like to count how many times lightning has struck since the alarm counter was last configured.

Fig. 10.20 The Provisioning > Persistent Alarm Counters menu

Ex. In the above picture, Counter 1 will log pulses for display 1.18, or Control #2. Counter 2 will count pulses for display 1.1, or Discrete Alarm #1. Counter 3 would log pulses for Discrete Alarm #3, but it is not enabled.

Basic Counter Configuration	
ID	Counter ID number.
Enab	Enable and disable the counter.
Description	Full description of counter.
Logged Point	
Display	Which display the counter will monitor. (See **Display Mapping** in **Reference** section, or click on **Display Map** at the top of the menu in the web interface)
Point	Which point on the above display will be counted.
Logging Config	
Counter Start Value	The starting value of the counter before it begins incrementing (usually zero).
Counter Wrap Value	How many times the alarm will be counted before resetting to zero (max 65535).
Limit Log Writes	Checking this box causes the alarm count to be held in RAM, and will only be written to NVRAM when the NetGuardian is rebooted by the user. **This means that if your NetGuardian experiences an unexpected loss of power, it will lose its count.** This can occur if the mains power goes out, or if the NetGuardian is unplugged during operation. Un-checking this box ensures that each count will be saved, at the cost of increased wear on the NetGuardian's NVRAM.

10.10 Controls

The NetGuardian DIN's control relays can be configured in the **Provisioning** > **Controls** menu. You can enter your own description for these relays and designate them to a notification device(s).

Fig. 10.21 *The Provisioning > Controls screen*

Basic Controls Configuration	
ID	ID number for the control relay.
Description	User-definable description for the NetGuardian DIN's control relay.
Derived Description	Formula to control relay operation.

	Control relays and virtual alarms can be created from derived formulas using the following operations: **_OR** : Set the current operation to OR. **_AN** : Set the current operation to AND. **_XR** : Set the current operation to XOR. **D** : Tag to change the active display number. . : Used like a comma to delimit numbers. - : Used to specify a range of points.
Momentary Time	Control on time (in milliseconds) when you execute the MOM command. Max limit of 600 seconds.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for the control relay.
Strobe Relay During Latch	Feature to strobe a relay. While relay is latched, it will oscillate between latched and released with momentary time frequency. This toggle will create a led blink.

10.11 Analogs

The NetGuardian DIN's multi-purpose analog inputs measure continuous ranges of voltage or current. Analog alarms are typically used to monitor battery voltage, charging current, temperature, humidity, wind speed, or other continuously changing conditions. To configure a user analog, simply fill in your description, thresholds, and other fields listed in the table below, then click **Save**.

Fig. 10.22 *The Provisioning > User Analogs menu*

Note: Analog channels 7 and 8 are for internal voltage monitoring (On a single power input build, channel 7 is unused.)

User Analogs	
Default monitoring to gauge view	Checking this box sets the default view in the **Monitor>User Analogs** menu to the gauge view.
Enab (Enable)	Checking the box in the **Enab** column enables monitoring of the analog channel.
Description	User-definable description for the analog channel
Rev	Checking the reverse button changes negative values to positive, and positive values to negative.
Notifications	Check which notification device(s), 1 through 8, you want to send alarm notifications for this analog input.
Details	
Record Freq	The frequency with which the NetGuardian will record the analog reading
Deadband	The additional qualifying value the NetGuardian requires above/below your alarm thresholds in order to set an alarm.
Units	The unit(s) of measurement reported by a connected analog input.
Low ref and High Ref	The low and high values for scaling voltage to your display units.
MjU (Major Under) MnU (Minor Under) MnO (Minor Over) MjO (Major Over)	Threshold settings that, when crossed, will prompt the NetGuardian to set an alarm. Recorded values less than an under value or greater than an over value will cause alarms.
Push-to-talk: Enable	Checking this box enables Push-to-Talk feature for this analog.
Discrete Input	Assign the alarm point associated with this analog.
Qual. Time (ms)	Length of time, in milliseconds, that an alarm point must be set before before an analog can post.
Analog Gauge Type	Select the type of analog gauge represented in the **Monitor>User Analogs>Gauge View** menu

10.12 Sensors

D-Wire Sensors
The NetGuardian DIN supports up to 32 daisy-chained D-Wire sensors via its D-Wire input. Sensors connected to the NetGuardian DIN will appear on the web interface. The background color of the ROM field informs the user of the sensor's configuration state.

Also the NetGuardian DIN's first D-Wire sensor used to monitor the internal temperature. The internal temperature sensor measures a range of -40° F to 180° F (-40° C to 82.2° C) within an accuracy of about ± 2°.

Basic configuration for the NetGuardian DIN's D-Wire temperature sensors can be accomplished from the **Provisioning** > **Sensors** menu. From this screen, you can configure D-Wire sensors, select notification devices, and set thresholds.
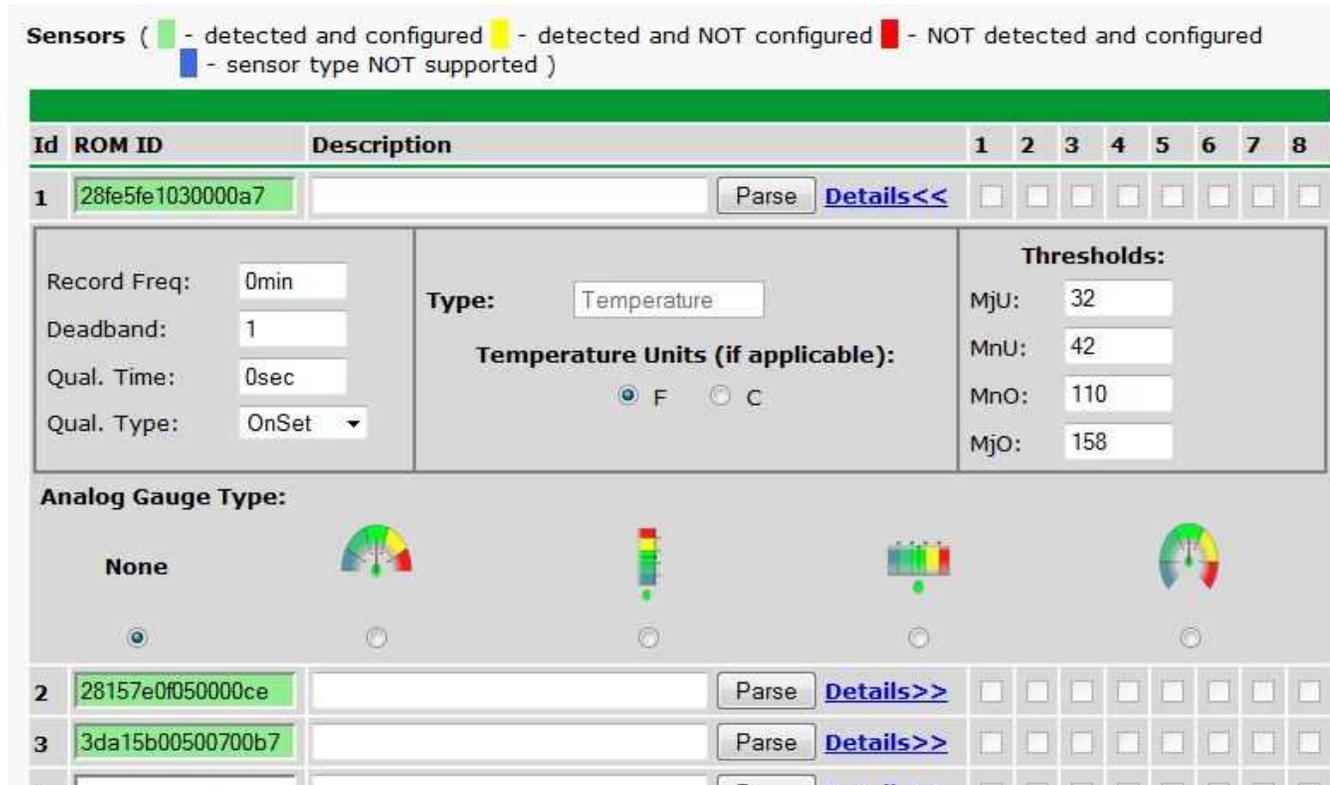
Fig. 10.22 The Provisioning > Sensors menu

Basic Sensor Configuration	
ID	Sensor ID number.
ROM ID	The ID number found on the sticker of the temperature sensor node. Your NetGuardian DIN will automatically detect the sensor ID when you plug a sensor into the unit. The color of the sensor ID field will tell you the status of the connected sensor. **Green** - The sensor is connected and properly configured. **Yellow** - The sensor is connected but has not yet been configured (fill in your configuration fields and click **Save** to configure the sensor). **Red** - The sensor is not detected and configured (i.e. a previous configured

	sensor is no longer connected). **Blue** - The sensor is not supported by the NetGuardian DIN. To reconfigure or disable the Sensor ID, simply delete any data in this field and click **Save**. The unit will refresh the sensor ID on that channel.
Description	User-definable description for the sensor channel.
Parse	Checks to see if the **Description** field contains a valid equation.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for that alarm point.
Advanced Sensor Configuration (Details>>)	
Record Freq	The amount of time, in minutes (min) or seconds (s), between each recorded sensor value.
Deadband	The amount (in native units) that the channel needs to go above or below a threshold in order to cause an alarm.
Qual Time (Qualification Time)	The length of time that must pass, without interruption, in order for the condition to be considered an Alarm or a Clear.
Qual. Type (Qualification Type)	Allows you to choose whether you want to apply the Qualification Time to the alarm Set, Clear, or Both.
Thresholds	These settings are set to indicate the severity of the alarm depending on which threshold values have been passed. Enter values for Major Under (MjU), Minor Under (MnU), Minor Over (MnO), and Major Over (MjO).
Analog Gauge Type	Select the color-coded gauge that best represents your data. Selecting **None** will disable the analog gauge and only a numerical representation of the value will be displayed under **Monitor** > **Sensors**.

Note: Before plugging in any additional D-Wire Sensors, set up the internal sensor.

Script Sensors
A Script Sensor can be setup by entering a script type in the sensor ID field. The following types are currently supported:

~count - The equation will be evaluated continuously. If the evaluation changes at any point, the sensor's value increases by an increment of 1. This mode can be useful for counting the number of times a discrete input toggles.

Evaluation Sensor; every tenth of a minute (6 seconds).
~evalMt - The equation is evaluated every 6 seconds and its result becomes the sensor's value.

Evaluation Sensor; every minute.
~evalMn -   The equation is evaluated every 60 seconds and its result becomes the sensor's value.
        Interval counter.

Interval Sensor
~intCnt - Sensor value will increment when the associated input's pulse length (high or low) is within a set interval. Example: **D5 V1000>V60000<** means the sensor value will increment when a 1ms to 60ms pulse is detected on Discrete Input 5. This is useful for frequency detection/tracking.

A Script Sensor is configured to evaluate Reverse Polish Notation equations. A data token in an equation

can represent a discrete alarm, analog reading, sensor reading, relay status, system alarm status, or a constant value. The format for a token in an equation must be a data type followed by an index (for example: Discrete Input 1 in an equation would be represented as "d1", Analog Channel 3 would be "a3", etc.). Each token is typically followed by another token or an operator. The equations are entered in the description field for the Script Sensor.

Valid data types:	
d	Discrete Input
a	Analog Channel
r	Relay State
n	Sensor
v	Positive Integer Constant
s	System Alarm

Valid operations:	
+	Addition
-	Subtraction
*	Multiplication
/	Division[1]
>	Greater than
<	Less than
|	Conditional Halt[2]

1. Division is NOT executed if the denominator's absolute value is less than 1!
2. An equation is evaluated until it reaches the Conditional Halt. If the running value at that point is zero, then the evaluation stops, otherwise the evaluation continues as a new equation.

How equations are evaluated:
Calculations are performed from left-to-right until the end of the equation is reached. As the equation is parsed, each token's value is pushed onto a stack until an operator is found. When an operator is found, the previous 2 values are popped from the stack and are used to perform the operation (the first item popped is the SECOND operand). The result of the operation is then pushed onto the stack. This repeats until the end of the equation is reached. An equation is valid only if there is exactly ONE item left in the stack when the end of the equation is reached.

Example of how an equation is evaluated:

Equation: a8 a5 a6 + * a4 -

Input	Operation	Stack	Comment
a8	Push value	a8	
a5	Push value	a5 a8	
a6	Push value	a6 a5 a8	
+	Add	(a5+a6) a8	Pop a6 and a5, add them, push result to stack
*	Multiply	a8*(a5+a6)	Pop (a5+a6) and a8, multiply them, push result to stack
a4	Push value	a4 a8*(a5+a6)	
-	Subtract	a8*(a5+a6) - a4	Pop a4 and a8*(a5+a6), subtract them, push result to stack

In this example, after the subtraction there is only ONE item left in the stack (which is the result of all of the previous computations), making this a valid equation.

10.12.1HVAC Monitoring

Temperature / Air Flow sensors can be used to monitor HVAC health. Enabling HVAC Monitoring on this sensor adds the extra fields below.

Fig. 10.23 *Sensor with HVAC Monitoring enabled.*

HVAC Monitor Mode	
Air Flow Qual Time	The time the HVAC has between starting and reaching operational Air Flow and Vent Temperature
Mate	The ROM ID for the temperate sensor in the same package as the Air Flow sensor
Air Flow Thresholds	Set MjU to -20
	Set MnU to -10
	Set MnO to a small, positive value. Once the air flow gets to that value, the HVAC will be considered starting.
	Set MjO to a higher value. This value will be the minimum amount of airflow required to be considered operational. An alarm will trigger if this threshold is not passed by the Air Flow Qual Time expires.
Temperature Thresholds	For a cooling HVAC, the vent temperature should reach between Cooling Under and Cooling Over.
	For a warming HVAC, the vent temperature should reach between Heating Under and Heating Over.
	An alarm will trigger if one of the above thresholds is not reached before Air Flow Qual

Time expires.

Note: When in HVAC Monitor Mode, the Temp sensor *Qual Type* is defaulted to *On Clear,* and the Air Flow sensor *Qual Type* is defaulted to *On Both.*

Setting up a Temperature/Air Flow Sensor as an HVAC Monitor:
1. In Provisioning->Sensors, open the Details menu of the airflow sensor that is going to be used as the HVAC Monitor.
2. Check the 'HVAC Monitor' checkbox
3. *Save* and *Write* changes. This will expand menu to display HVAC Monitor Settings.
4. Set Qual Time to allow the HVAC unit adequate time to start up (ex: 10sec).
5. Set the thresholds to the following:
    -   MjU = -20
    -   MnU = -10
    -   MnO = 10
    -   MjO = 75

    -Though the values listed above will work in most situations, they can be adjusted as needed.
3. Return to Provisioning-> Sensors->details menu of the airflow sensor being used as the HVAC Monitor and confirm that the new field named 'Mate' that has appeared underneath the HVAC monitor checkbox contains the ROM ID of the temperature sensor that is also being used to monitor HVAC health

10.13 Ping Targets

The **Provisioning** > **Ping Targets** menu allows you to configure the Description, IP Address, and Notification Devices for each of your ping targets.

Ping Targets

Id	Enab	Description Display Map	Server (IP or Hostname)	1	2	3	4	5	6	7	8
1	☐	Cisco Router	126.102.218.3	☐	☐	☐	☐	☐	☑	☐	☐
2	☐	Ethernet Switch 1	126.102.218.24	☐	☐	☐	☐	☐	☑	☐	☐
3	☐	Ethernet Switch 2	126.102.218.12	☐	☐	☐	☐	☐	☑	☐	☐
4	☐	Ethernet Switch 2	126.102.218.14	☐	☐	☐	☐	☐	☑	☐	☐
5	☐	Router 2	126.102.218.67	☐	☐	☐	☐	☐	☑	☐	☐
6	☐	Media Converter	126.102.218.29	☐	☐	☐	☐	☐	☑	☐	☐
7	☐	Microwave Transmitter	126.102.218.90	☐	☐	☐	☐	☐	☑	☐	☐
8	☐	Cisco 15454	126.102.218.43	☐	☐	☐	☐	☐	☑	☐	☐
9	☐	Calix	126.102.218.31	☐	☐	☐	☐	☐	☑	☐	☐
10	☐	Modem	126.102.218.7	☐	☐	☐	☐	☐	☑	☐	☐
11	☐	PBX	126.102.218.15	☐	☐	☐	☐	☐	☑	☐	☐
12	☐	Proxy Server	126.102.218.39	☐	☐	☐	☐	☐	☑	☐	☐

***Fig. 10.24** The Provisioning > Ping Targets menu*

Provisioning Ping Targets	
ID	ID number for the ping target.
Enab	Check this box to enable the ping target.
Description	User-definable description for the ping target.
Server (IP or Hostname)	IP address or hostname of the device you would like to ping.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for ping target.

10.14 Modbus Devices

Modbus Interrogator Global Settings			
Modbus Poll Delay		600	ms (10 - 16000)
Modbus Poll Timeout		10	sec (1 - 255)
Send Notification on every register update		☐ **Readme**	

Device Settings Display Map

Id	Device Type	Description	
1	Modbus RTU ▾	Generac	Details>>
2	Modbus RTU ▾	PC	Details>>
3	Modbus RTU ▾	other	Details<<

Connection:	TCP ▾
IP Address:	0.0.0.0
Port:	000
Modbus address:	1
Device Register Offset:	0

Threshold Mode:	Idle/Running Thresholds: Status Register ▾

This modbus device will use a status register to determine whether the device is idle or running.
- It is recommended to set a qualification time of at least 1 minute when using this feature.
  This will ensure that the status register will be polled at least once before using new thresholds.

Device will use Device Idle Thresholds ▾ **when the status register does not match any conditions.**

Status Register: 2

	Enable	Match Type	Value
Running when:	☑	Value Equals ▾	5.00
or	☐	Value Equals ▾	0.00

4	None ▾		Details>>

Save

Fig. 10.29 Provisioning > Modbus Devices

Global Settings	
Modbus Poll Delay	Delay between Modbus polls in milliseconds.
Modbus Poll Timeout	Time duration before the Modbus repsonse time fails in seconds.
Send Notification of every register update	This option is used to send a notification whenever a Modbus register is polled. If the poll delay is too low this may cause some notifications to be lost.
Device Settings	
ID	Modbus device ID.
Device Type	Modbus device type.
Connection	TCP or Serial connection.
Host Name or IP	IP used for polling when using TCP Modbus. Unused otherwise.
TCP Port or Serial Port	TCP or physical serial port used when performing Modbus polling.
Modbus Address	Address of Modbus device.
Device Register Offset	Amount to offset "Modbus Address" by.

Threshold Mode	This will configure different threshold values based on Modbus register values. Threshold mode options:
	
	    1) "standard thresholds" - default threshold setting. Only one value of thresholds will be used
	    2) "Idle/Running Thresholds: Status Register" - device idle thresholds will be triggered based on the value of a status register.
	    3) "Idle/Running Thresholds: Point Reference" - device idle thresholds will be triggered based on the value of a point reference.

10.15 Modbus Registers

Fig. 10.30 *Provisioning > Modbus Registers*

Basic Configuration	
ID	Modbus register ID
Modbus Device	Modbus device settings used when polling.
Description	User0definable description for the Modbus register.
Notifications	Check which notification device(s), 1 through 8, you want to send alarm notifications for that Modbus register.
Details	
Function Code	
Modbus function code to use when polling device	
Event Qualification	
Qual. Time - Threshold must be crossede for this length of time before alarms is triggered. (set to 0 to deactivate)	
Qual. Type - Determines which actions Qual Time applies to.	
Recording Settings	
Stable Frequency	Frequency used when logging response history.
Register Attributes	
Register Number	Register to be polled.
Number of Bits	Number of bits used to mask the response value.
Integer/Float	Interpret response value as an integer for a float.
Unsigned/Signed	Interpret the response value as signed or unsigned.
Byte Order	Byte ordering of response from Modbus device.
Scaling	Scaling factor that the response value is multiplied by.
Units	Units displayed with the response value.
Thresholds	
MjU (Major Under) MnU (Minor Under) MnO (Minor Over) MjO (Major Over)	Threshold settings that, when crossed, will prompt the NetGuardian to set an alarm. Recorded values less than an under value or greater than an over value will cause alarms. NOTE: If the user has one of the Idle/Running threshold modes selected in Device settings then there will be two sets of thresholds displayed here. If Standard Thresholds is selected there will only be one.
Deadband	The additional qualifying calue the NetGuardian requires above/below your alarm thresholds in order to set an alarm.

10.16 System Alarms

See "Display Mapping" in the Reference Section for a complete description of system alarms.

System Alarms

Pnt	Description Display Map	Silence	1	2	3	4	5	6	7	8
33	Default configuration	☐	☐	☐	☐	☐	☐	☐	☐	☐
34	DCP poller inactive	☐	☐	☐	☐	☐	☐	☐	☐	☐
39	SNMP community error	☐	☐	☐	☐	☐	☐	☐	☐	☐
41	Notification 1 failed	☐	☐	☐	☐	☐	☐	☐	☐	☐
42	Notification 2 failed	☐	☐	☐	☐	☐	☐	☐	☐	☐
43	Notification 3 failed	☐	☐	☐	☐	☐	☐	☐	☐	☐
44	Notification 4 failed	☐	☐	☐	☐	☐	☐	☐	☐	☐

Fig. 10.31 *The Provisioning > System Alarms menu*

Editing System Alarms	
Pnt (Point)	The system alarm point number
Description	Non-editable description for this System (housekeeping) Alarm.
Silence	Check this box to choose to silence this alarm.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for that alarm point.

10.17 Timers

Enter the amount of time in seconds (sec) or minutes (m), in each value field and click **Save**.

Fig. 10.32 *The Provisioning > Timers menu*

10.18 Date and Time

Fig. 10.33 *The Provisioning > Date and Time menu*

Unit Time	
Date	Set today's date.
Time	Set the current time.
Automatic Time Adjustment (NTP)	
Enable NTP	Check this box to enable Network Time Protocol.
NTP Server Address or Host Name	Enter the NTP server's IP address or host name, then click **Sync**. Example: us.pool.ntp.org. **Note**: Make sure to configure DNS before using host name instead of IP address.
Time Zone	Select your time zone from the drop-down menu.
Adjust Clock for Daylight Savings Time (DST)	
Enable DST	Check this box to have the NetGuardian DIN observe Daylight Savings.
Start Day	Select the month, weekday, and time when Daylight Savings will begin.
End Day	Select the month, weekday, and time when Daylight Savings will end.

11 Monitoring via the Web Browser

11.1 Alarms

This selection provides the status of the base alarms by indicating if an alarm has been triggered. Under the **State** column, the status will appear in red if an alarm has been activated. The status will be displayed in green when the alarm condition is not present.

Alarms

Id	Description Display Map	State
1		Alarm
2		Clear
3		Clear
4		Clear
5		Clear
6		Clear
7		Clear
8		Clear

Click on Alarms in the Monitor menu to see if any base alarms (1-8) have been triggered.

Basic Alarm Monitoring	
ID	Alarm ID number.
Description	User-definable description for the discrete alarm point.
State	The current state of the alarm. (Clear or Alarm)

11.2   Alarm Echo

Echo alarms are the first 16 alarms and 10 controls information of other unit.
For example, if a unit 1 has alarm 1 active, the unit 2 echo alarm 1 will be active.

Alarm Echo

Id	Description Display Map	State
1	Echo - Fresno office AC Fail	Clear
2	Echo - Push Button - Gun Hill Door Strike	Clear
3		Clear
4		Clear
5		Clear
6		Clear
7		Clear
8		Clear
9		Clear
10		Clear
11		Clear
12		Clear
13		Clear
14		Clear
15		Clear
16		Clear
17	Echo - AC Loss or Low Battery, Fresno office	Clear
18	Echo - System Summary Alarm, Fresno office	Clear
19	Echo - AC Loss or Low Battery, Airport	Clear
20	Echo - System Summary Alarm, Airport	Clear
21		Clear
22		Clear
23		Clear
24		Clear
25		Clear
26		Clear

Alarm Echo in the Monitor Menu

11.3   Persistent Alarm Counters

The status of your Alarm Counters can be viewed in the **Monitor > Persistent Alarm Counters** menu. You can see whether the discrete event is currently **Set** or **Clear**, as well as the number of times that it has been set since configuration.

Persistent Alarm Counters

Id	Display	Point	Description Display Map	Point State	Pulse Counter	Config Date
1	1	18	Persistent Alarm Counter 1	Clear	1	07/02/2018
2	1	1	Persistent Alarm Counter 2	Set	1	07/02/2018
3	N/A	N/A	Persistent Alarm Counter 3	Disabled	0	07/02/2018

Note: A persistent alarm counter will record the number of alarm pulses received on a specified point from the device's display mapping. A pulse is recorded when the point is set from a clear state.

The Monitor > Persistent Alarm Counters menu

Ex. The above picture indicates that display 1.18 (control #2) is **Released**, but was at one point **Latched**, and that display 1.1 (discrete #1) is in **Alarm** for the first time since reset.
(see **Controls** for more info on control states, or **Display Mapping** for more info on how Display and Point values map to specific modules)

11.4   Controls

Use the following rules to operate the NetGuardian DIN's control:
1.   Select **Controls** from the **Monitor** menu.
2.   Under the **State** field, you can see the current condition of the control.
3.   To issue the control, click on a command (**OPR** - operate, **RLS** - release, or **MOM** - momentary)
4.   If a Derived Description is assigned to a control ID, the command buttons for that control ID will be disabled.

Controls

Id	Description Display Map	State	Command		
1		Released	OPR	RLS	MOM
2		Released	OPR	RLS	MOM
3		Released	OPR	RLS	MOM
4		Released	OPR	RLS	MOM

View and operate control relays from the Monitor > Controls menu

Control Relay Operation	
ID	ID number for the control relay.
Description	Description for the NetGuardian DIN's control relay defined in the Provisioning > Controls menu.
State	Status of the control relay. Can either be **Released** or **Latched**.
Command	**OPR** - Latch the relay. **RLS** - Release the relay. **MOM** - Momentarily latch the relay, then automatically release the relay. The duration of the latch is defined in the Provisioning > Controls menu.

11.5 Analogs

If you requested your DIN to be built with an analog relay, your 8 analog inputs will be displayed under **Monitor > Analogs** as shown. Otherwise, you will see "Hardware not supported!". Note that channels 7 and 8 are reserved for internal power monitoring.

User Analogs (Gauge View)

Id	Description Display Map	Thresholds	Reading	
1		Disabled	0.00	VDC
2		Disabled	0.00	VDC
3		Disabled	0.00	VDC
4		Disabled	0.00	VDC
5		Disabled	0.00	VDC
6		Disabled	0.00	VDC
7	Power Input B	Disabled	0.00	VDC
8	Power Input A	Disabled	0.00	VDC

Monitor > Analogs

11.6 Sensors

This selection provides the status of the system's analog channels by indicating if an alarm has been triggered. The **Monitor > Sensors** screen provides a description of each analog channel, the current reading, the units being read, and alarm conditions (major under, minor under, major over, minor over) according to your temperature settings. If configured under **Provisioning > Sensors**, your analog values will be displayed as a graphical gauge. Selecting **Table View** will display a non-graphical interface of your values.

User Analogs (Table View)

No.	5		No.	6	
Enab	Yes		Enab	Yes	
Units	VDC		Units	VDC	
MjU			MjU	X	
MnU			MnU	X	
MnO			MnO		
MjO			MjO		

24.33 VDC
Power Input A

0.00 VDC
Power Input B
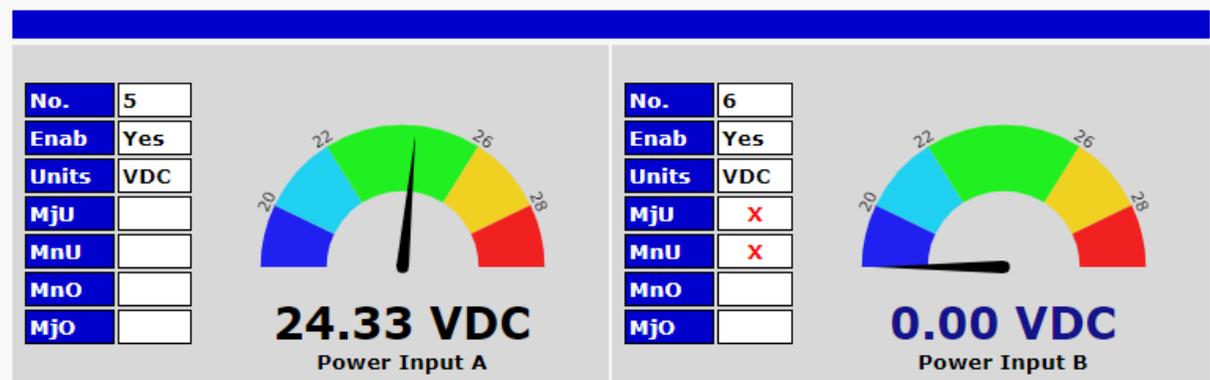
The Monitor > Sensors menu

11.6.1 HVAC Monitoring

When using a Temp/Air Flow sensor for HVAC Monitoring, the HVAC Air Flow sensor monitor section will display 4 thresholds instead of one.

Alarm Descriptions	
HVAC Air Flow	This alarm will tell you if there is air flow coming from the HVAC unit.
(HVFail) HVAC Failed	This alarm will trigger if the temperature is not within Heating or Cooling range by the time Air Flow Qual Time expires, or if during operation Temperature goes out of Heating or Cooling range.
(AFFail) HVAC Air Flow Failed	This alarm will trigger if air flow gets to Minor Over but doesn't reach Major Over by Air Flow Qual Time.
(MNotDet) Air Flow Sensor Mate Not Detected	This alarm will trigger if the mated Temp sensor is not detected.

11.7 Ping Targets

Ping Targets can be viewed by going to **Monitor** > **Ping Targets**. Here you can view the state (either **Clear** or **Alarm**) for each of your configured Ping Targets.

Id	Description Display Map	State
1	Cisco Router	Clear
2	Ethernet Switch 1	Clear
3	Ethernet Switch 2	Clear
4	Ethernet Switch 2	Clear
5	Router 2	Clear
6	Media Converter	Clear
7	Microwave Transmitter	Clear
8	Cisco 15454	Clear
9	Calix	Clear
10	Modem	Clear
11	PBX	Clear
12	Proxy Server	Clear

View the status of Ping Targets from the Monitor > Ping Targets menu.

11.8   Modbus Registers

Modbus Registers

Id	Description Display Map	Thresholds	Reading
1	Fuel Level Low Warning	Not Detected	
2	Engine Coolant Temp Low Warning	Not Detected	
3	Battery Charger Failure	Not Detected	
4	Engine Stop Shutdown	Not Detected	
5	Generator Not in Auto	Not Detected	
6	Engine Speed High Shutdown	Not Detected	
7	Engine Oil Pressure Low	Not Detected	
8	Engine Coolant Temp High Shutdown	Not Detected	

Monitor > Modbus Registers

This selection provides the status of the Modbus registers being polled by the unit. The Monitor > Modbus Registers screen provides a description of each Modbus register, the current response value along with the units, and alarm conditions (major under, minor under, minor over, major over) according to your settings.

11.9   System Alarms

System alarms are not-editable, housekeeping alarms that are programmed into NetGuardian DIN. The **Monitor** > **System Alarms** screen provides the status of the system alarms by indicating if an alarm has been triggered. Under the **State** column, the status will appear in red if an alarm has been activated. The status will be displayed in green when the alarm condition is not present.

See "Display Mapping" in the Reference Section for a complete description of system alarms.

Pnt	**Description Display Map**	**State**
33	Default configuration	Clear
34	DCP poller inactive	Clear
39	SNMP community error	Clear
41	Notification 1 failed	Clear
42	Notification 2 failed	Alarm
43	Notification 3 failed	Clear
44	Notification 4 failed	Clear
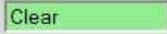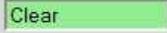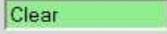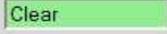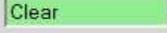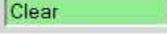
View the status of System Alarms from the Monitor > System Alarms menu.

11.10 Graph

The Graph section of the monitor menu lets you build a graph of past analog and sensor measurements, which gives you a visual indication of data over time and points out trending values. To create your Graph, specify the Channel (Analogs 1-8 or Sensors 1-32), Group Interval (1-120 minutes, hours, days, or weeks), the Group Function (Average, Min, Max), and Start & End Times. Once you have entered all of the desired values, click "Build Graph."

Provision the Channels, Group Interval, Group Function and more - all from the Graph Parameters section of the web browser interface.

Your graph will appear on the next screen. This graph is Adobe Flash-based and allows you to mouse over the lines to quickly view measurements (date, time, and value) within their context of the overall graphing trend. Below the graph is a full textual list of all indexed points with their dates and values.
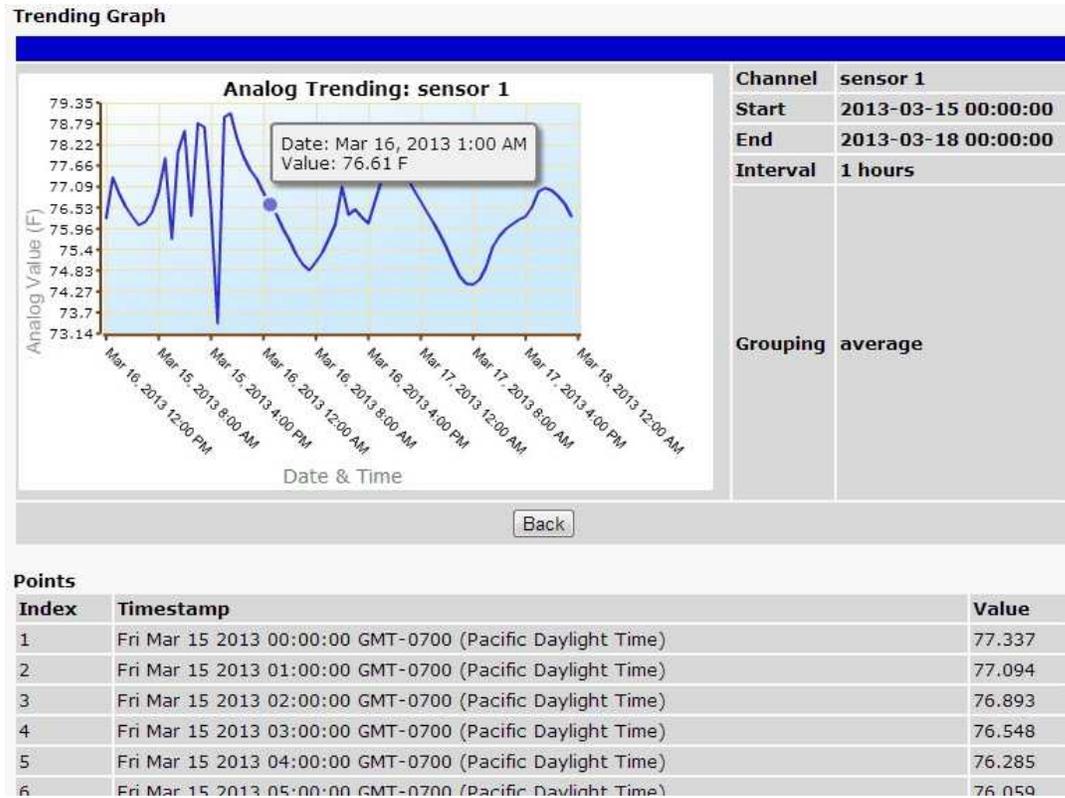
Specify your parameter values and build an interactive graph based on the alarm point history.

12 Device Access Descriptions

The **Device Access** options, listed in pink on the left side of the web interface, provide options for generating reports, updating the NetGuardian DIN's firmware, and rebooting the unit. Click any of the options under **Device Access** to perform the desired action.

The control menu is located in the bottom left of the web interface

Device Access Option	Description
Backup Config	Backs up the units configuration settings
Read	Reads a configuration file from the unit
Write	Commits all changes made in the web interface to the NetGuardian DIN's non-volatile memory
Initialize	Sets the unit's configuration to factory default values
Get Log	Opens the NetGuardian DIN's event log in Notepad (or another plain text editor).
Purge Log	Deletes the NetGuardian DIN's event log history.
Reboot	Reboots the NetGuardian DIN.

13 Backup Configuration

With the NetGuardian DIN you can backup your current configuration from the Web Interface. These configuration files can then be uploaded later, or uploaded to other NetGuardian DIN units.

The Backup Config tab is located in the Device Access menu shown above.

How to backup your current configuration:
1. Click the Backup Config tab from the Device Access menu.
2. When prompted by your web browser, download the file to your desktop or other location on your computer.
3. Now your configuration should be saved. If you need to upload a configuration, follow the steps below.

Fig. 13.2 *To upload your configuration file, click on **Upload** on the top right corner of the web interface*

How to upload a saved configuration:
1. Click the upload button at the top right corner of the Welcome screen.
2. Click the Browse... button
3. Browse to the location of the .bin file from the steps above.
4. Select that .bin file and press the Upload button.
5. You should now have the same configuration settings loaded from when you saved the .bin file above.

14 Firmware Upgrade

To access the **Firmware Load** screen, click on the **Provisioning** > **System** menu. At the bottom of this screen, click the **Restore Configuration** link located in the **System Controls** section.

*To upload firmware, click on **Upload** on the top right corner of the web interface*

At the **Firmware Load** screen, simply browse for the firmware update you've downloaded from www.dpstele.com and click **Load**.
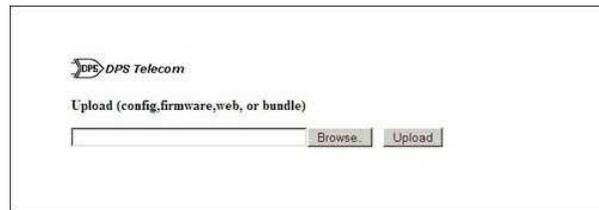
Browse for downloaded firmware upgrade

15 Reference Section

15.1 Display Mapping

Display Mapping

Display	Point	Description
	1-16	Discrete Alarms 1-16
	17-26	Controls 1-10
	27-32	Undefined
	33	Default configuration
	34	DIP Switch Config
	35	MAC Address Not Set
	36	IP Address Not Set
	37	LAN Hardware Error
	38	SNMP processing error
	39	SNMP community error
	40	LAN TX packet drop
	41	Notification 1 failed
	42	Notification 2 failed
	43	Notification 3 failed
	44	Notification 4 failed
	45	Notification 5 failed
	46	Notification 6 failed
Display 1	47	Notification 7 failed
	48	Notification 8 failed
	49	NTP failed
	50	Timed tick
	51	Serial RCV Q full
	52	Dynamic memory full
	53	Unit reset
	54	DCP poll inactive
	55	TRIP error
	56	No dial tone
	57	Modem failed
	58	Reserved
	59	Reserved
	60	Reserved
	61	Reserved
	62	Reserved
	63	Reserved
	64	Reserved

Display	Point	Description
Display 2	1-32	Ping Alarms 1 - 32
	33-64	Undefined

Display	Point	Description
Display 3	1	Analog 1 Minor Under
	2	Analog 1 Minor Over
	3	Analog 1 Major Under

	4	Analog 1 Major Over
	9-16	Control
	17-32	Value
	33	Analog 2 Minor Under
	34	Analog 2 Minor Over
	35	Analog 2 Major Under
	36	Analog 2 Major Over
	41-48	Control
	49-64	Value

Display	Point	Description
Display 4	1	Analog 3 Minor Under
	2	Analog 3 Minor Over
	3	Analog 3 Major Under
	4	Analog 3 Major Over
	9-16	Control
	17-32	Value
	33	Analog 4 Minor Under
	34	Analog 4 Minor Over
	35	Analog 4 Major Under
	36	Analog 4 Major Over
	41-48	Control
	49-64	Value

Display	Point	Description
Display 5	1	Analog 5 Minor Under
	2	Analog 5 Minor Over
	3	Analog 5 Major Under
	4	Analog 5 Major Over
	9-16	Control
	17-32	Value
	33	Analog 6 Minor Under
	34	Analog 6 Minor Over
	35	Analog 6 Major Under
	36	Analog 6 Major Over
	41-48	Control
	49-64	Value

Display	Point	Description
Display 6	1	Analog 7 Minor Under
	2	Analog 7 Minor Over
	3	Analog 7 Major Under
	4	Analog 7 Major Over
	9-16	Control
	17-32	Value
	33	Analog 8 Minor Under
	34	Analog 8 Minor Over
	35	Analog 8 Major Under
	36	Analog 8 Major Over
	41-48	Control
	49-64	Value

Display	Point	Description

Display	Point	Description
Display 7	1	Digital sensor 1 Minor Under
	2	Digital sensor 1 Minor Over
	3	Digital sensor 1 Major Under
	4	Digital sensor 1 Major Over
	5	Digital sensor 1 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 2 Minor Under
	34	Digital sensor 2 Minor Over
	35	Digital sensor 2 Major Under
	36	Digital sensor 2 Major Over
	37	Digital sensor 2 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
Display 8	1	Digital sensor 3 Minor Under
	2	Digital sensor 3 Minor Over
	3	Digital sensor 3 Major Under
	4	Digital sensor 3 Major Over
	5	Digital sensor 3 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 4 Minor Under
	34	Digital sensor 4 Minor Over
	35	Digital sensor 4 Major Under
	36	Digital sensor 4 Major Over
	37	Digital sensor 4 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
Display 9	1	Digital sensor 5 Minor Under
	2	Digital sensor 5 Minor Over
	3	Digital sensor 5 Major Under
	4	Digital sensor 5 Major Over
	5	Digital sensor 5 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 6 Minor Under
	34	Digital sensor 6 Minor Over
	35	Digital sensor 6 Major Under
	36	Digital sensor 6 Major Over
	37	Digital sensor 6 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
Display 10	1	Digital sensor 7 Minor Under
	2	Digital sensor 7 Minor Over
	3	Digital sensor 7 Major Under
	4	Digital sensor 7 Major Over
	5	Digital sensor 7 Sensor not detected

	9-16	Control
	17-32	Value
	33	Digital sensor 8 Minor Under
	34	Digital sensor 8 Minor Over
	35	Digital sensor 8 Major Under
	36	Digital sensor 8 Major Over
	37	Digital sensor 8 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 9 Minor Under
	2	Digital sensor 9 Minor Over
	3	Digital sensor 9 Major Under
	4	Digital sensor 9 Major Over
	5	Digital sensor 9 Sensor not detected
	9-16	Control
	17-32	Value
Display 11	33	Digital sensor 10 Minor Under
	34	Digital sensor 10 Minor Over
	35	Digital sensor 10 Major Under
	36	Digital sensor 10 Major Over
	37	Digital sensor 10 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 11 Minor Under
	2	Digital sensor 11 Minor Over
	3	Digital sensor 11 Major Under
	4	Digital sensor 11 Major Over
	5	Digital sensor 11 Sensor not detected
	9-16	Control
	17-32	Value
Display 12	33	Digital sensor 12 Minor Under
	34	Digital sensor 12 Minor Over
	35	Digital sensor 12 Major Under
	36	Digital sensor 12 Major Over
	37	Digital sensor 12 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 13 Minor Under
	2	Digital sensor 13 Minor Over
	3	Digital sensor 13 Major Under
	4	Digital sensor 13 Major Over
	5	Digital sensor 13 Sensor not detected
Display 13	9-16	Control
	17-32	Value
	33	Digital sensor 14 Minor Under
	34	Digital sensor 14 Minor Over
	35	Digital sensor 14 Major Under

	36	Digital sensor 14 Major Over
	37	Digital sensor 14 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
Display 14	1	Digital sensor 15 Minor Under
	2	Digital sensor 15 Minor Over
	3	Digital sensor 15 Major Under
	4	Digital sensor 15 Major Over
	5	Digital sensor 15 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 16 Minor Under
	34	Digital sensor 16 Minor Over
	35	Digital sensor 16 Major Under
	36	Digital sensor 16 Major Over
	37	Digital sensor 16 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
Display 15	1	Digital sensor 17 Minor Under
	2	Digital sensor 17 Minor Over
	3	Digital sensor 17 Major Under
	4	Digital sensor 17 Major Over
	5	Digital sensor 17 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 18 Minor Under
	34	Digital sensor 18 Minor Over
	35	Digital sensor 18 Major Under
	36	Digital sensor 18 Major Over
	37	Digital sensor 18 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
Display 16	1	Digital sensor 19 Minor Under
	2	Digital sensor 19 Minor Over
	3	Digital sensor 19 Major Under
	4	Digital sensor 19 Major Over
	5	Digital sensor 19 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 20 Minor Under
	34	Digital sensor 20 Minor Over
	35	Digital sensor 20 Major Under
	36	Digital sensor 20 Major Over
	37	Digital sensor 20 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 21 Minor Under
	2	Digital sensor 21 Minor Over
	3	Digital sensor 21 Major Under
	4	Digital sensor 21 Major Over
	5	Digital sensor 21 Sensor not detected
	9-16	Control
	17-32	Value
Display 17	33	Digital sensor 22 Minor Under
	34	Digital sensor 22 Minor Over
	35	Digital sensor 22 Major Under
	36	Digital sensor 22 Major Over
	37	Digital sensor 22 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 23 Minor Under
	2	Digital sensor 23 Minor Over
	3	Digital sensor 23 Major Under
	4	Digital sensor 23 Major Over
	5	Digital sensor 23 Sensor not detected
	9-16	Control
	17-32	Value
Display 18	33	Digital sensor 24 Minor Under
	34	Digital sensor 24 Minor Over
	35	Digital sensor 24 Major Under
	36	Digital sensor 24 Major Over
	37	Digital sensor 24 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 25 Minor Under
	2	Digital sensor 25 Minor Over
	3	Digital sensor 25 Major Under
	4	Digital sensor 25 Major Over
	5	Digital sensor 25 Sensor not detected
	9-16	Control
	17-32	Value
Display 19	33	Digital sensor 26 Minor Under
	34	Digital sensor 26 Minor Over
	35	Digital sensor 26 Major Under
	36	Digital sensor 26 Major Over
	37	Digital sensor 26 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 27 Minor Under
Display 20	2	Digital sensor 27 Minor Over
	3	Digital sensor 27 Major Under
	4	Digital sensor 27 Major Over

Display	Point	Description
	5	Digital sensor 27 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 28 Minor Under
	34	Digital sensor 28 Minor Over
	35	Digital sensor 28 Major Under
	36	Digital sensor 28 Major Over
	37	Digital sensor 28 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 29 Minor Under
	2	Digital sensor 29 Minor Over
	3	Digital sensor 29 Major Under
	4	Digital sensor 29 Major Over
	5	Digital sensor 29 Sensor not detected
	9-16	Control
	17-32	Value
Display 21	33	Digital sensor 30 Minor Under
	34	Digital sensor 30 Minor Over
	35	Digital sensor 30 Major Under
	36	Digital sensor 30 Major Over
	37	Digital sensor 30 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 31 Minor Under
	2	Digital sensor 31 Minor Over
	3	Digital sensor 31 Major Under
	4	Digital sensor 31 Major Over
	5	Digital sensor 31 Sensor not detected
	9-16	Control
	17-32	Value
Display 22	33	Digital sensor 32 Minor Under
	34	Digital sensor 32 Minor Over
	35	Digital sensor 32 Major Under
	36	Digital sensor 32 Major Over
	37	Digital sensor 32 Sensor not detected
	41-48	Control
	49-64	Value

15.2   System Alarms

Display	Point	Description
1	33	Default Configuration
	34	DIP Switch Configuration
	35	MAC Address Not Set
	36	IP Address Not Set
	37	LAN hardware error
	38	SNMP Process Error
	39	SNMP Community Error
	40	LAN TX packet drop
	41	Notification 1 Failed
	42	Notification 2 Failed
	43	Notification 3 Failed
	44	Notification 4 Failed
	45	Notification 5 Failed
	46	Notification 6 Failed
	47	Notification 7 Failed
	48	Notification 8 failed
	49	NTP Failed
	50	Timed Tick
	51	Serial 1 RcvQ full
	52	Dynamic Memory Full
	53	Unit Reset
	54	DCP Poller inactive

System Alarms

15.3   SNMP Manager Functions

The SNMP Manager allows the user to view alarm status, set date/time, issue controls, and perform a resync. The display and tables below outline the MIB object identifiers. The table below begins with dpsRTU; however, the MIB object identifier tree has several levels above it. The full English name is as follows: root.iso.org.dod.internet.private.enterprises.dps-Inc.dpsAlarmControl.dpsRTU. Therefore, dpsRTU's full object identifier is 1.3.6.1.4.1.2682.1.2. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the Control Grid is 1.3.6.1.4.1.2682.1.2.3.3 because the object identifier of dpsRTU is 1.3.6.1.4.1.2682.1.4 + the Control Grid (.3) + the Display (.3).
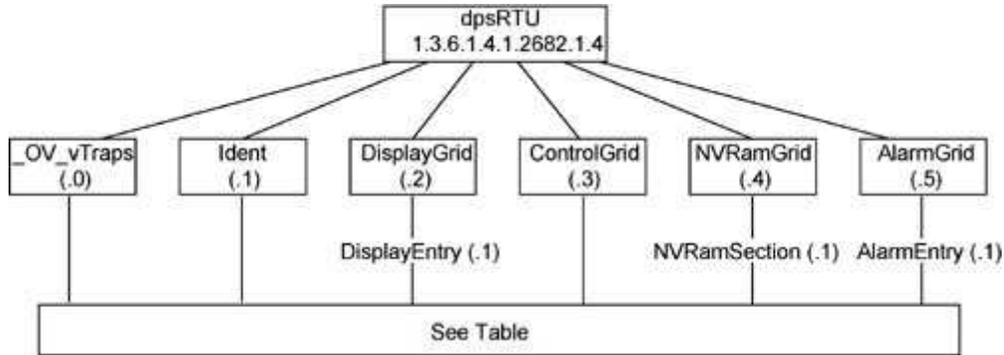
Tbl. B1 (O.)_OV_Traps points
_OV_vTraps (1.3.6.1.4.1.2682.1.2.0)
PointSet (.20)
PointClr (.21)
SumPSet (.101)
SumPClr (.102)
ComFailed (.103)
ComRestored (.014)
P0001Set (.10001) through P0064Set (.10064)
P0001Clr (.20001) through P0064Clr (.20064)

Tbl. B2 (.1) Identity points
Ident (1.3.6.1.4.1.2682.1.2.1)
Manufacturer (.1)
Model (.2)
Firmware Version (.3)
DateTime (.4)
ResyncReq (.5)*
* Must be set to "1" to perform the resync request which will resend TRAPs for any standing alarm.

Tbl. B3 (.2) DisplayGrid points
DisplayEntry (1.3.6.1.4.1.2682.1.2.2.1)
Port (.1)
Address (.2)
Display (.3)
DispDesc (.4)*
PntMap (.5)*

Tbl. B3 (.3) ControlGrid points
ControlGrid (1.3.6.1.4.1.2682.1.2.3)
Port (.1)
Address (.2)
Display (.3)
Point (.4)

Tbl. B6 (.6) Analog Channels
Channel Entry (1.3.6.1.4.1.2682.1.4.6.1)
Channel Number (.1)
Enabled (.2)
Description (.3)
Value (.4)

Tbl. B5 (.5) AlarmEntry points
AlarmEntry (1.3.6.4.1.2682.1.2.5.1)
Aport (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)

Action (.5)

Thresholds (.5)*
*If Mj, Mn is assumed

APntDesc (.5)*
AState (.6)
* For specific alarm points, see Table B6

15.4   SNMP Granular Trap Packets

The tables below provide a list of the information contained in the SNMP Trap packets sent by the NetGuardian DIN.

SNMP Trap managers can use one of two methods to get alarm information:
1. Granular traps (not necessary to define point descriptions for the NetGuardian DIN) **OR**
2. The SNMP manager reads the description from the Trap.

UDP Header	Description
1238	Source port
162	Destination port
303	Length
0xBAB0	Checksum

UDP Headers and descriptions

SNMP Header	Description
0	Version
Public	Request
Trap	Request
1.3.6.1.4.1.2682.1.4	Enterprise
126.10.230.181	Agent address
Enterprise Specific	Generic Trap
8001	Specific Trap
617077	Time stamp
1.3.7.1.2.1.1.1.0	Object
NetGuardian DIN v1.0K	Value
1.3.6.1.2.1.1.6.0	Object
1-800-622-3314	Value
1.3.6.1.4.1.2682.1.4.4.1.0	Object
01-02-1995 05:08:27.760	Value
1.3.6.1.4.1.2682.1.4.5.1.1.99.1.1.1	Object
99	Value
1.3.6.1.4.1.2682.1.4.5.1.2.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.4.5.1.3.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.4.5.1.4.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.4.5.1.5.99.1.1.1	Object
Rectifier Failure	Value
1.3.6.1.4.1.2682.1.4.5.1.6.99.1.1.1	Object
Alarm	Value

SNMP Headers and descriptions

16 Frequently Asked Questions

Here are answers to some common questions from NetGuardian DIN users. The latest FAQs can be found on the NetGuardian DIN support web page, **http://www.dpstele.com.**

If you have a question about the NetGuardian DIN, please call us at **(559) 454-1600** or e-mail us at **support@dpstele.com.**

16.1 General FAQs

Q. How do I telnet to the NetGuardian DIN?
A. You must use **Port 2002** to connect to the NetGuardian DIN. Configure your Telnet client to connect using TCP/IP (**not** "Telnet," or any other port options). For connection information, enter the IP address of the NetGuardian DIN and Port 2002. For example, to connect to the NetGuardian DIN using the standard Windows Telnet client, click Start, click Run, and type "telnet <NetGuardian DIN IP address> 2002."

Q. How do I connect my NetGuardian DIN to the LAN?
A. To connect your NetGuardian DIN to your LAN, you need to configure the unit IP address, the subnet mask and the default gateway. A sample configuration could look like this:
Unit Address: 192.168.1.100
subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1
Save your changes by writing to NVRAM and reboot. Any change to the unit's IP configuration requires a reboot.

Q. When I connect to the NetGuardian DIN through the craft port on the front panel it either doesn't work right or it doesn't work at all. What's going on?
A. Make sure your using the right COM port settings. Your COM port settings should read:
Bits per second: 9600 (9600 baud)
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None
Important! Flow control **must** be set to **none**. Flow control normally defaults to hardware in most terminal programs, and this will not work correctly with the NetGuardian DIN.

Q. The LAN link LED is green on my NetGuardian DIN, but I can't poll it from my T/Mon.
A. Some routers will not forward packets to an IP address until the MAC address of the destination device has been registered on the router's Address Resolution Protocol (ARP) table. Enter the IP address of your gateway and your T/Mon system to the ARP table.

16.2 SNMP FAQs

Q. Which version of SNMP is supported by the SNMP agent on the NetGuardian DIN?
A. SNMP v1, SNMPv2 and SNMPv3.

Q. How do I configure the NetGuardian DIN to send traps to an SNMP manager? Is there a separate MIB for the NetGuardian DIN? How many SNMP managers can the agent send traps to? And how do I set the IP address of the SNMP manager and the community string to be used when sending traps?
A. The NetGuardian DIN begins sending traps as soon as the SNMP notification type is set up. The NetGuardian DIN MIB can be found on the DPS Telecom website. The MIB should be compiled on your SNMP manager. (**Note:** MIB versions may change in the future.) For step-by-step instructions, refer back to the "How to Send SNMP Traps" section of the user manual.

Q. Does the NetGuardian DIN support MIB-2 and/or any other standard MIBs?
A. The NetGuardian DIN supports the bulk of MIB-2.

Q. Does the NetGuardian DIN SNMP agent support both NetGuardian DIN and T/MonXM variables?
A. The NetGuardian DIN SNMP agent manages an embedded MIB that supports only the NetGuardian DIN's RTU variables. The T/MonXM variables are included in the distributed MIB only to provide SNMP managers with a single MIB for all DPS Telecom products.

Q. How many traps are triggered when a single point is set or cleared? The MIB defines traps like "major alarm set/cleared," "RTU point set," and a lot of granular traps, which could imply that more than one trap is sent when a change of state occurs on one point.
A. Generally, a single change of state generates a single trap.

Q. What does "point map" mean?
A. A point map is a single MIB leaf that presents the current status of a 64-alarm-point display in an ASCII-readable form, where a "." represents a clear and an "x" represents an alarm.

Q. The NetGuardian DIN manual talks about control relay outputs. How do I control these from my SNMP manager?
A. The control relays are operated by issuing the appropriate set commands, which are contained in the DPS Telecom MIB.

Q. How can I associate descriptive information with a point for the RTU granular traps?
A. The NetGuardian DIN alarm point descriptions are individually defined using the Web Browser.

Q. My SNMP traps aren't getting through. What should I try?
A. Try these three steps:
1. Make sure that the Trap Address (IP address of the SNMP manager) is defined. (If you changed the Trap Address, make sure you saved the change to NVRAM and rebooted.)
2. Make sure all alarm points are configured to send SNMP traps.
3. Make sure the NetGuardian DIN and the SNMP manager are both on the network. Use the unit's ping command to ping the SNMP manager.

17 Technical Support

DPS Telecom products are backed by our courteous, friendly Technical Support representatives, who will give you the best in fast and accurate customer service. To help us help you better, please take the following steps before calling Technical Support:

1. Check the DPS Telecom website.
You will find answers to many common questions on the DPS Telecom website, at **http://www.dpstele.com/support/**. Look here first for a fast solution to your problem.

2. Prepare relevant information.
Having important information about your DPS Telecom product in hand when you call will greatly reduce the time it takes to answer your questions. If you do not have all of the information when you call, our Technical Support representatives can assist you in gathering it. Please write the information down for easy access. Please have your user manual and hardware serial number ready.

3. Have access to troubled equipment.
Please be at or near your equipment when you call DPS Telecom Technical Support. This will help us solve your problem more efficiently.

4. Call during Customer Support hours.
Customer support hours are Monday through Friday, from 7 A.M. to 6 P.M., Pacific time. The DPS Telecom Technical Support phone number is **(559) 454-1600**.

Emergency Assistance: *Emergency assistance is available 24 hours a day, 7 days a week. For emergency assistance after hours, allow the phone to ring until it is answered with a paging message. You will be asked to enter your phone number. An on-call technical support representative will return your call as soon as possible.*

18 End User License Agreement

All Software and firmware used in, for, or in connection with the Product, parts, subsystems, or derivatives thereof, in whatever form, including, without limitation, source code, object code and microcode, including any computer programs and any documentation relating to or describing such Software is furnished to the End User only under a non-exclusive perpetual license solely for End User's use with the Product.

The Software may not be copied or modified, in whole or in part, for any purpose whatsoever. The Software may not be reverse engineered, compiled, or disassembled. No title to or ownership of the Software or any of its parts is transferred to the End User. Title to all patents, copyrights, trade secrets, and any other applicable rights shall remain with the DPS Telecom.

DPS Telecom's warranty and limitation on its liability for the Software is as described in the warranty information provided to End User in the Product Manual.

End User shall indemnify DPS Telecom and hold it harmless for and against any and all claims, damages, losses, costs, expenses, obligations, liabilities, fees and costs and all amounts paid in settlement of any claim, action or suit which may be asserted against DPS Telecom which arise out of or are related to the non-fulfillment of any covenant or obligation of End User in connection with this Agreement.

This Agreement shall be construed and enforced in accordance with the laws of the State of California, without regard to choice of law principles and excluding the provisions of the UN Convention on Contracts for the International Sale of Goods. Any dispute arising out of the Agreement shall be commenced and maintained only in Fresno County, California. In the event suit is brought or an attorney is retained by any party to this Agreement to seek interpretation or construction of any term or provision of this Agreement, to enforce the terms of this Agreement, to collect any money due, or to obtain any money damages or equitable relief for breach, the prevailing party shall be entitled to recover, in addition to any other available remedy, reimbursement for reasonable attorneys' fees, court costs, costs of investigation, and other related expenses.

Warranty

DPS Telecom warrants, to the original purchaser only, that its products a) substantially conform to DPS' published specifications and b) are substantially free from defects in material and workmanship. This warranty expires two years from the date of product delivery with respect to hardware and ninety days from the date of product delivery with respect to software. If the purchaser discovers within these periods a failure of the product to substantially conform to the specifications or that the product is not substantially free from defects in material and workmanship, the purchaser must promply notify DPS. Within reasonable time after notification, DPS will endeavor to correct any substantial non-conformance with the specifications or substantial defects in material and workmanship, with new or used replacement parts. All warranty service will be performed at the company's office in Fresno, California, at no charge to the purchaser, other than the cost of shipping to and from DPS, which shall be the responsiblity of the purchaser. If DPS is unable to repair the product to conform to the warranty, DPS will provide at its option one of the following: a replacement product or a refund of the purchase price for the non-conforming product. These remedies are the purchaser's only remedies for breach of warranty. Prior to initial use the purchaser shall have determined the suitability of the product for its intended use. DPS does not warrant a) any product, components or parts not manufactured by DPS, b) defects caused by the purchaser's failure to provide a suitable installation environment for the product, c) damage caused by use of the product for purposes other than those for which it was designed, d) damage caused by disasters such as fire, flood, wind or lightning unless and to the extent that the product specification provides for resistance to a defined disaster, e) damage caused by unauthorized attachments or modifications, f) damage during shipment from the purchaser to DPS, or g) any abuse or misuse by the purchaser.

THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In no event will DPS be liable for any special, incidental, or consequential damages based on breach of warranty, breach of contract, negligence, strict tort, or any other legal theory. Damages that DPS will not be responsible for include but are not limited to, loss of profits; loss of savings or revenue; loss of use of the product or any associated equipment; cost of capital; cost of any substitute equipment, facilities or services; downtime; claims of third parties including customers; and injury to property.

The purchaser shall fill out the requested information on the Product Warranty Card and mail the card to DPS. This card provides information that helps DPS make product improvements and develop new products.

For an additional fee DPS may, at its option, make available by written agreement only an extended warranty providing an additional period of time for the applicability of the standard warranty.

Technical Support

If a purchaser believes that a product is not operating in substantial conformance with DPS' published specifications or there appear to be defects in material and workmanship, the purchaser should contact our technical support representatives. If the problem cannot be corrected over the telephone and the product and problem are covered by the warranty, the technical support representative will authorize the return of the product for service and provide shipping information. If the product is out of warranty, repair charges will be quoted. All non-warranty repairs receive a 90-day warranty.

Free Tech Support is Only a Click Away

Need help with your alarm monitoring? DPS Information Services are ready to serve you … in your email or over the Web!

www.DpsTelecom.com

Free Tech Support in Your Email: The Protocol Alarm Monitoring Ezine

The Protocol Alarm Monitoring Ezine is your free email tech support alert, delivered directly to your in-box every two weeks. Every issue has news you can use right away:

- Expert tips on using your alarm monitoring equipment — advanced techniques that will save you hours of work

- Educational White Papers deliver fast informal tutorials on SNMP, ASCII processing, TL1 and other alarm monitoring technologies

- New product and upgrade announcements keep you up to date with the latest technology

- Exclusive access to special offers for DPS Telecom Factory Training, product upgrade offers and discounts

To get your free subscription to The Protocol register online at
www.TheProtocol.com/register

Free Tech Support on the Web: MyDPS

MyDPS is your personalized, members-only online resource. Registering for MyDPS is fast, free, and gives you exclusive access to:

- Firmware and software downloads and upgrades
- Product manuals
- Product datasheets
- Exclusive user forms

Register for MyDPS online at
www.DpsTelecom.com/register

(800) 622-3314 • www.dpstele.com • 4955 E. Yale Avenue, Fresno, California 93727