DPS Telecom

"Your Partners in Network Alarm Monitoring"

NetGuardian 224A

USER MANUAL

D-PK-NG224-12003

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

January 4, 2019 **D-UM-NG224**

Revision History

January 4, 2019	Added Section RJ45 Pinout (Analogs)
May 30, 2017	Secure Web Feature
March 23, 2017	Added History Log Format and Operation Section
October 24, 2016	Added HVAC Monitor Mode
July 19, 2016	Push-to-talk function added
April 27, 2015	Timers Update
March 10, 2015	Minor Browser Updates
December 23, 2014	Updated User Analogs, minor edits
November 18, 2014	Updated Timers Page
November 22, 2013	Added Conditional Halt, ~evalMt & corrected ~evalMn in Provisioning Sensors
November 13, 2013	Added ~intCnt mode description
November 8, 2013	Fixed timing on ~evailMn mode to 15 sec
October 10, 2013	Modbus and Sensor clarifications
October 4, 2013	Sensor slot equation explanation, tables and examples
October 3, 2013	Added images and instructions for Modbus functionality
September 6, 2013	Updated Images, Specifications, Shipping List & Misc. Details for G2
August 20, 2013	Updated Images & Misc. Details
August 15, 2013	Updated Specifications and Images
August 14, 2013	Initial Release

Notice

The material in this manual is for information purposes and is subject to change without notice. DPS Telecom shall not be liable for errors contained herein or consequential damages in connection with the furnishing, performance, or use of this manual.

Contents

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

1 NetGuardian 224A Overview

The NetGuardian 224A

Could you estimate **how much** money your company has invested in your remote shelter, IT server room, or data center? **How much** is your network uptime worth to you? These questions might be difficult to answer, but monitoring your valuable IT equipment certainly doesn't have to be.

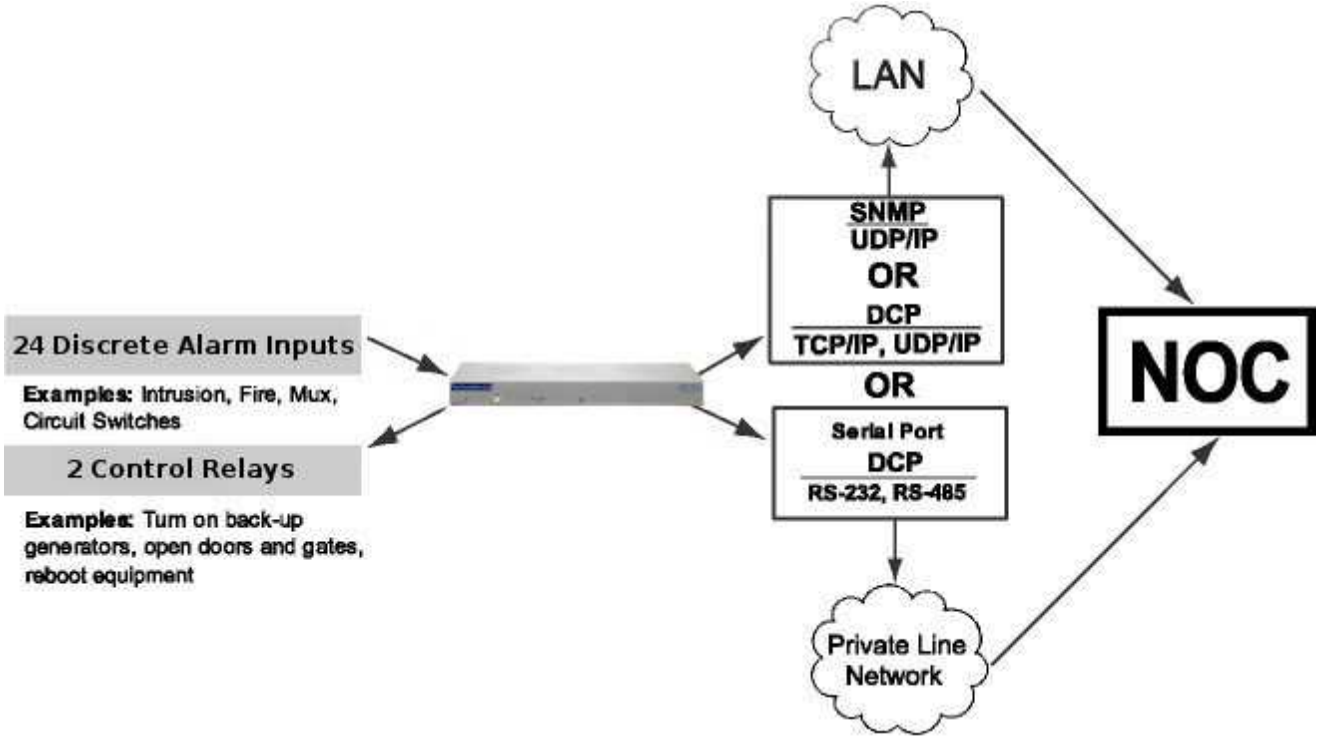
You need a compact, simple, and reliable device to monitor basic environmental conditions (like temperature, humidity, smoke...) around your valuable equipment. Without this basic visibility, it's just a matter of time before your investment in your server room is seriously damaged.

- **24 Discrete Alarm Inputs (TTL)**
- **4 D-Wire sensor ports**
- **2 Form C Control Relay Outputs**
- **Fast, integrated, and secure Web browser**
- **32 ping targets to monitor other devices on the network**

Meet the NetGuardian 224A
This small device keeps tabs on all the environmental levels that affect your servers, phone closets, data centers, and other equipment locations. The 24 discrete alarms on the back panel are used to monitor dry contacts, such as motion sensors, UPS, smoke detectors, flood sensors, AC and room entry.

What's the current room temperature? When was the last time someone entered the room? Get all of this information - right from your network PC.

Don't wait until the day your AC unit fails and your server closet **overheats** to start protecting your gear. This small, 1RU device alerts you of changing conditions 24 hours a day, 7 days a week, either to your cell or SNMP manager. The NetGuardian 224A is the cost-effective way to stay proactive in your monitoring.



Common Applications for the NetGuardian 224A

The NetGuardian 224A reports alarms as SNMP traps over LAN and supports DCP polling over RS-232, RS-485 or LAN. The NetGuardian 224A supports simultaneous SNMP and DCP operation.

The NetGuardian 224A supports both LAN and serial port connectivity. The LAN connection and serial port can be used at the same time to support simultaneous SNMP and DCP alarm reporting. However, only one DCP channel can be used, therefore the NetGuardian 224A cannot simultaneously report DCP over LAN and DCP over serial port connection.

In addition to its 24 discrete input points, the NetGuardian 224A has 2 control relays, both form C, for user defined NO/NC connections, 2 analogs, and dwire. 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, exhaust fans, or perform other functions. The NetGuardian 224A also allows you to reverse the logic state of the alarm on a point by point basis for discrete alarms.

Another feature of the NetGuardian 224A is user-defined alarm qualification times. This will allow you to clearly distinguish momentary status changes from serious problems.

2 Specifications

Hardware

Dimensions:	17.026" W x 1.720" H x 5.636" D
Mounting:	19" or 23" Rack
Weight:	3.5 lbs (1.56 kg)
Power Input:	24/48VDC (18 to 60 VDC) Polarity Insensitive
Power Supply Output:	+24VDC, 1 amp +12VDC, 1 amp
[3] **Current Draw:**	100mA @ 48 VDC 200mA @ 24 VDC
Fuse:	3/4 Amp GMT Fuse
Visual Interfaces:	8 Front Panel LEDs 6 back LED's
[1] **Hardware Interfaces:**	1 DB50 (Discrete Inputs) 1 RJ45 10/100BaseT Ethernet 1 RS-232 Serial (optional USB serial) 1 USB Craft Port 4 RJ-12 D-Wire sensor port 1 Pluggable port for Controls 2 RJ45 for analongs/power supply
Discrete Alarm Inputs:	24 (TTL, 5V biased)
Analogs:	2
Input Range:	-92 to +92VDC or 4 to 20mA
[4] **Analog Accuracy:**	±1% of Analog Range
Control Outputs:	2 Form C Relays
Max Voltage:	60 VDC/120 VAC
Max Current:	1A AC/DC
Operating Temp:	32° to 140°F (0° to 60°C)
[1] **Industrial Operating Temp:**	-22° to 158°F (-30° to 70°C)
Operating Humidity:	0% to 95% non-condensing
MTBF:	60 Years
RoHS:	RoHS 5/6 Approved

Software

Downloadable Firmware:	Yes
Built-in Web Interface:	Yes
Browser Support:	IE9, IE10, Firefox, Chrome
Protocols:	HTTPS, DCPx, TELNET, HTTP, Email
SNMP Support:	V1, V2c, V3
[1] **D-Wire Sensor Support:**	Temp, Temp/Humidity, Temp/Airflow
Ping Alarms:	32

Note:

[1] Valid if hardware option is included.
[2] Minimum lengths determined with TTL voltage level alarms. Actual distance may vary.
[3] Current measured at rated voltage with all controls latched and all alarms triggered.
[4] See analog section in manual for detailed analog accuracy breakdown.

* This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Secure Web: TLS v1.2 and AES128 with built in self signed certificate by DPS Telecom for 128bit key exchange

3 Shipping List

Please make sure all of the following items are included with your NetGuardian 224A. 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 224A
D-PK-NG224

NetGuardian 224A Resource CD

NetGuardian 224A User Manual
D-UM-NGDIN

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

x 2

3/4-Amp GMT Fuses
2-741-00750-00

x 2

Locking RIA Connector (Main Pwr)
2-820-00862-02

6-Pin Pluggable Phoenix Connector (Controls)
2-821-10635-00

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

x 2

23" Rack Ear
D-CS-325-10A-01

x 2

19" Rack Ear
D-CS-325-10A-00

 x 8

3/8" Ear Screws
1-000-60375-05

 x 4

Metric Rack Screws
2-000-80750-03

 x 4

Two Standard Rack Screws
1-000-12500-06

Pads
2-015-00030-00

3.1 Optional Shipping Items - Available by Request

Small WAGO connector
2-802-01020-00

4 NetGuardian 224A Front Panel

NetGuardian 224A Front Panel

LED	Status	Description
Power	Solid Green	Power Supply OK
	Off	No Voltage (or) Power Leads Reversed
FA	Solid Red	Blown Fuse
	Off	Fuse OK
Status	Flashing Green	Application Running
	Flashing Red	Bootloader Running
Alarm	Flashing Red	New Alarm
	Solid Red	Standing Alarm Acknowledged via DCP poll
	Off	No Alarms
Serial	Flashing Green	Data Transmitted on Serial Connection
	Flashing Red	Data Received on Serial Connection
Power (Lamp)	Solid Green	Processor has power
	Off	Processor does not have power
USB	Flashing Green	Data Transmitted over USB
	Flashing Red	Data Received over USB
D-Wire	Solid Green	At least 1 dwire enabled, no alarm
	Flashing Green	Standing acknowledged alarm (Threshold)
	Flashing Red	New Alarm
	Off	No D-Wire Alarms
Lnk	Solid Green	LAN Connected
	Off	LAN Not Connected
LAN	Flashing Yellow	Activity over Ethernet Connection
	Off	No Activity
100BT	Solid Green	LAN Connection Speed is 100BaseT
	Off	LAN Connection Speed is 10BaseT
Analog	Solid Green	Analogs enabled, no alarm
	Solid Red	Standing acknowledged alarm (Threshold)
	Flashing Red	New Alarm
	Off	No Analogs enabled
Relay	Solid Green	1 or more relays latched
	Flashing Green	New relay latched or released
	Off	All relay off

Front Panel LED Descriptions

5 NetGuardian 224A Back Panel

5.1 Installation

5.1.1 Tools Needed

To install the NetGuardian 224A, you'll need the following tools:

Phillips No. 2 Screwdriver

Small Standard No. 2 Screwdriver

PC with terminal emulator, such as HyperTerminal

5.1.2 Mounting

The NetGuardian 224A can be flush or rear-mounted

The NetGuardian 224A mounts in a 19" rack or a 23" rack using the provided rack ears for each size. Two rack ear

locations are provided. Attach the appropriate rack ears in the flush-mount or rear-mount locations shown in Figure 6.2.1.

Note: Rack ears can be rotated 90° for wall mounting or 180º for other mounting options (not shown).

5.1.3 Power Connection

The NetGuardian 224A uses single or dual (Optional) power inputs, powered through two barrier plug power connectors.

NetGuardian 224A Power Terminals and Fuses

To connect the NetGuardian 224A 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. One plug is used for main power and the other is used for backup power. Both plugs are interchangeable so it does not matter which plug you select. Each plug's right terminal is Ground and its left terminal is Battery Lead.
4. Insert a battery return into the power connector plug's right terminal (+) 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 for polarity. The LED will be off if polarity is wrong, and green if it is correct.
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. Insert the local fuse into the power fuse slot. The power plug can be inserted into the power connector only one way to ensure the correct polarity.

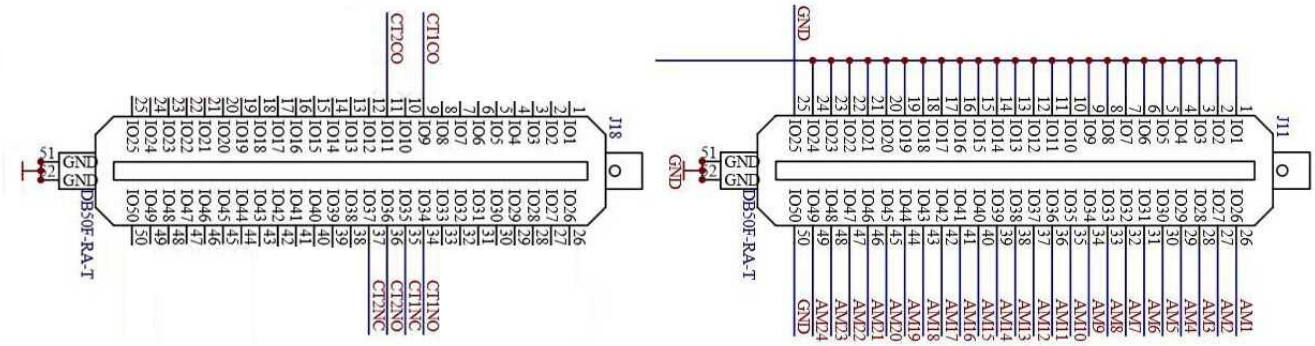
Note: The negative voltage terminal is on the left and the (+) terminal is on the right.

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

5.2 Amphenol Pinouts

If your unit has only one amphenol connector, your controls are pluggable. See next section for wiring.

For alarms 1-24, the inputs are TTL 5V biased.

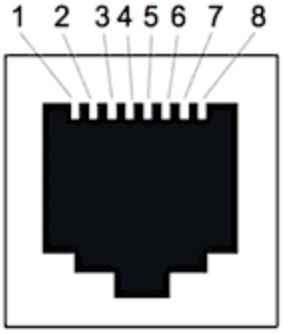


5.3 Pluggable Connectors

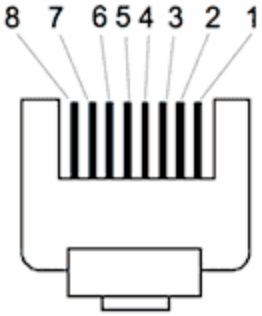
If your controls use a pluggable connector, attach your wires into the included screw-down 6-pin phoenix connector. Refer to the labels on the unit.

If your controls have an amphenol connector, refer to previous section.

5.4 RJ45 Pinout (Analogs)



Rj-45 Jack
(Female)



Rj-45 Plug
(Male)

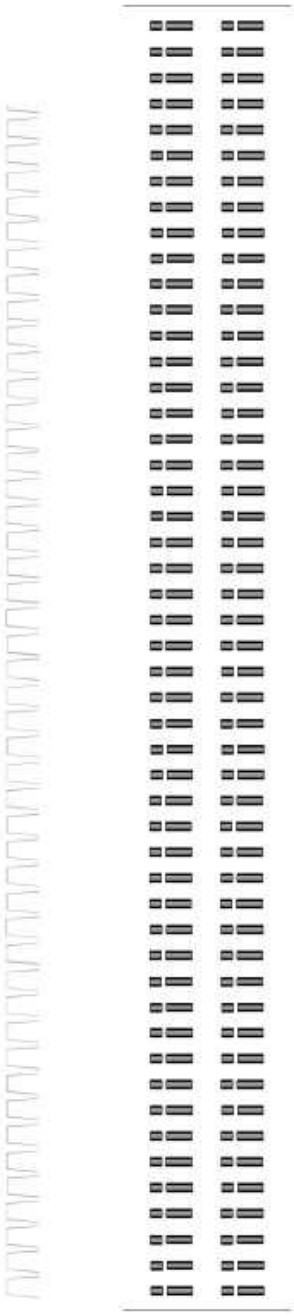
Pin	Desc.
3	+ANA

4	+12Vdc
6	-ANA
8	GND
1, 2, 5, 7	NC

RJ45 Pinout for Analogs

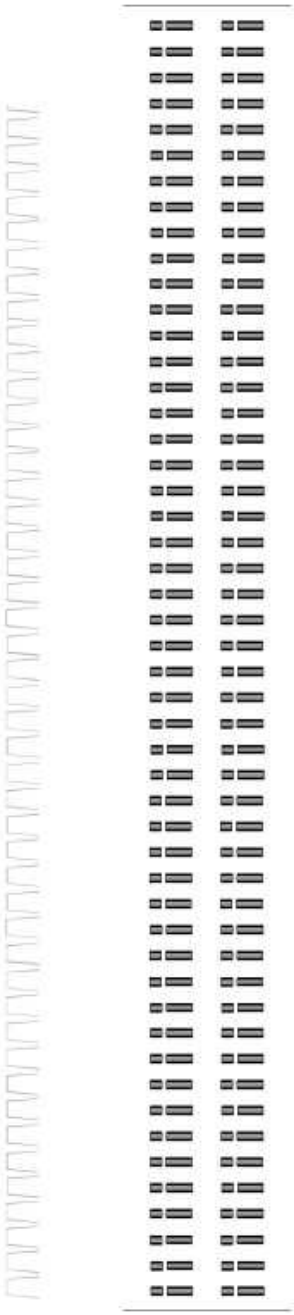
5.5 66Block diagrams

66 block pinout for Amphenol 1 (TTL Discretes 1-24)



Wire color (wire/stripe)	Connection	66 Block Pair #	Corresponding 50-Pin Connector Pin #
WHT/BLU	ALM 1	1	26
BLU/WHT	RTN 1		1
WHT/ORG	ALM 2	2	27
ORG/WHT	RTN 2		2
WHT/GRN	ALM 3	3	28
GRN/WHT	RTN 3		3
WHT/BRN	ALM 4	4	29
BRN/WHT	RTN 4		4
WHT/GRY	ALM 5	5	30
GRY/WHT	RTN 5		5
RED/BLU	ALM 6	6	31
BLU/RED	RTN 6		6
RED/ORG	ALM 7	7	32
ORG/RED	RTN 7		7
RED/GRN	ALM 8	8	33
GRN/RED	RTN 8		8
RED/BRN	ALM 9	9	34
BRN/RED	RTN 9		9
RED/GRY	ALM 10	10	35
GRY/RED	RTN 10		10
BLK/BLU	ALM 11	11	36
BLU/BLK	RTN 11		11
BLK/ORG	ALM 12	12	37
ORG/BLK	RTN 12		12
BLK/GRN	ALM 13	13	38
GRN/BLK	RTN 13		13
BLK/BRN	ALM 14	14	39
BRN/BLK	RTN 14		14
BLK/GRY	ALM 15	15	40
GRY/BLK	RTN 15		15
YEL/BLU	ALM 16	16	41
BLU/YEL	RTN 16		16
YEL/ORG	ALM 17	17	42
ORG/YEL	RTN 17		17
YEL/GRN	ALM 18	18	43
GRN/YEL	RTN 18		18
YEL/BRN	ALM 19	19	44
BRN/YEL	RTN 19		19
YEL/GRY	ALM 20	20	45
GRY/YEL	RTN 20		20
VIO/BLU	ALM 21	21	46
BLU/VIO	RTN 21		21
VIO/ORG	ALM 22	22	47
ORG/VIO	RTN 22		22
VIO/GRN	ALM 23	23	48
GRN/VIO	RTN 23		23
VIO/BRN	ALM 24	24	49
BRN/VIO	RTN 24		24
VIO/GRY	GND	25	50
GRY/VIO	GND		25

66 block pinout for Amphenol 2 (Controls 1-2)



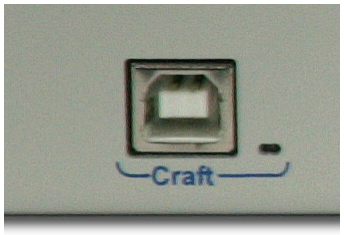
Wire color (wire/stripe)	Connection	66 Block Pair #	Corresponding 50-Pin Connector Pin #
WHT/BLU		1	26
BLU/WHT			1
WHT/ORG		2	27
ORG/WHT			2
WHT/GRN		3	28
GRN/WHT			3
WHT/BRN		4	29
BRN/WHT			4
WHT/GRY		5	30
GRY/WHT			5
RED/BLU		6	31
BLU/RED			6
RED/ORG		7	32
ORG/RED			7
RED/GRN		8	33
GRN/RED			8
RED/BRN	CTRL1 NO	9	34
BRN/RED	CTRL1 CO		9
RED/GRY	CTRL1 NC	10	35
GRY/RED			10
BLK/BLU	CTRL2 NO	11	36
BLU/BLK	CTRL2 CO		11
BLK/ORG	CTRL2 NC	12	37
ORG/BLK			12
BLK/GRN		13	38
GRN/BLK			13
BLK/BRN		14	39
BRN/BLK			14
BLK/GRY		15	40
GRY/BLK			15
YEL/BLU		16	41
BLU/YEL			16
YEL/ORG		17	42
ORG/YEL			17
YEL/GRN		18	43
GRN/YEL			18
YEL/BRN		19	44
BRN/YEL			19
YEL/GRY		20	45
GRY/YEL			20
VIO/BLU		21	46
BLU/VIO			21
VIO/ORG		22	47
ORG/VIO			22
VIO/GRN		23	48
GRN/VIO			23
VIO/BRN		24	49
BRN/VIO			24
VIO/GRY		25	50
GRY/VIO			25

6 Quick Start: How to Connect to the NetGuardian 224A

Most NetGuardian 224A 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 224A and access its Web Browser.

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



NetGuardian 224A Craft Port

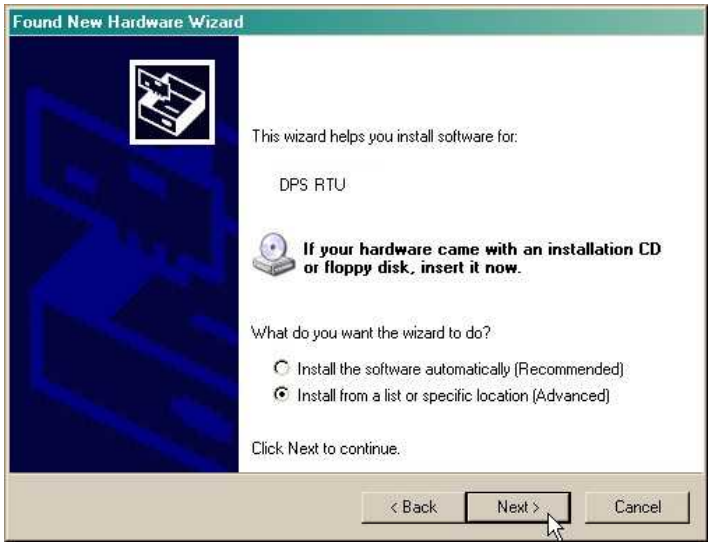
Use the front panel craft port to connect the NetGuardian 224A IT to a PC for onsite unit configuration. To use the craft port, connect the included DB9 download cable from your PC's COM port to the craft port.

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

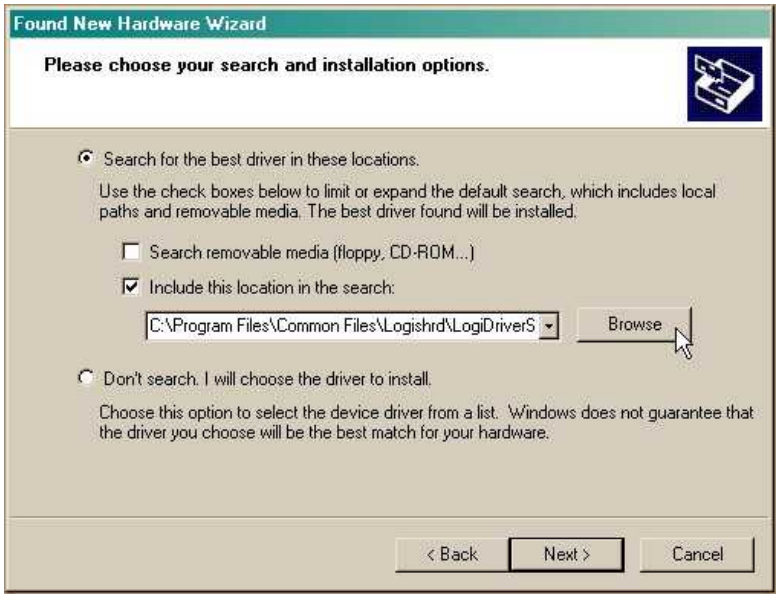
The following steps will occur the first time any DPS USB equipment is used on this PC. If you've used a different DPS USB device before and have installed the DPS USB drivers, then **skip to Step 9**.

When you first connect the NetGuardian 224A to your PC via USB, a "Found New Hardware" message will appear:

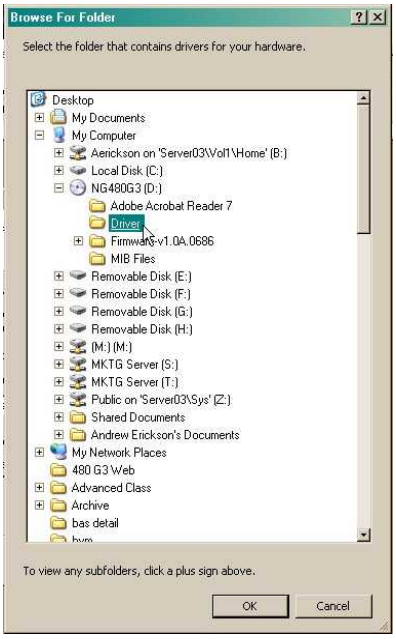
1. Click the "Found New Hardware" message/icon to launch the "Found New Hardware Wizard".



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 224A Resource Disc (CD) into your PC.
6. Click "Browse"

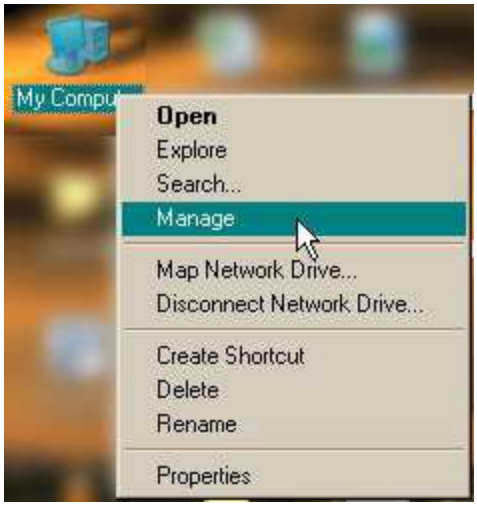


7. Select the "Driver" folder of your NetGuardian 224A Resource Disc Disc (CD) and click "OK"

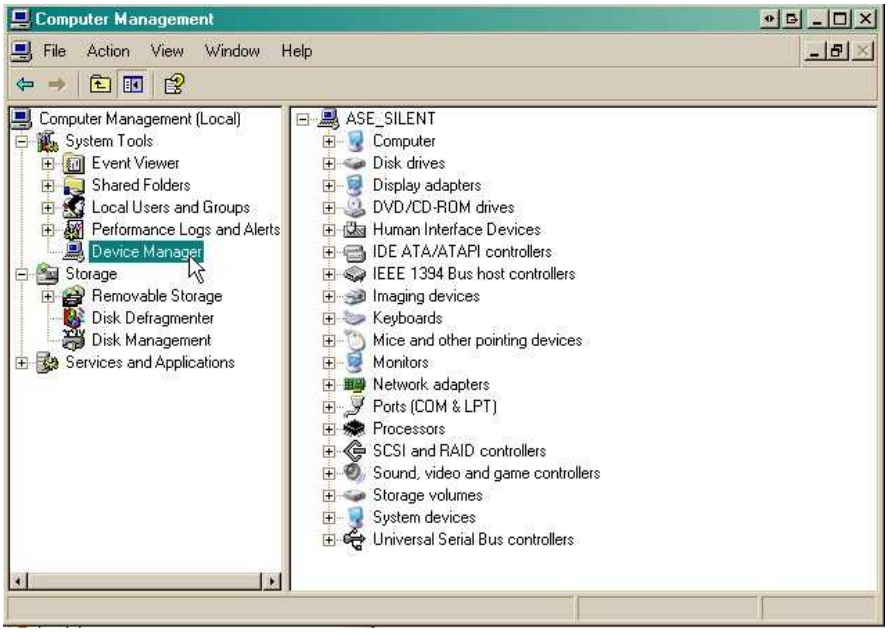
The following message will confirm installation of a new "USB Communications Port"

8. Click "Finish" to close the Wizard.

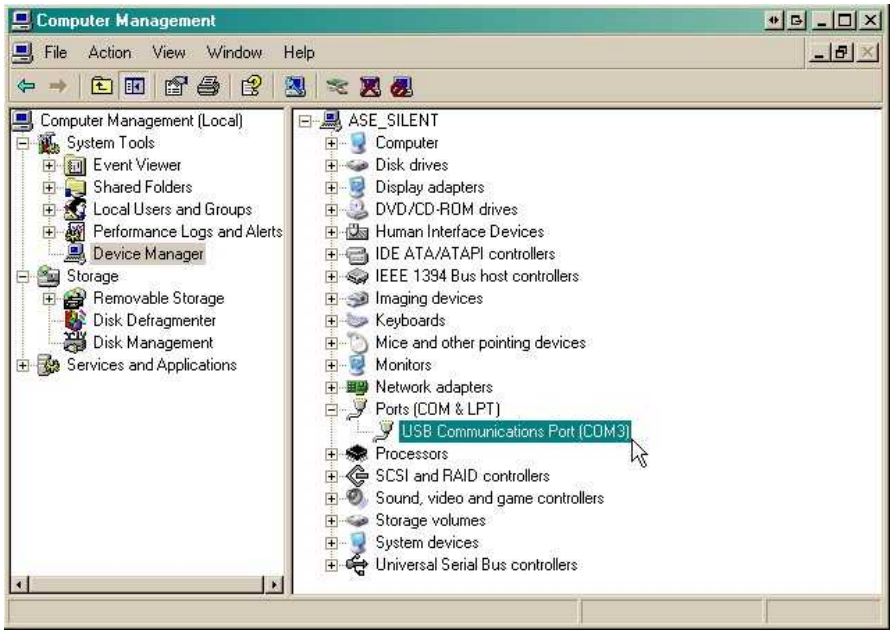
Now that the driver has been installed, a new COM port is being emulated on your PC. Before using hyperterminal, you must confirm the identity of that new COM port (COM1, COM2, COM3...) in the Windows Device Manager.



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).

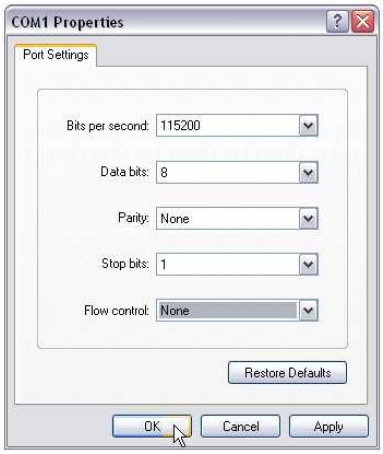
12. Click on the **Start** menu **>** select **Programs** > **Accessories** > **Communications** > **HyperTerminal.**

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.

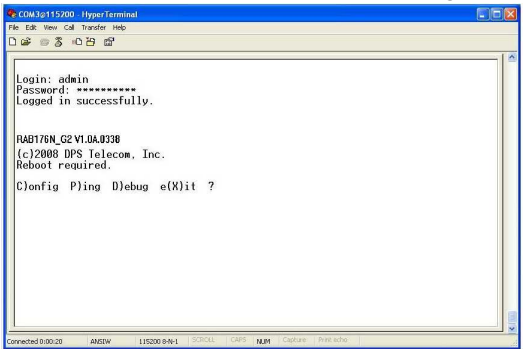
15. Select the following COM port options:
    - Bits per second: 9600
    - Data bits: 8
    - Parity: None
    - Stop bits: 1
    - Flow control: **None**

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

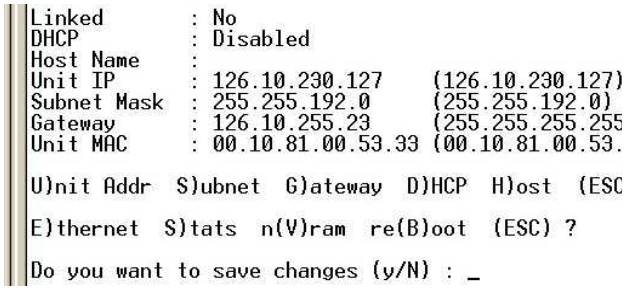


16. When prompted, enter the default user name **admin** and password **dpstelecom**. NOTE**:** If you don't receive a prompt for your user name and password, check the Com port you are using on your PC and make sure you are using the cable provided. Additional cables can be ordered from DPS Telecom.

17. The NetGuardian 224A's main menu will appear. Type C for C)onfig, then E for E)thernet. Configure the unit's IP address, subnet mask, and default gateway.

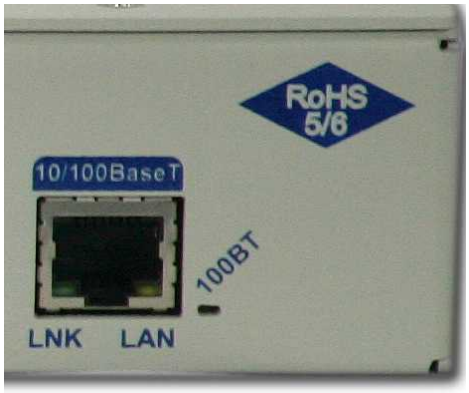


18. ESC to the main menu. When asked if you'd like to save your changes, type Y for Y)es. Reboot the NetGuardian 224A to save its new configuration.



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.

6.2 ...via LAN



NetGuardian 224A Ethernet Port

To connect to the NetGuardian 224A 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 224A, 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 224A's factory default IP settings. Follow these steps:

1. Get a LAN crossover cable and plug it directly into the NetGuardian 224A'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 224A 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 224A and see "Logging On to the NetGuardian 224A" to continue databasing using the Web Browser.

7 TTY Interface

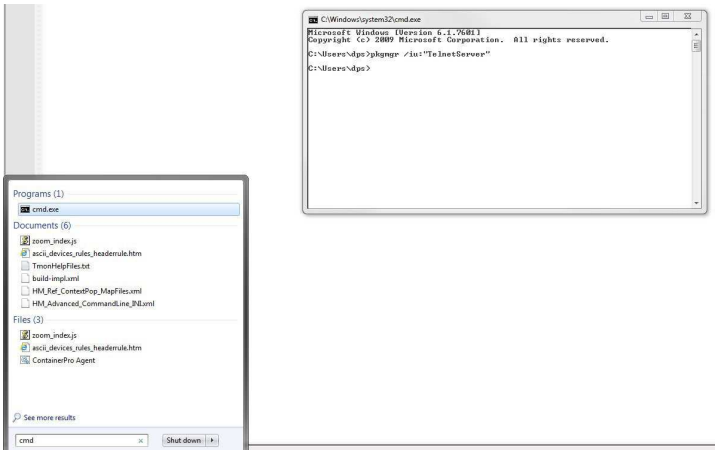
The TTY interface is the NetGuardian 224A's built-in interface for basic configuration. From the TTY interface, you can:

- 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.

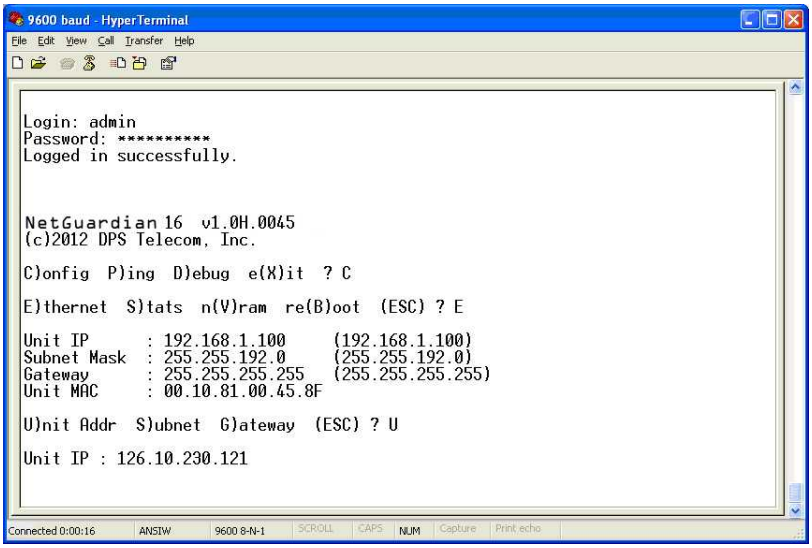


From the command line, type in **pkgmgr /iu:"TelnetClient"** then press **enter**. When the command prompt appears again, the installation is complete.

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.

7.1 Configure Serial Port via TTY



Serial port configuration

1. To enter configuration setting for the Serial Port, login to the TTY interface and press **C)onfig** > **s(E)rial**.

2. Press the hot keys to toggle through the following options. (* Indicates default settings:)
   NOTE: Default settings may not reflect the primary interface that shipped in the unit.
   - **Port Type**: 232*, 485
   - **Baud**: 9600*, 57600, 19200, 9600, 4800, 2400, 1200
   - **Parity**: None*, even, odd
   - **Stop bits**: 1*, 2

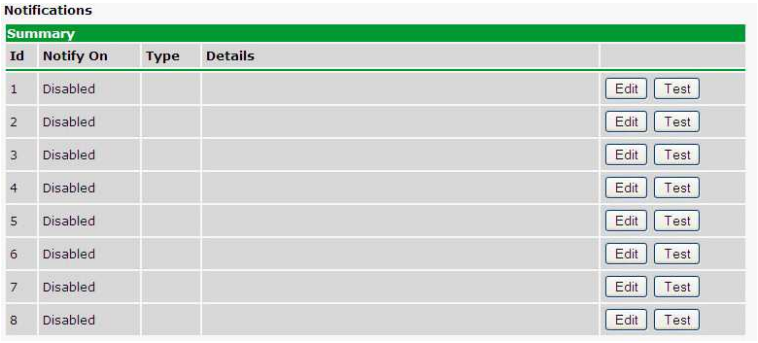
3. Set the RTS head / tail (Carrier time) Suggested settings are: 0,0 if using RS232.

8 Quick Turn Up

The next sections of this manual will walk you through some of the most common tasks for using the NetGuardian 224A. 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.

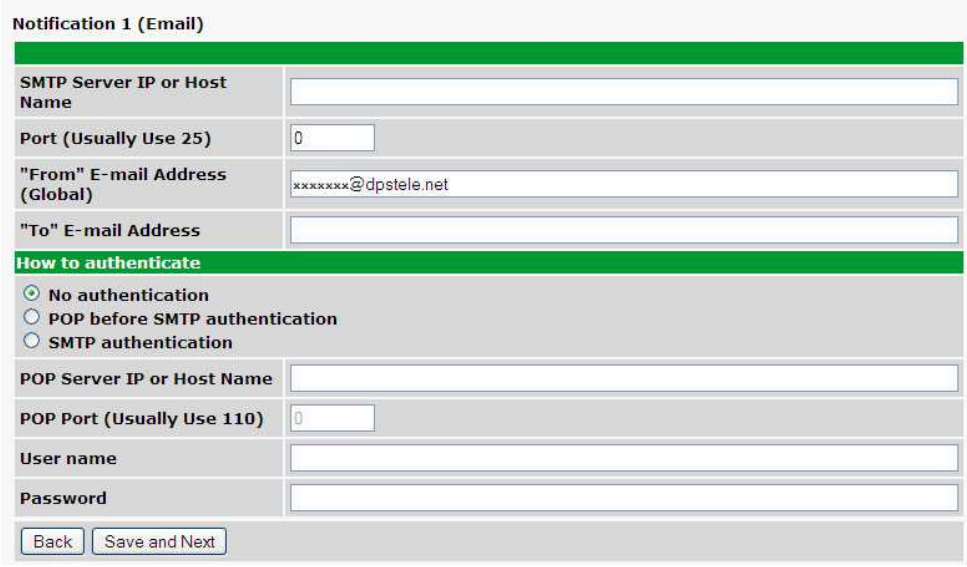
8.1 How to Send Email Notifications

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.



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**.

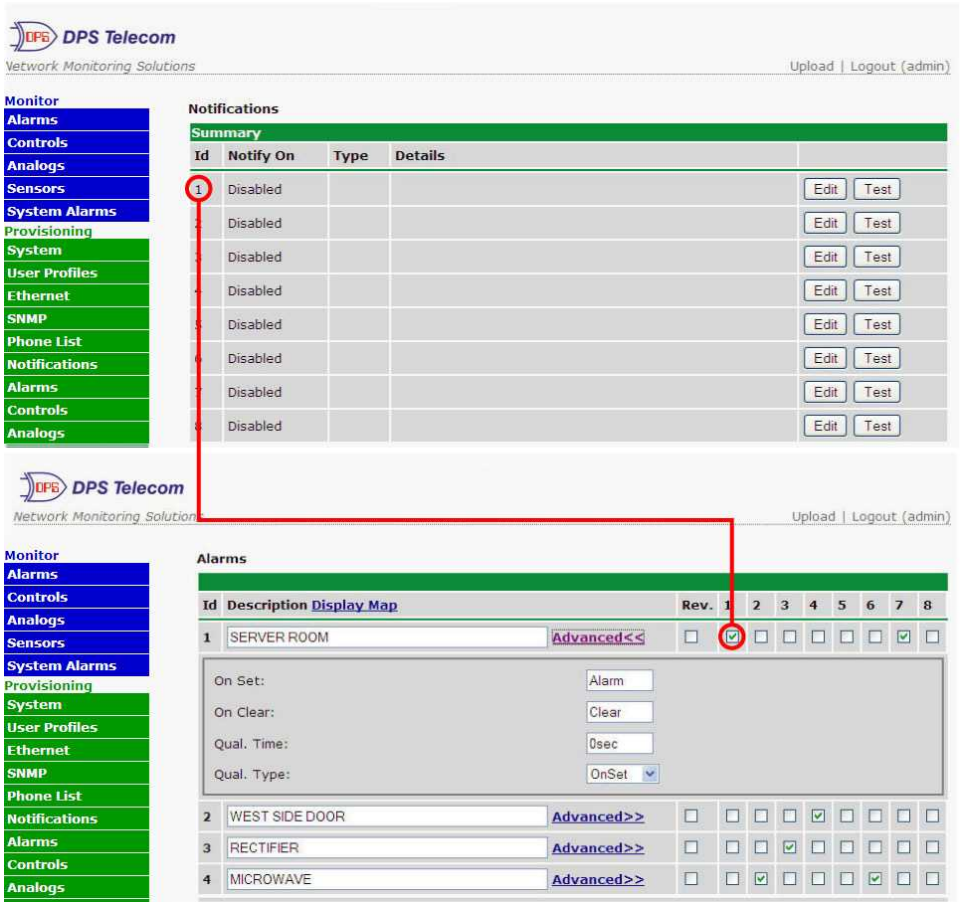
3. At the **Email Notification** screen, you'll enter your email server settings. Enter the **IP address** or **Host Name** of your email server. Enter the **Port Number** (usually 25) and the **"To" Email Address** of the technician that will receive these emails. If authentication is required, chose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



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.)

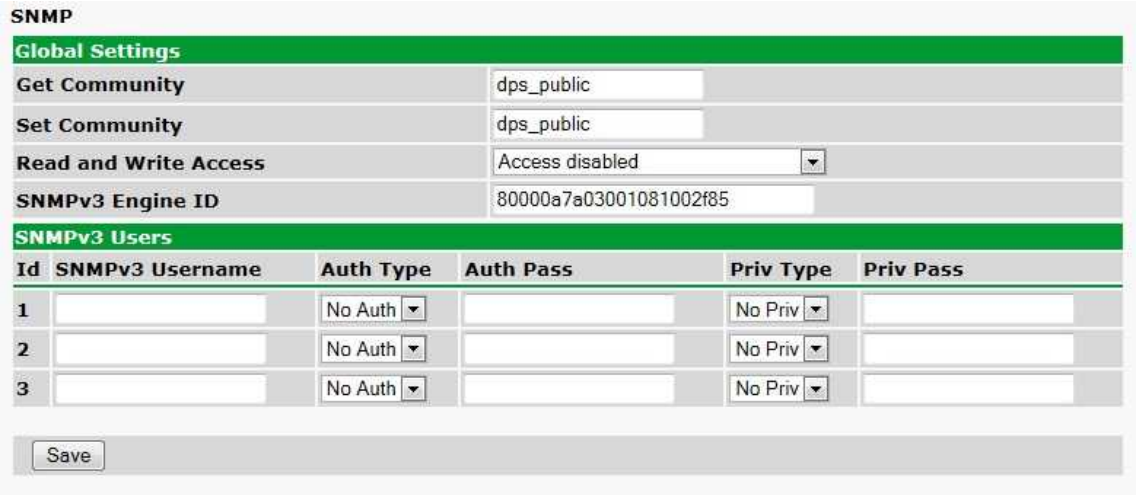
5. If you chose to test the email notification you've just setup, you will prompted with a pop up . Click **OK** to send a test email alarm notification. Confirm all your settings by checking your email to see if you've received it. **NOTE:** This test only means that your notification settings are correct,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

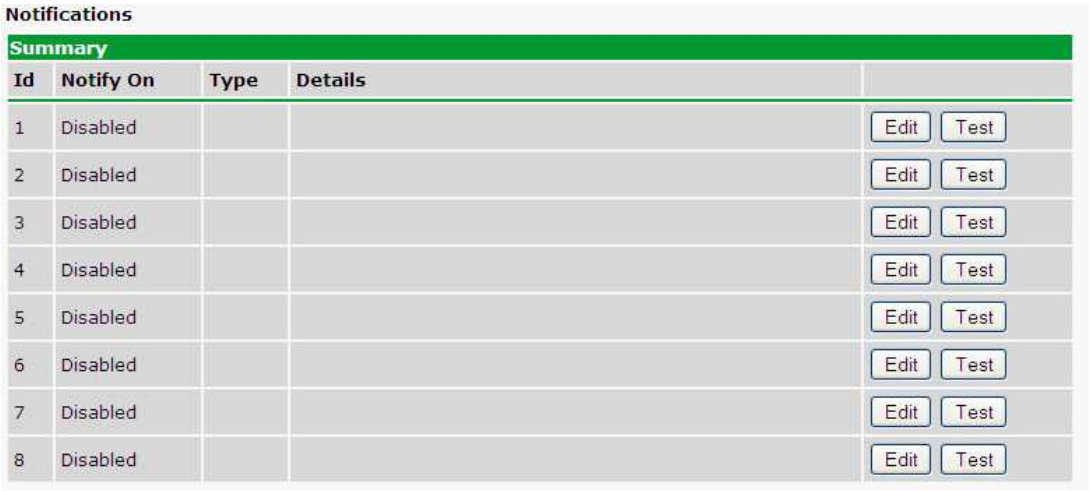


8.2 How to Send SNMP Traps

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".

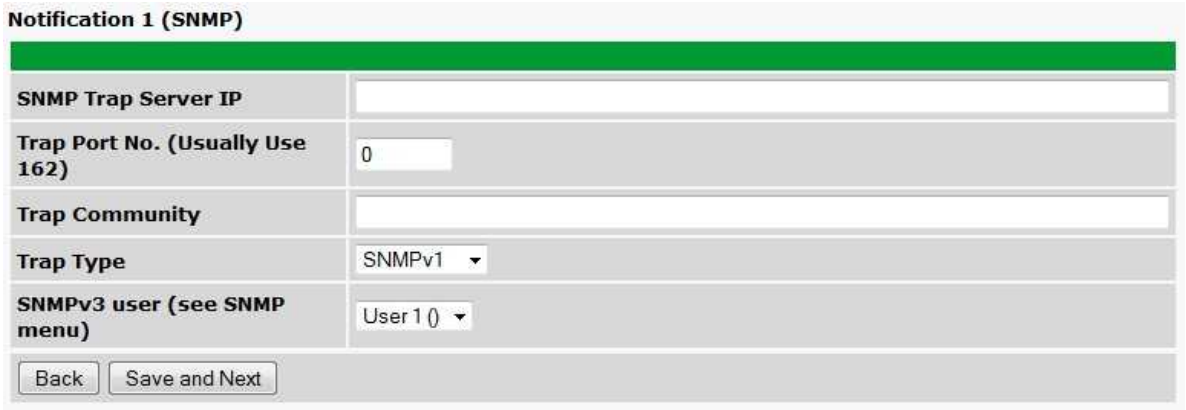


2. Click on the **Notifications** button in the **Provisioning** menu. You can setup as many as 8 different notifications. Begin the setup "wizard" by clicking **Edit** for a notification number. In this example, we'll setup Notification 1 to send SNMP traps to your alarm master.



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.

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**.



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.)

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.

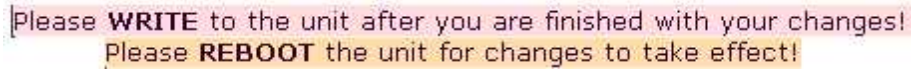
NOTE: This test only means that your notification settings are correct, but you still need to assign the notification to an alarm point. See Step 6 in "How to Send Email Notifications" for more detail.

9 Provisioning Menu Field Descriptions

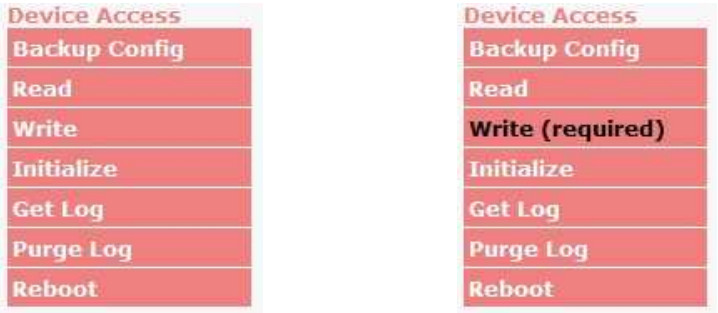
NetGuardian 224A configuration is performed from the **Provisioning** menus, the menu options in green on the left-side of the web interface. The following pages provide a brief description of the options available in each menu.

Saving Configuration Changes to the NetGuardian 224A:
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.



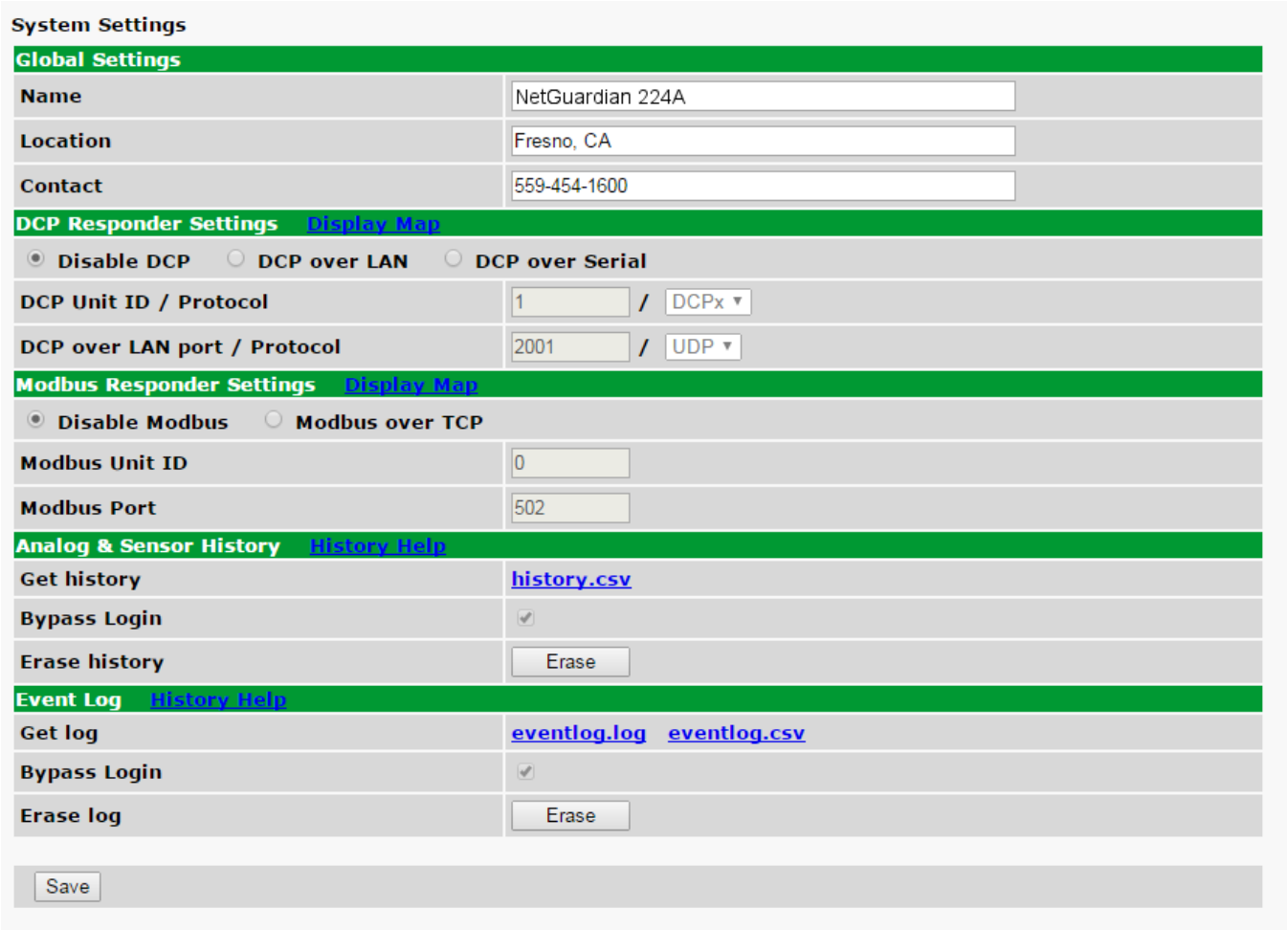
Status messages on the NetGuardian 224A Device Access menu, inform you how to implement your changes



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

9.1 System

From the **Provisioning** > **System** menu, you will configure and edit the global system, call, T/Mon and control settings for the NetGuardian 224A.



The Provisioning > System menu

Global System Settings	
Name	A name for this NetGuardian 224A unit. (Optional field)
Location	The location of this NetGuardian 224A unit. (Optional field)
Contact	Contact telephone number for the person responsible for this NetGuardian 224A unit. (Optional field)
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
Modbus Responder Settings	
Modbus Unit ID	User-definable ID number (Modbus Address)
Modbus Port	Enter the Modbus port number
Analog & Sensor History	
Get History	Download a log of all configured analog and sensor values.
Bypass Login	File can be downloaded without logging in when checked.
Erase History	Erase the log of all configured analog and sensor values.

Event Log	
Get Log	Download a log of all alarm events in either plain text (event.log, open with notepad) or spreadsheet format (eventlog.csv, open with Excel).
Bypass Login	File can be downloaded without logging in when checked.
Purge Log	Erase the log of all alarm events.

9.1.1 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:

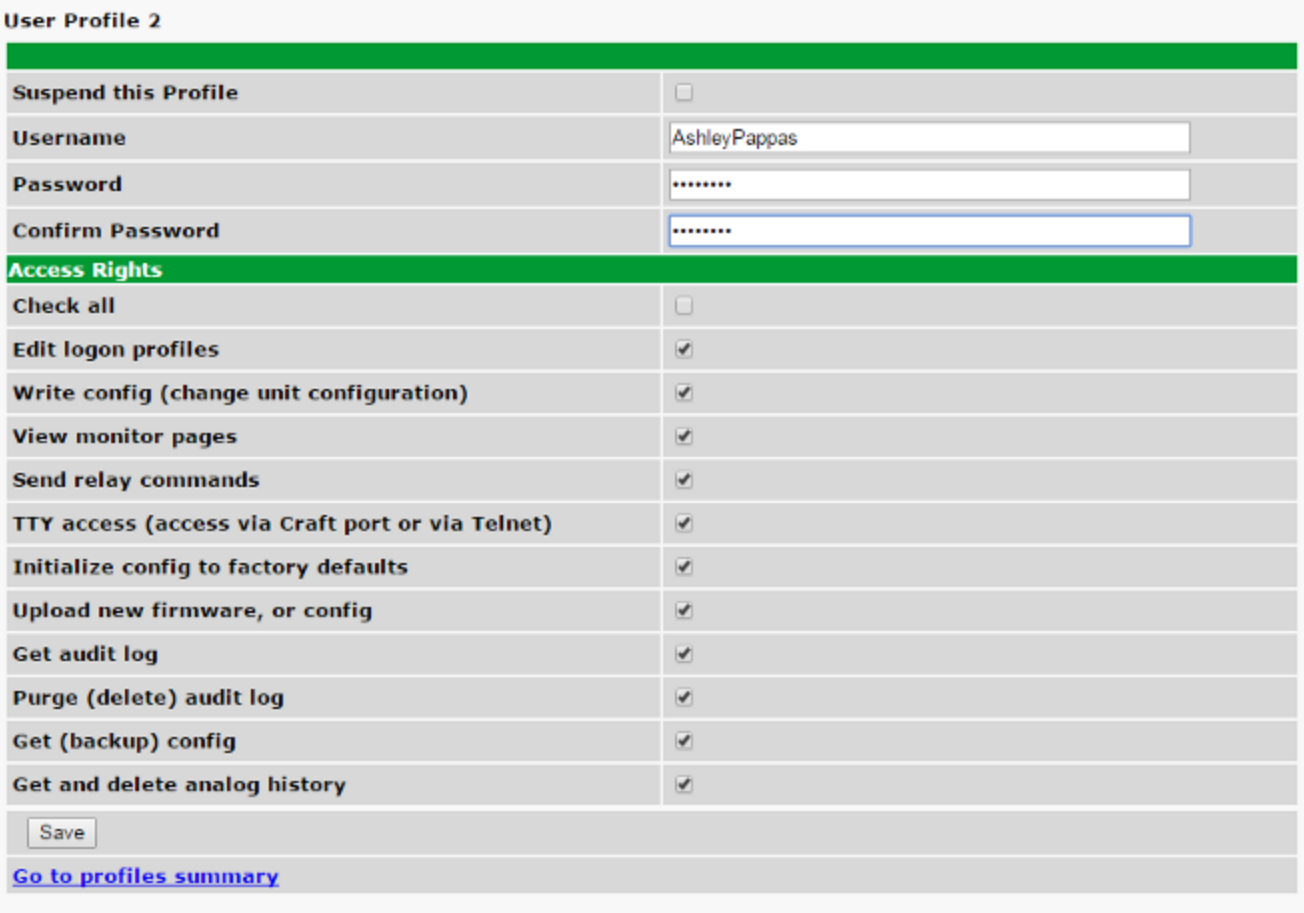
```
systime,utime,chan,romid,description,average,minimum,maximum,units,ukey1,ukey2,ukey3
2011-02-03 11:13:27,1296731607,9,28E5644407000046,test,75.750,75.750,75.750,F,,,
2011-02-03 11:12:27,1296731547,9,28E5644407000046,test,75.750,75.750,75.750,F,,,
2011-02-03 11:11:27,1296731487,9,28E5644407000046,test,75.750,75.750,75.750,F,,,
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.

9.2 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 224A's web interface.



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.

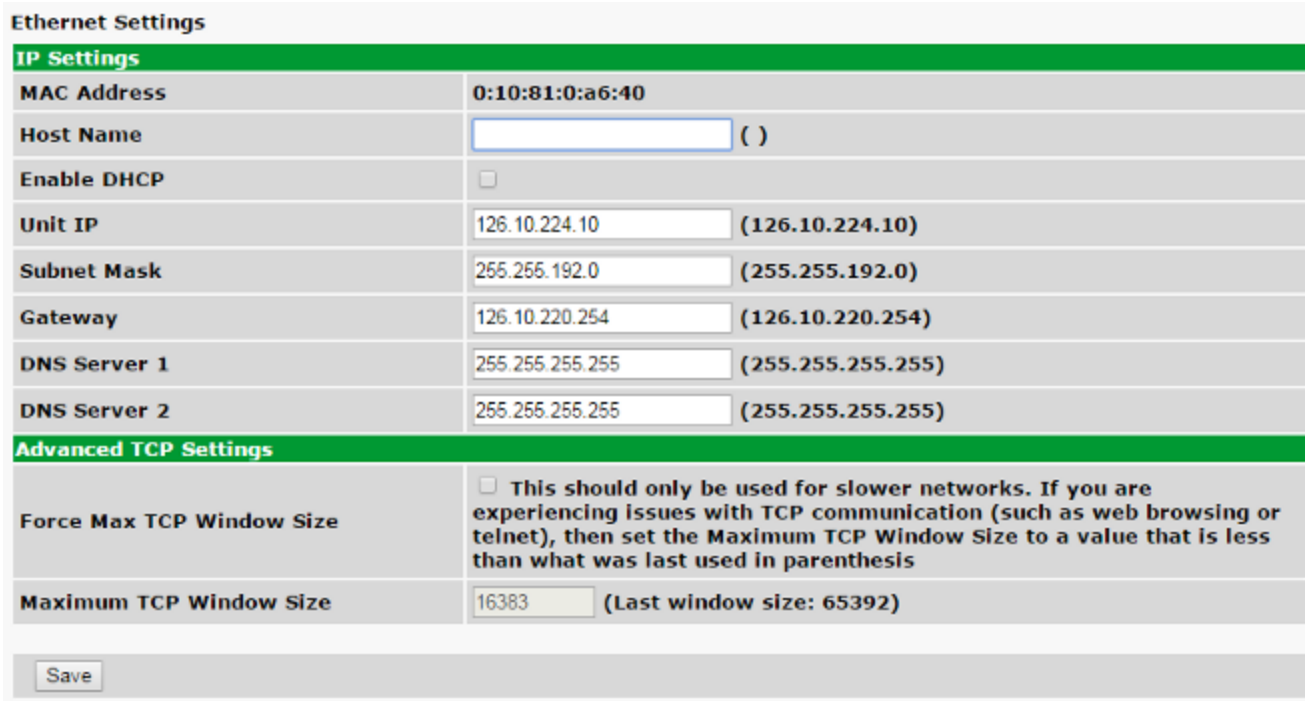
	User Profile
Suspend this Profile	If this box is checked, the profile will not be able to access the NetGuardian 224A.
Username	Enter a username or a user description
Password	Enter a unique user password **Note:** All passwords are AES 128 encrypted.
Confirm Password	Re-enter the password.
Access Rights	
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	Allows the user to use the **Initialize** option in the **Device Access** menu, resetting the

	User Profile
factory defaults	NetGuardian 224A to factory default settings. All user settings will be lost.
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 log	Allows the user to deletes the existing audit 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

9.3 Ethernet

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



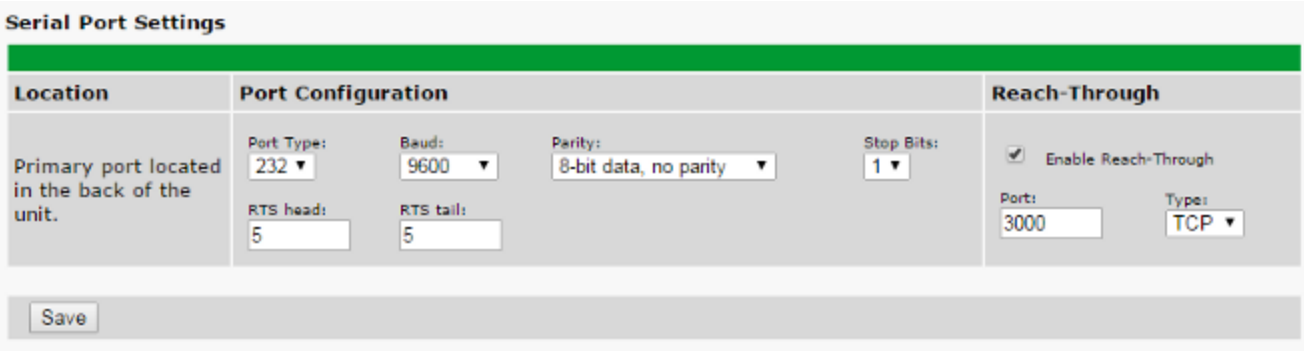
The Provisioning > Ethernet menu

Ethernet Settings	
MAC Address	Hardware address of the NetGuardian 224A. (Not editable - For reference only.)
Host Name	Used only for web browsing. Example: If you don't want to remember this NetGuardian 224A's IP address, you can type in a name is this field, such as "MyNetGuardian 224A". Once you save and reboot the unit, you can now browse to it locally by simply typing in "MyNetGuardian 224A" 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 224A.
Subnet Mask	A road sign to the NetGuardian 224A, 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 224A 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.

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

9.4 Serial Port

The **Provisioning > Serial Port** menu allows you to change settings depending on the port type of your NetGuardian 224A. From this menu, you can select a mode of operation and enable reach-through serial port functionality.

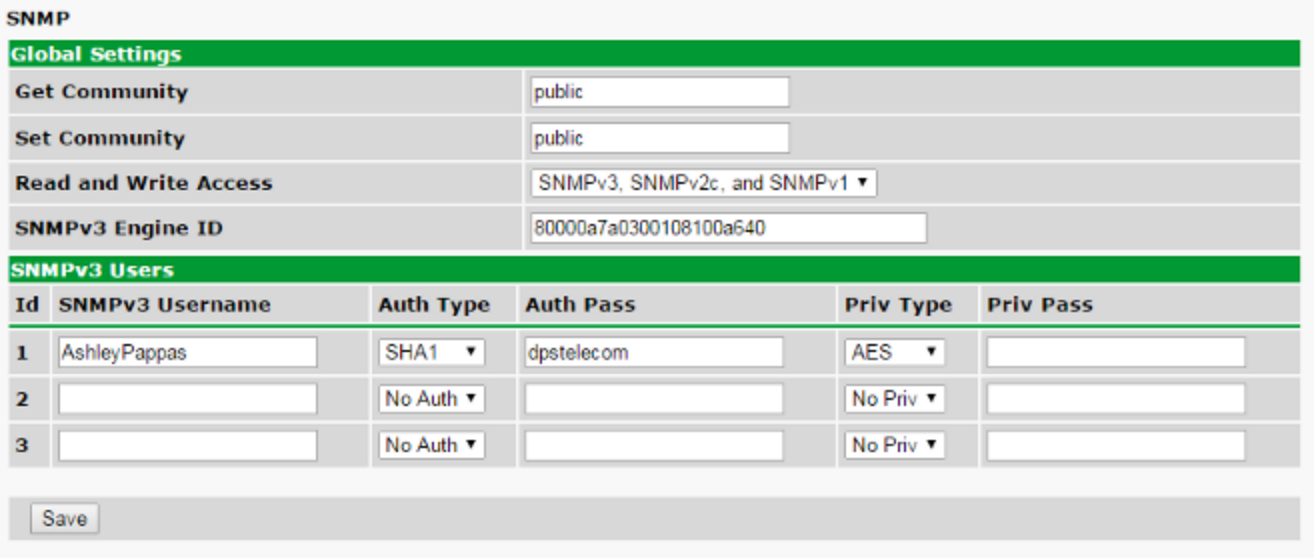


The Provisioning > Serial Ports menu

Location	
A reminder that your primary serial port is located on the back of the NetGuardian 224A chassis.	
Port Configuration	
Port Type	Select the serial port for your build of the NetGuardian 224A. 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 224A was built with a 202 modem. The most commonly used value is 30.
RTS Tail	Only used if your NetGuardian 224A 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.

9.5 SNMP

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



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 224A 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

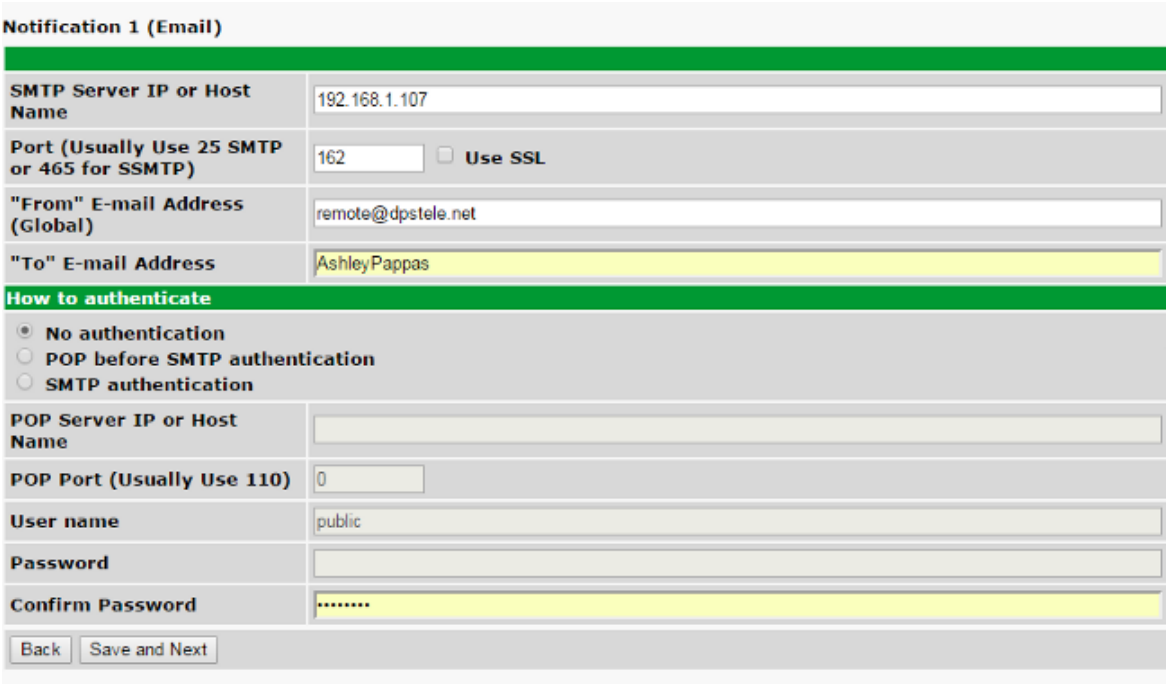
Fields in the Provisioning > SNMP settings

9.6 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).

9.6.1 Notification Settings

Email Notification Fields

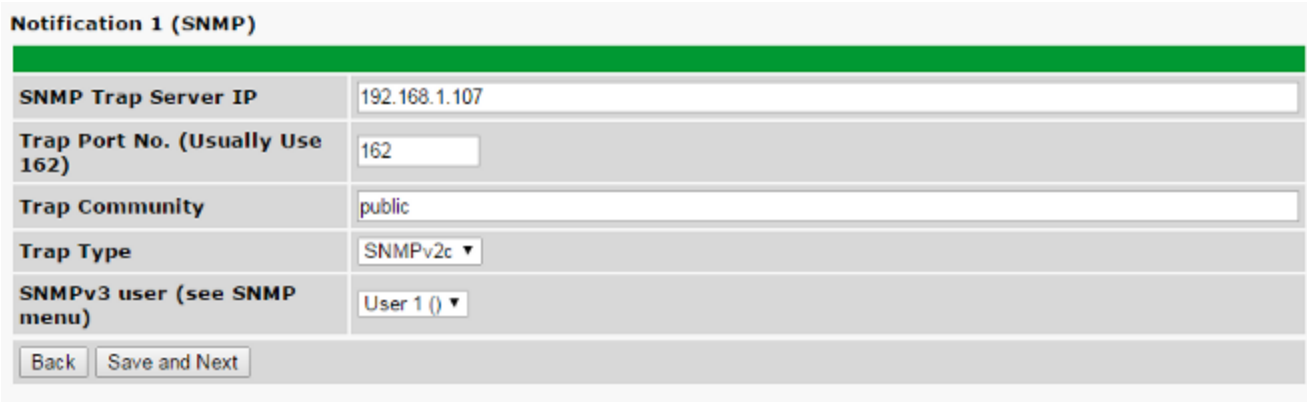


Editing Email Notification Settings

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 224A will send emails from. Not editable from this screen.
"To" E-mail Address	The email address of the person responsible for this NetGuardian 224A, 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.

SNMP Notification Fields



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.

9.6.2 Schedule

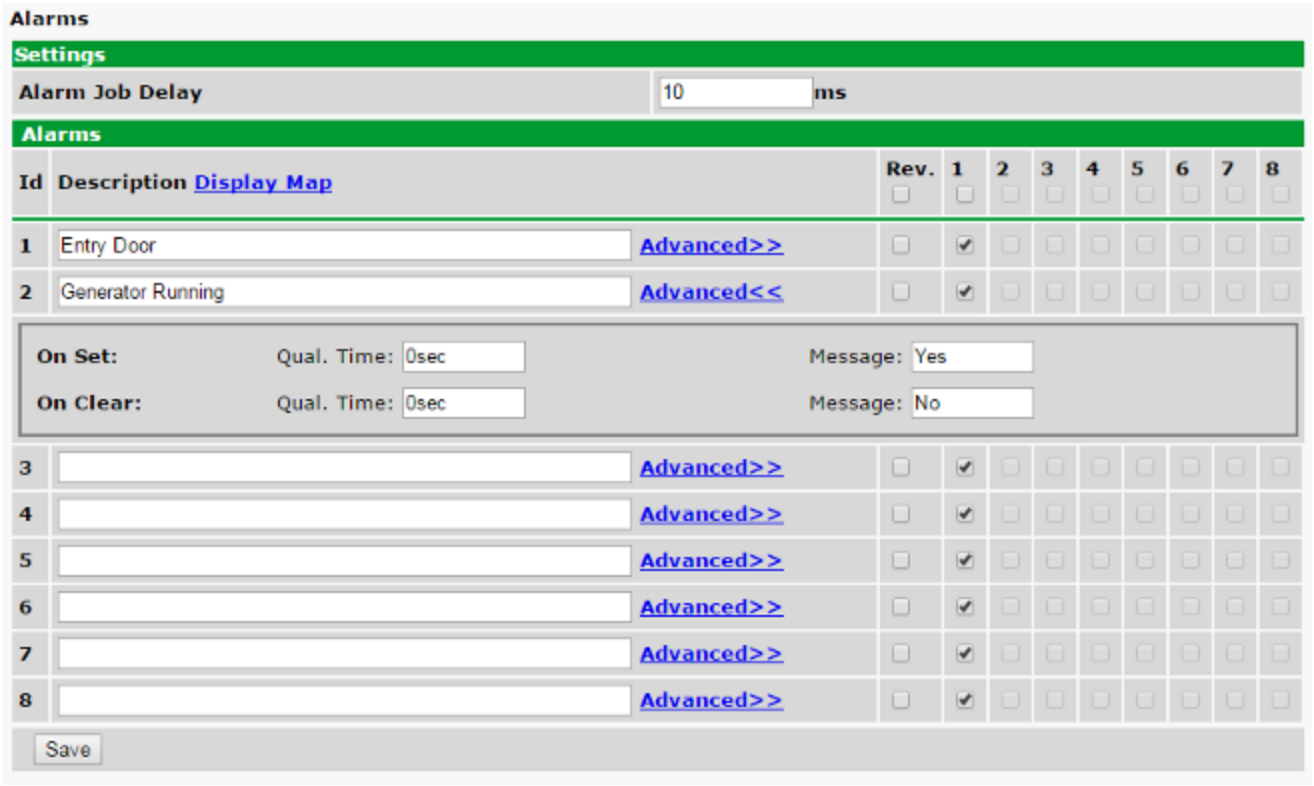
The notifications scheduling menu is where you will tell the NetGuardian 224A exactly which days and times you want to receive alarm notifications. You set 2 different schedules for each.

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.

9.7 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.

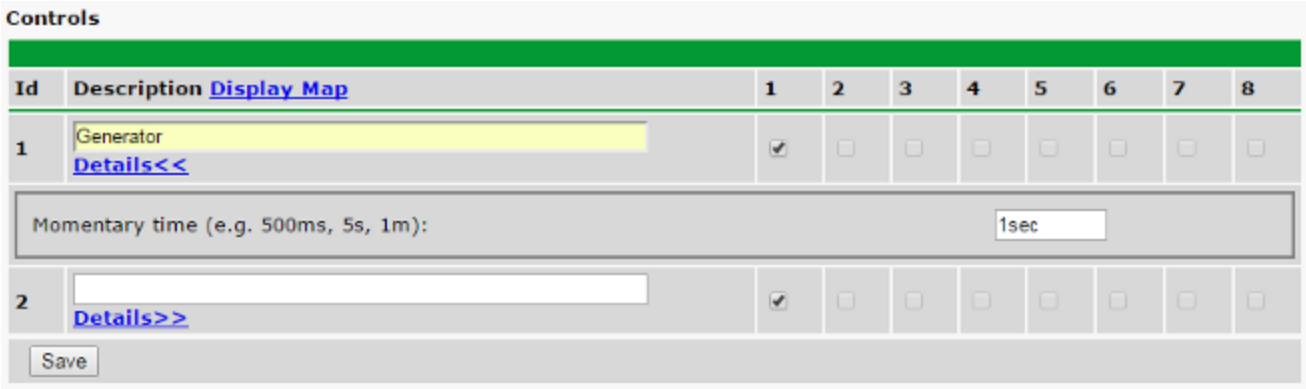


The Provisioning > Alarms menu

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.

9.8 Controls

The NetGuardian 224A's 2 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).

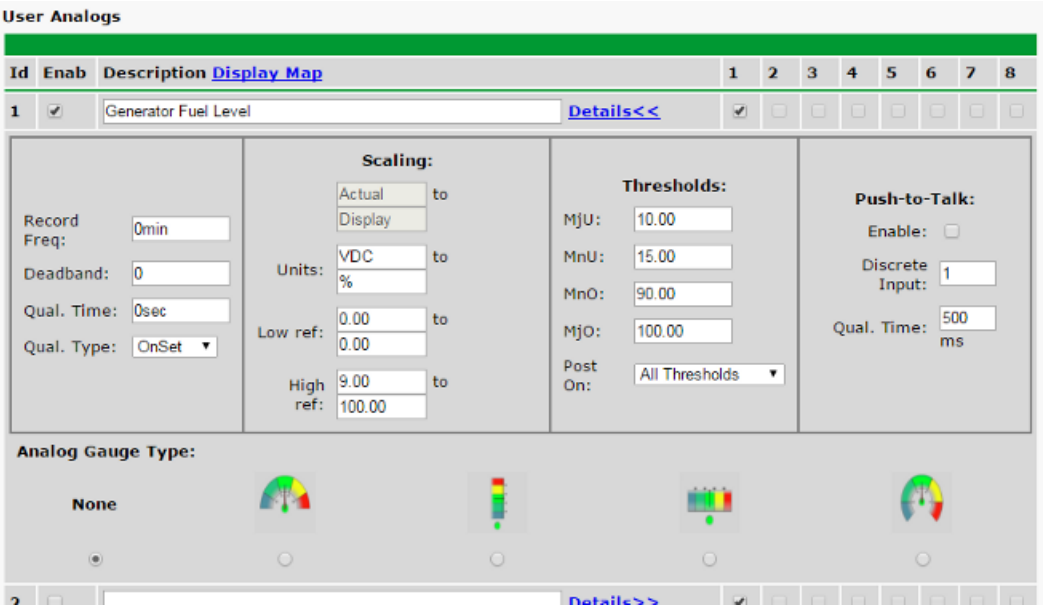


The Provisioning > Controls screen

Basic Controls Configuration	
ID	ID number for the control relay.
Description	User-definable description for the NetGuardian 224A's control relay.
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.

9.9 User Analogs

The NetGuardian 224's two 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**.



The Provisioning > User Analogs menu

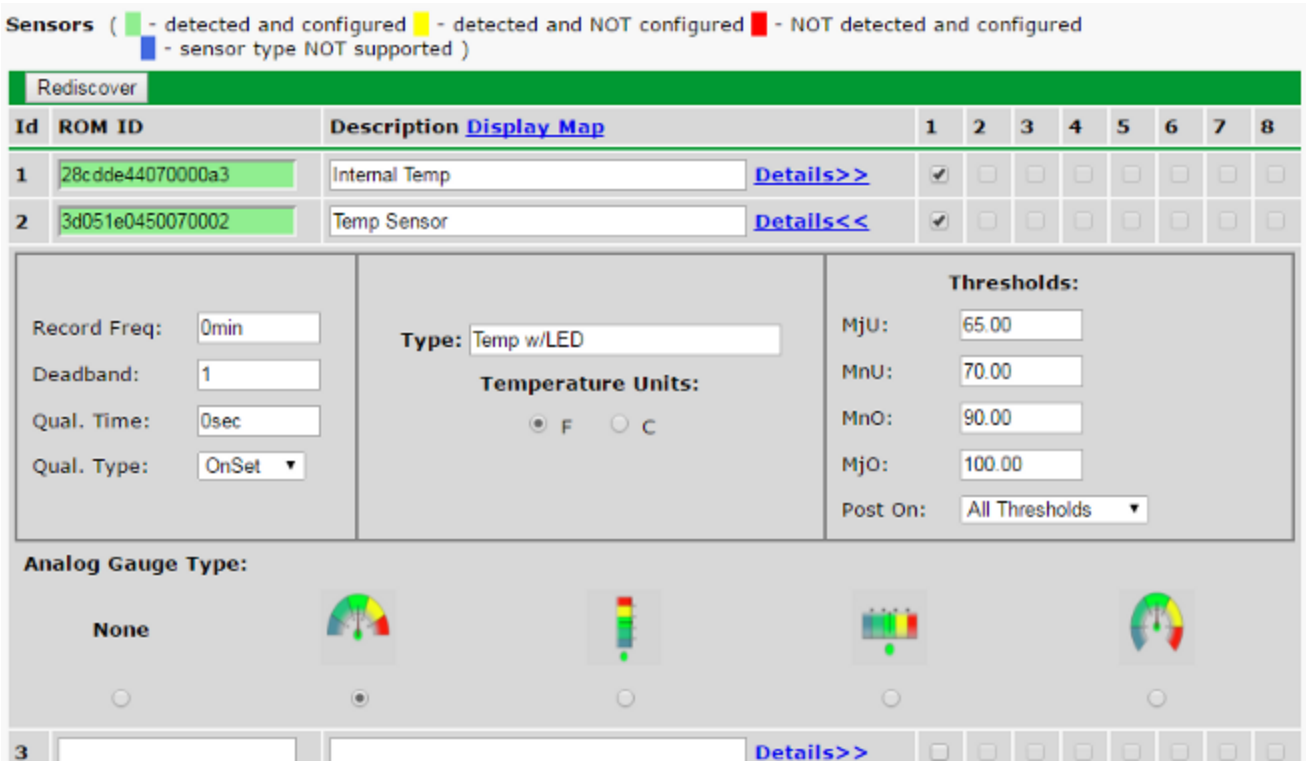
User Analogs	
Default monitoring to gauge view	Checking this box sets the default view in the **Monitor>User Analogs** menu to the gauge view.
Enab (Enable)	Checking the box in the **Enab** column enables monitoring of the analog channel.
Description	User-definable description for the analog channel
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.
Post On	Select the threshold alarms to post. All thresholds, Major Only, Minor Only, Major Over Only, Major Under Only.
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

9.10 Sensors

D-Wire Sensors
The NetGuardian 224A supports up to 32 daisy-chained D-Wire sensors via its D-Wire input. Sensors connected to the NetGuardian 224A 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 224A'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 224A'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.



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 224A 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 224A. 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).
Post On	Select the threshold alarms to post. All thresholds, Major Only, Minor Only, Mojor Over Only, Major Under Only.
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.

9.10.1 HVAC Monitoring

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

Sensor with HVAC Monitoring enabled.

HVAC Monitor Mode	
HVAC Start 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 Airflow sensor
Air Flow Thresholds	Set MjU to -20
	Set MnU to -10
	Set MnO to a small 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 HVAC Start 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 HVAC Start Time expires.

9.10.2 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
p	Point Index

Valid operations:	
+	Addition[1]
-	Subtraction
*****	Multiplication[1]
/	Division[2]
>	Greater than
<	Less than
|	Conditional Halt[3]
=	Assignment

1. Can be used as OR (+) operator / AND (*) operator when used with assignment (=) operator.
2. Division is NOT executed if the denominator's absolute value is less than 1!
3. 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.

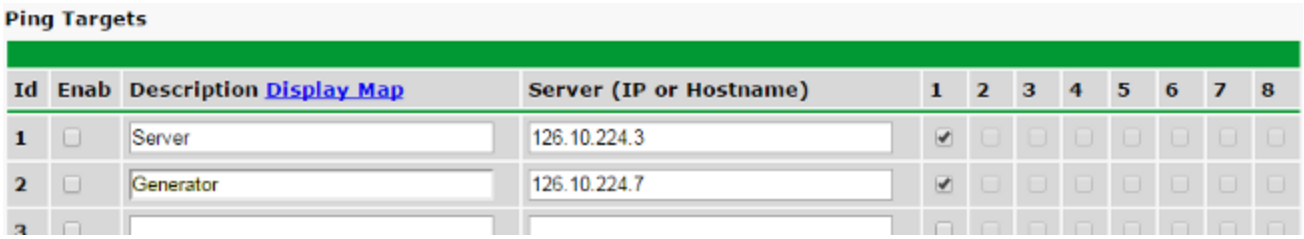
Equation: d1 d2 + d3 * r1 =

Input	Operation	Stack	Comment
d1	Push value	d1	
d2	Push value	d2 d1	
+	OR	(d1+d2)	Pop d1 and d2, OR them, push result to stack
d3	Push value	d3 (d1+d2)	
*****	AND	(d1+d2)*d3	Pop (d1+d2) and d3, AND them, push result to stack
r1	Push value	r1 (d1+d2)*d3	
=	Assign Value	r1=(d1+d2)*d3	Pop (d1+d2)*d3 and r1and assign value to r1

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

9.11 Ping Targets

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

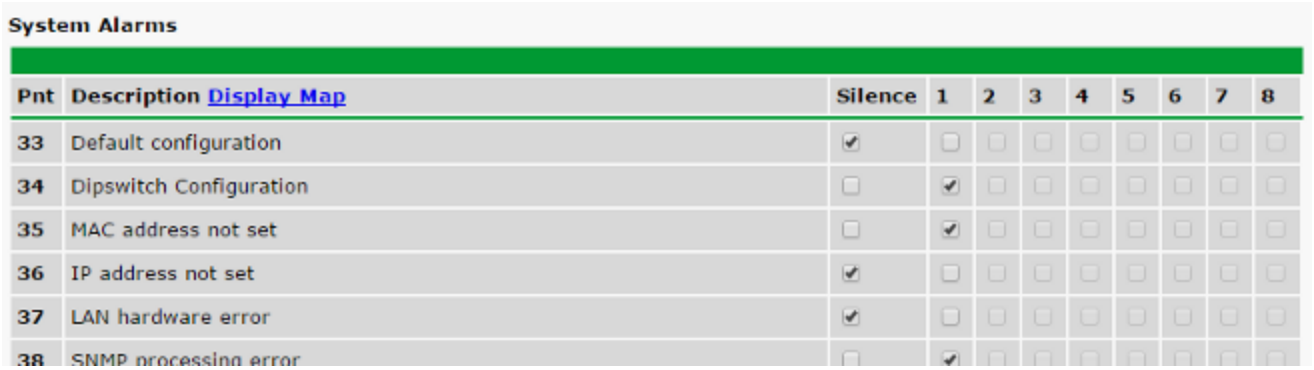


The Provisioning > Ping Targets menu

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.

9.12 System Alarms

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

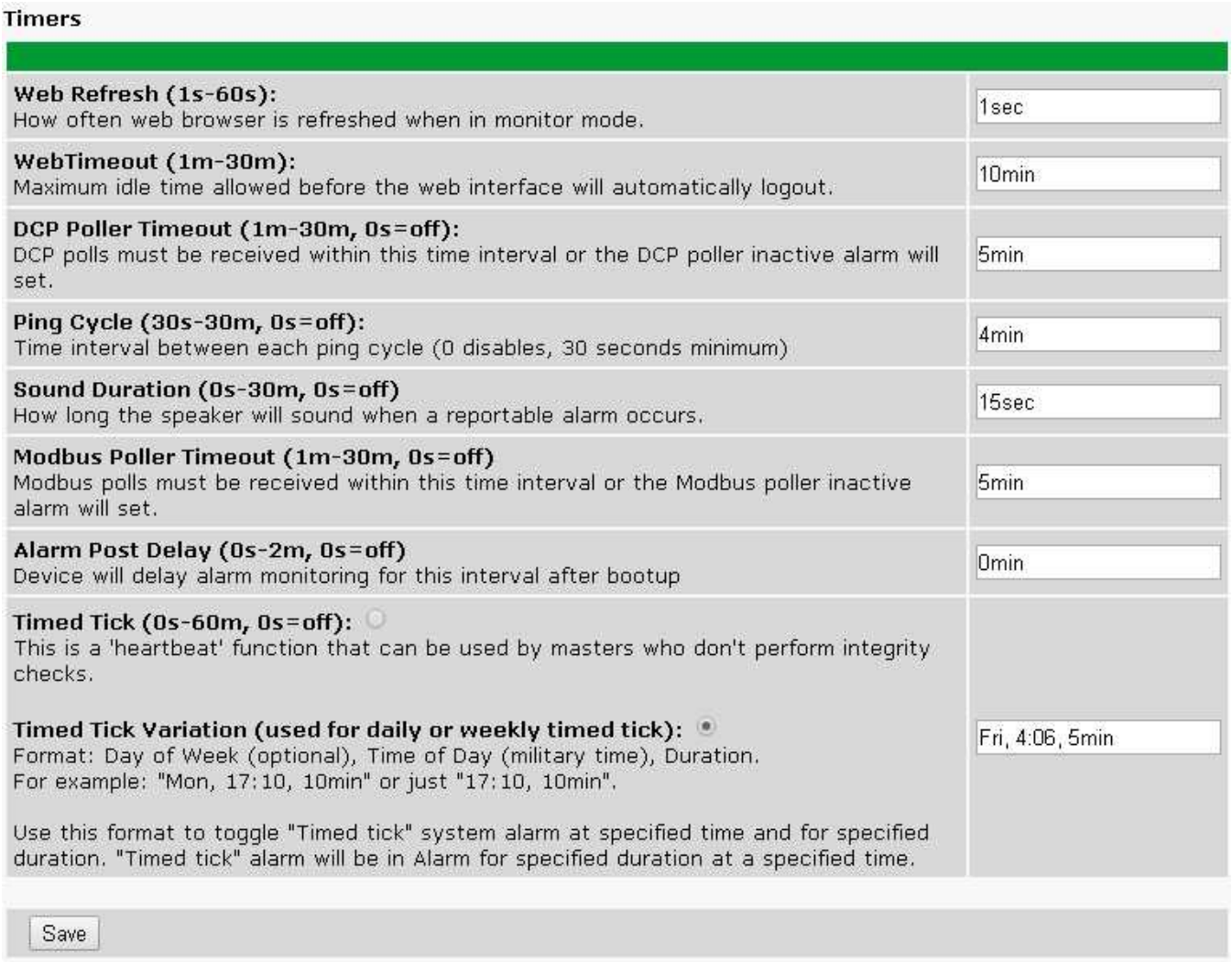


The Provisioning > System Alarms menu

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.

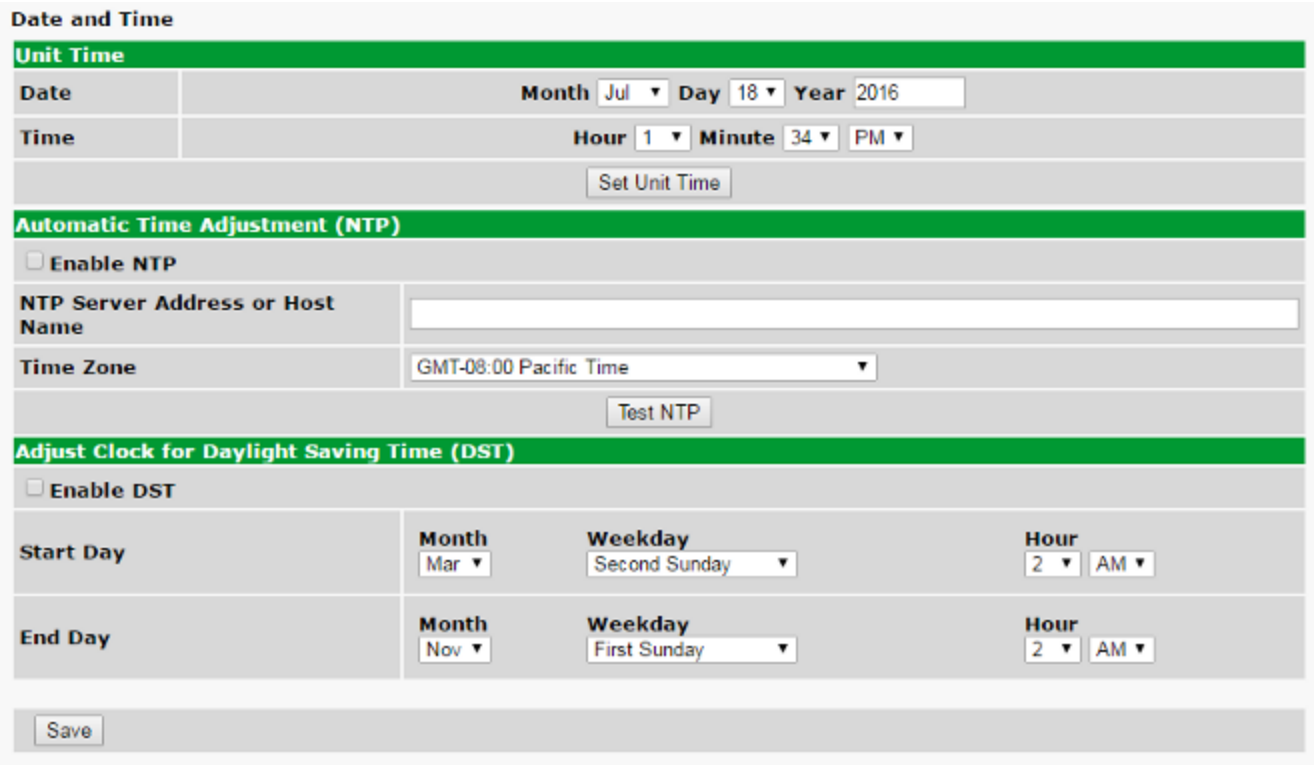
9.13 Timers

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



The Provisioning > Timers menu

9.14 Date and Time



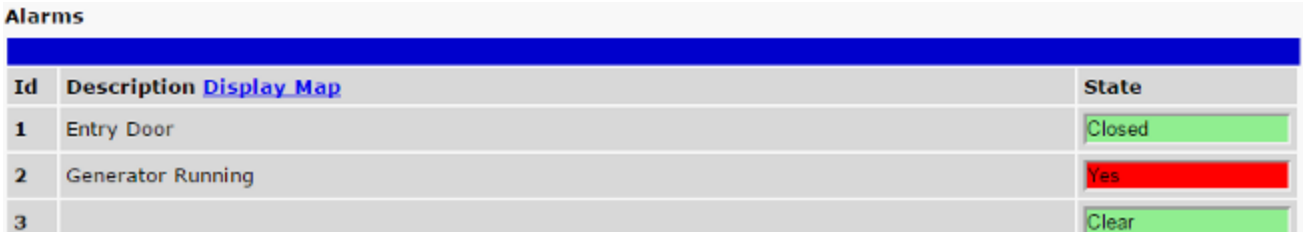
The Provisioning > Date and Time menu

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 224A 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.

10 Monitoring via the Web Browser

10.1 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.



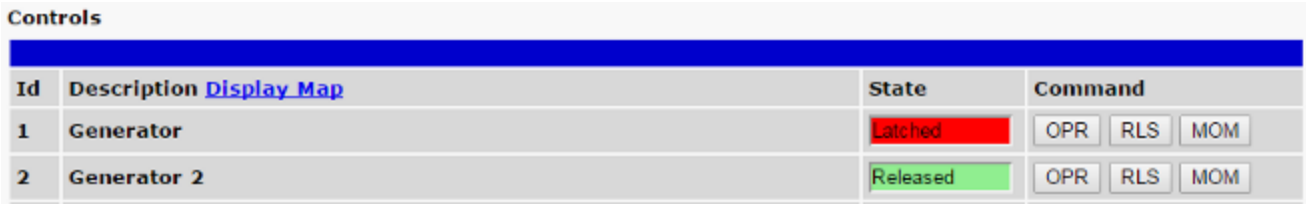
Click on Alarms in the Monitor menu to see if any base alarms (1-8) have been triggered.

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)

10.2 Controls

Use the following rules to operate the NetGuardian 224A'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)

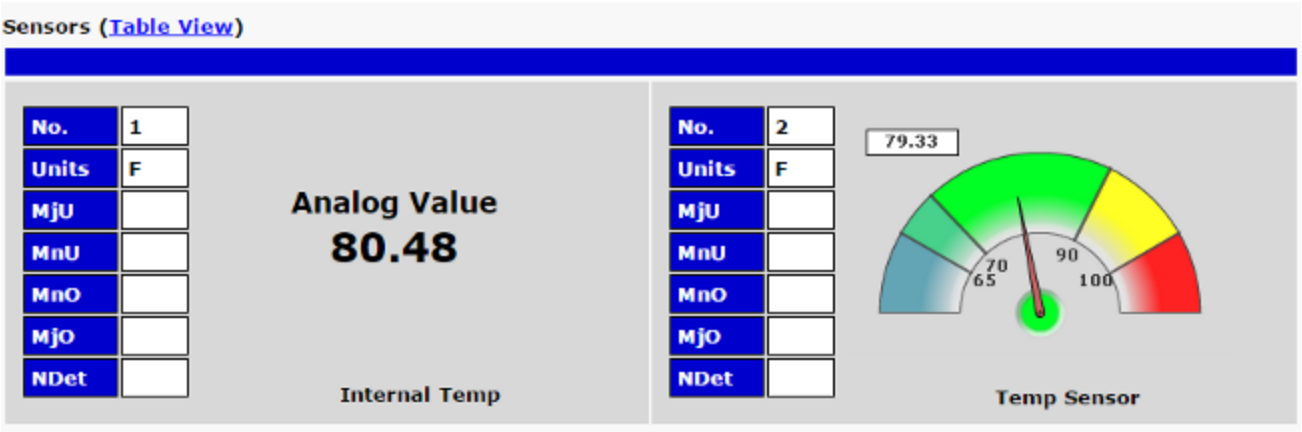


View and operate control relays from the Monitor > Controls menu

Control Relay Operation	
ID	ID number for the control relay.
Description	Description for the NetGuardian 224A'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.

10.3 Sensors

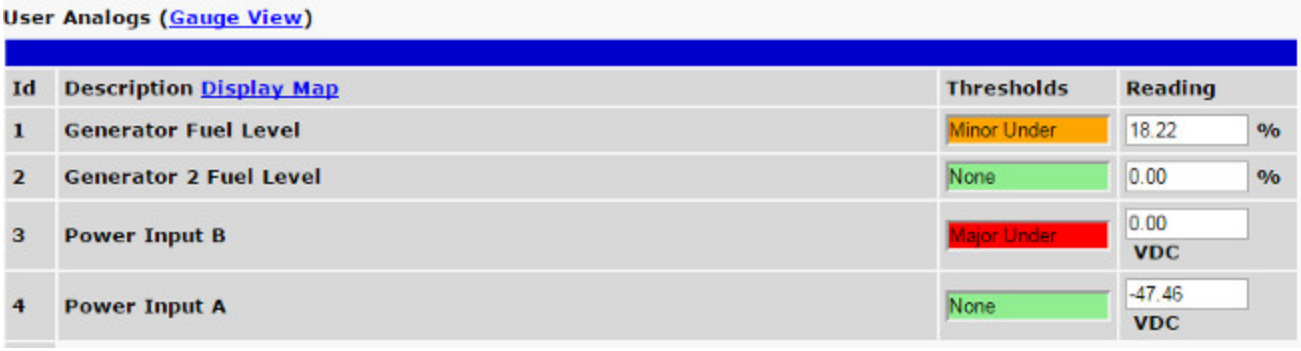
This selection provides the status of the system's analog channels by indicating if an alarm has been triggered. The **Monitor** > **Sensors** screen provides a description of each analog channel, the current reading, the units being read, and alarm conditions (major under, minor under, major over, minor 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.



The Monitor > Sensors menu

10.4 User Analogs

On the **Monitor > User Analogs** menu, you can monitor all analog inputs. The most recent measurement will be shown, and any alarm thresholds crossed will be shown in shown in either orange for minor alarms or red for major alarms.



User Analogs (Gauge View)

Id	Description Display Map	Thresholds	Reading
1	Generator Fuel Level	Minor Under	18.22 %
2	Generator 2 Fuel Level	None	0.00 %
3	Power Input B	Major Under	0.00 VDC
4	Power Input A	None	-47.46 VDC

Fig. 12.5 *Current status of all analog inputs in the Monitor > User Analogs in Table View.*

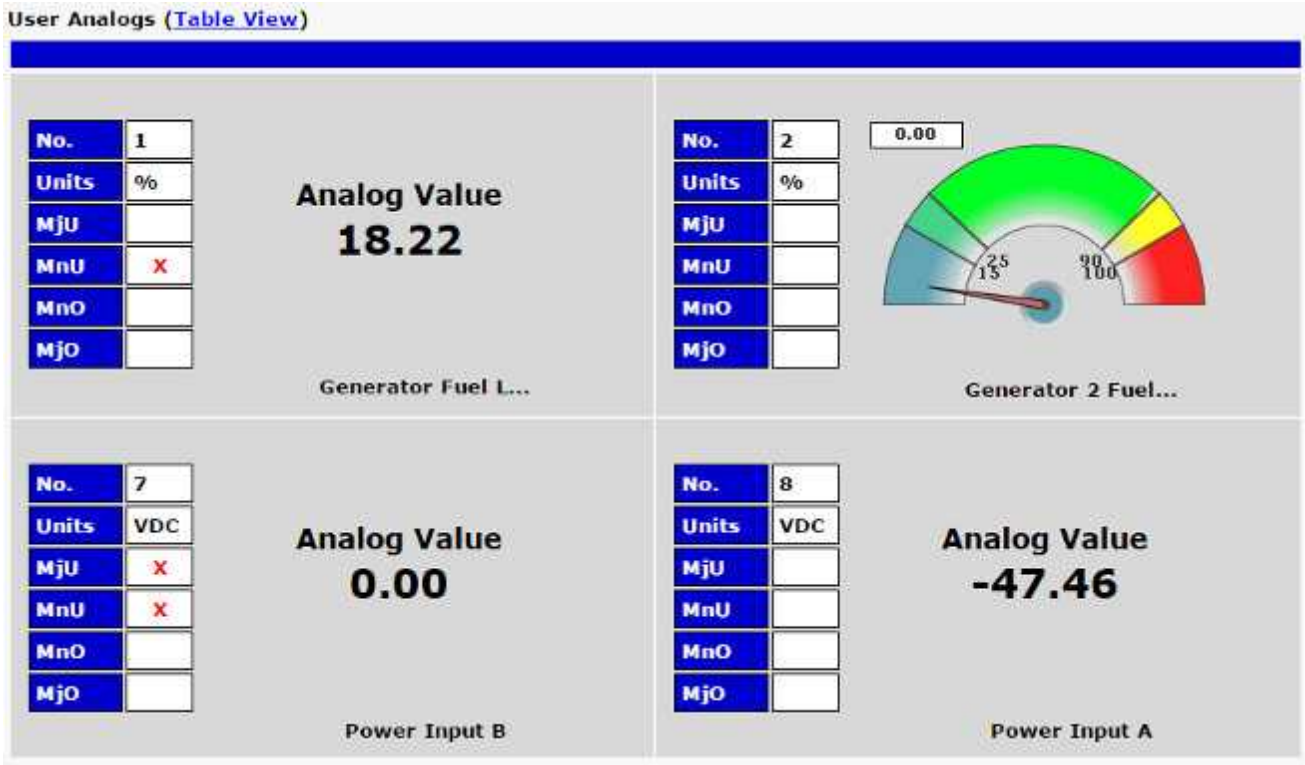
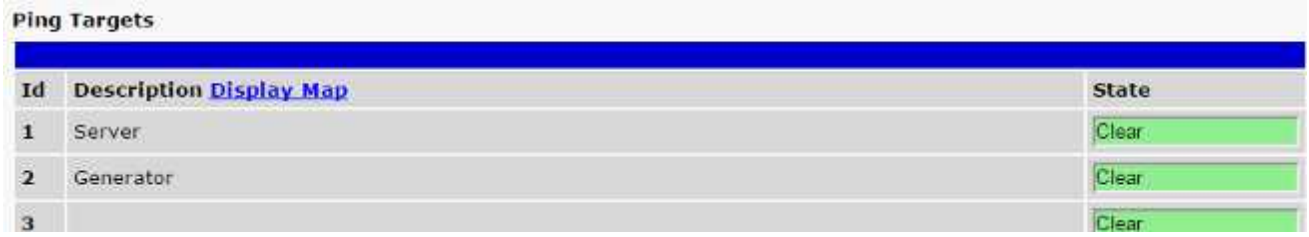


Fig. 12.6 *Current status of all analog inputs in the Monitor > User Analogs in Gauge View.*

Note: The analog gauges do not account for the user definable Deadband. This may result in an alarm threshold to appear crossed in the gauge animation when the point has not set or cleared.

10.5 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.



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

10.6 System Alarms

System alarms are not-editable, housekeeping alarms that are programmed into NetGuardian 224A. 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.

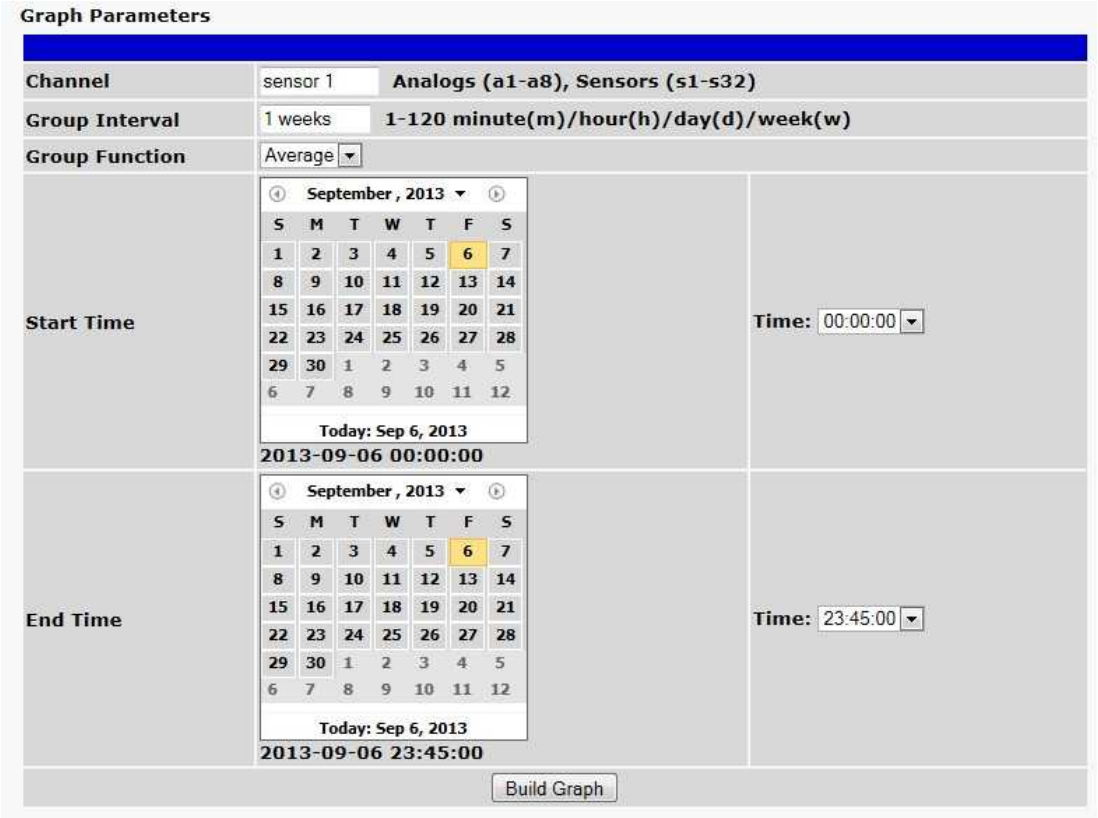
System Alarms

Pnt	Description Display Map	State
33	Default configuration	Clear
34	Dipswitch Configuration	Clear
35	MAC address not set	Clear
36	IP address not set	Clear
37	LAN hardware error	Clear
38	SNMP processing error	Clear
39	SNMP community error	Clear
40	LAN TX packet drop	Clear
41	Notification 1 failed	Clear
42	Notification 2 failed	Clear
43	Notification 3 failed	Clear
44	Notification 4 failed	Clear
45	Notification 5 failed	Clear
46	Notification 6 failed	Clear
47	Notification 7 failed	Clear
48	Notification 8 failed	Clear
49	NTP failed	Clear
50	Timed tick	Clear
51	Serial 1 RcvQ full	Clear
52	Dynamic memory full	Clear
53	Unit reset	Clear
54	DCP poller inactive	Clear
56	Modbus poller inactive	Clear

View the status of System Alarms from the Monitor > System Alarms menu.

10.7 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."

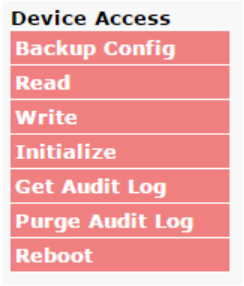


Provision the Channels, Group Interval, Group Function and more - all from the Graph Parameters section of the web browser interface.

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.

11 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 224A's firmware, and rebooting the unit. Click any of the options under **Device Access** to perform the desired action.

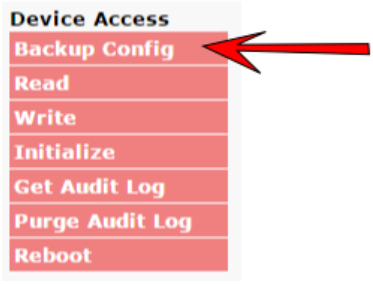


The control menu is located in the bottom left of the web interface

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 224A's non-volatile memory
Initialize	Sets the unit's configuration to factory default values
Get Audit Log	Opens the NetGuardian 224A's audit log in Notepad (or another plain text editor).
Purge Audit Log	Deletes the NetGuardian 224A's audit log history.
Reboot	Reboots the NetGuardian 224A.

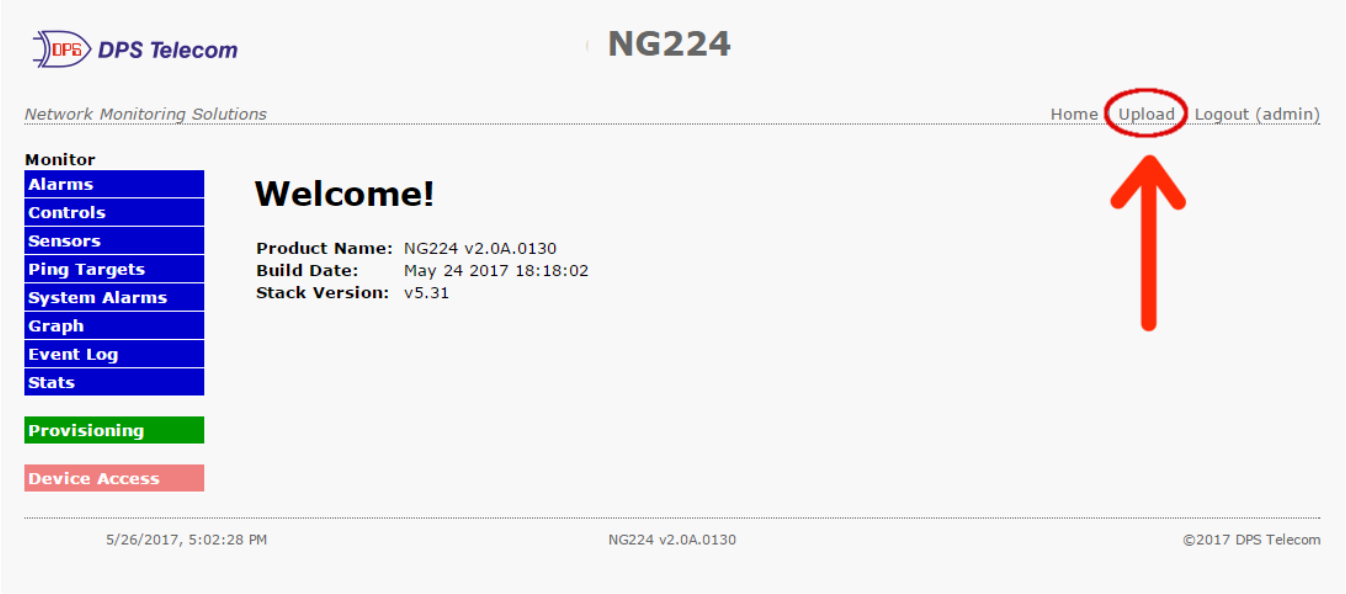
12 Backup Configuration

With the NetGuardian 224A you can backup your current configuration from the Web Interface. These configuration files can then be uploaded later, or uploaded to other NetGuardian 224A 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.

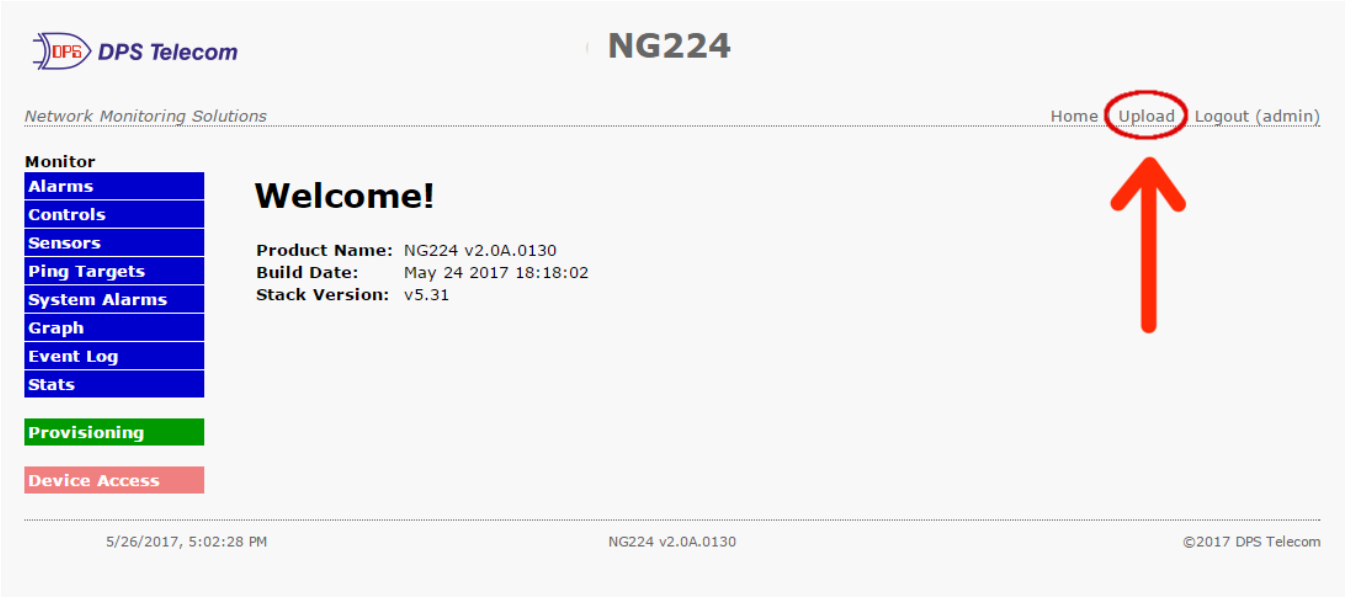


*To upload your configuration file, click on **Upload** on the top right corner of the web interface*

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.

13 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**.

14 Reference Section

14.1 Display Mapping

	Description	Port	Address	Point
Display 1	Discrete Alarms 1-24	99	1	1-24
	Undefined	99	1	25-32
	Default Configuration	99	1	33
	DIP Switch Config	99	1	34
	MAC Address Not Set	99	1	35
	IP Address Not Set	99	1	36
	LAN Hardware Error	99	1	37
	SNMP Processing Error	99	1	38
	SNMP community error	99	1	39
	LAN TX packet drop	99	1	40
	Notification Failed 1-8	99	1	41-48
	NTP failed	99	1	49
	Timed Tick	99	1	50
	Serial 1 RcvQ full	99	1	51
	Dynamic memory full	99	1	52
	Unit reset	99	1	53
	DCP poller inactive	99	1	54
	Reserved	99	1	55-64
Display 2	Ping Alarms 1-32	99	1	1-32
	Controls 1-2	99	1	33-34
	Undefined	99	1	35-64
Display 3	Analog 1 Minor Under	99	1	1
	Analog 1 Minor Over	99	1	2
	Analog 1 Major Under	99	1	3
	Analog 1 Major Over	99	1	4
	Reserved (CTRL)	99	1	9-16
	Value	99	1	17-32
	Analog 2 Minor Under	99	1	33
	Analog 2 Minor Over	99	1	34
	Analog 2 Major Under	99	1	35
	Analog 2 Major Over	99	1	36
	Reserved (CTRL)	99	1	41-48
	Value	99	1	49-64

Display Mapping

	Description	Port	Address	Point
Display 4	Analog 3 Minor Under	99	1	1
	Analog 3 Minor Over	99	1	2
	Analog 3 Major Under	99	1	3
	Analog 3 Major Over	99	1	4
	Reserved (CTRL)	99	1	9-16
	Value	99	1	17-32
	Analog 4 Minor Under	99	1	33
	Analog 4 Minor Over	99	1	34
	Analog 4 Major Under	99	1	35
	Analog 4 Major Over	99	1	36
	Reserved (CTRL)	99	1	41-48
	Value	99	1	49-64
Display 5	Digital Sensor 1 Minor Under	99	1	1
	Digital Sensor 1 Minor Over	99	1	2
	Digital Sensor 1 Major Under	99	1	3
	Digital Sensor 1 Major Over	99	1	4
	Digital Sensor 1 Not detected	99	1	5
	Digital Sensor 1 HVAC Fail	99	1	6
	Digital Sensor 1 Air Flow Below Normal	99	1	7
	Digital Sensor 1 Mate not detected	99	1	8
	Control	99	1	9-16
	Value	99	1	17-32
	Digital Sensor 2 Minor Under	99	1	33
	Digital Sensor 2 Minor Over	99	1	34
	Digital Sensor 2 Major Under	99	1	35
	Digital Sensor 2 Major Over	99	1	36
	Digital Sensor 2 Not detected	99	1	37
	Digital Sensor 2 HVAC Fail	99	1	38
	Digital Sensor 2 Air Flow Below Normal	99	1	39
	Digital Sensor 2 Mate not detected	99	1	40
	Control	99	1	41-48
	Value	99	1	49-64
Display 6	Digital Sensor 3 Minor Under	99	1	1
	Digital Sensor 3 Minor Over	99	1	2
	Digital Sensor 3 Major Under	99	1	3
	Digital Sensor 3 Major Over	99	1	4
	Digital Sensor 3 Not Detected	99	1	5
	Digital Sensor 3 HVAC Fail	99	1	6
	Digital Sensor 3 Air Flow Below Normal	99	1	7
	Digital Sensor 3 Mate not detected	99	1	8
	Control	99	1	9-16
	Value	99	1	17-32
	Digital Sensor 4 Minor Under	99	1	33
	Digital Sensor 4 Minor Over	99	1	34
	Digital Sensor 4 Major Under	99	1	35
	Digital Sensor 4 Major Over	99	1	36
	Digital Sensor 4 Not Detected	99	1	37
	Digital Sensor 4 HVAC Fail	99	1	38
	Digital Sensor 4 Air Flow Below Normal	99	1	39
	Digital Sensor 4 Mate not detected	99	1	40
	Control	99	1	41-48
	Value	99	1	49-64

Display Mapping

	Description	Port	Address	Point
Display 7	Digital Sensor 5 Minor Under	99	1	1
	Digital Sensor 5 Minor Over	99	1	2
	Digital Sensor 5 Major Under	99	1	3
	Digital Sensor 5 Major Over	99	1	4
	Digital Sensor 5 Not Detected	99	1	5
	Digital Sensor 5 HVAC Fail	99	1	6
	Digital Sensor 5 Air Flow Below Normal	99	1	7
	Digital Sensor 5 Mate not detected	99	1	8
	Control	99	1	9-16
	Value	99	1	17-32
	Digital Sensor 6 Minor Under	99	1	33
	Digital Sensor 6 Minor Over	99	1	34
	Digital Sensor 6 Major Under	99	1	35
	Digital Sensor 6 Major Over	99	1	36
	Digital Sensor 6 Not Detected	99	1	37
	Digital Sensor 6 HVAC Fail	99	1	38
	Digital Sensor 6 Air Flow Below Normal	99	1	39
	Digital Sensor 6 Mate not detected	99	1	40
	Control	99	1	41-48
	Value	99	1	49-64
Display 8	Digital Sensor 7 Minor Under	99	1	1
	Digital Sensor 7 Minor Over	99	1	2
	Digital Sensor 7 Major Under	99	1	3
	Digital Sensor 7 Major Over	99	1	4
	Digital Sensor 7 Not Detected	99	1	5
	Digital Sensor 7 HVAC Fail	99	1	6
	Digital Sensor 7 Air Flow Below Normal	99	1	7
	Digital Sensor 7 Mate not detected	99	1	8
	Control	99	1	9-16
	Value	99	1	17-32
	Digital Sensor 8 Minor Under	99	1	33
	Digital Sensor 8 Minor Over	99	1	34
	Digital Sensor 8 Major Under	99	1	35
	Digital Sensor 8 Major Over	99	1	36
	Digital Sensor 8 Not Detected	99	1	37
	Digital Sensor 8 HVAC Fail	99	1	38
	Digital Sensor 8 Air Flow Below Normal	99	1	39
	Digital Sensor 8 Mate not detected	99	1	40
	Control	99	1	41-48
	Value	99	1	49-64
Display 9	Digital Sensor 9 Minor Under	99	1	1
	Digital Sensor 9 Minor Over	99	1	2
	Digital Sensor 9 Major Under	99	1	3
	Digital Sensor 9 Major Over	99	1	4
	Digital Sensor 9 Not Detected	99	1	5
	Digital Sensor 9 HVAC Fail	99	1	6
	Digital Sensor 9 Air Flow Below Normal	99	1	7
	Digital Sensor 9 Mate not detected	99	1	8
	Control	99	1	9-16
	Value	99	1	17-32
	Digital Sensor 10 Minor Under	99	1	33
	Digital Sensor 10 Minor Over	99	1	34
	Digital Sensor 10 Major Under	99	1	35
	Digital Sensor 10 Major Over	99	1	36
	Digital Sensor 10 Not Detected	99	1	37

	Digital Sensor 10 HVAC Fail	99	1	38
	Digital Sensor 10 Air Flow Below Normal	99	1	39
	Digital Sensor 10 Mate not detected	99	1	40
	Control	99	1	41-48
	Value	99	1	49-64

Display Mapping

	Description	Port	Address	Point
Display 10	Digital Sensor 11 Minor Under	99	1	1
	Digital Sensor 11 Minor Over	99	1	2
	Digital Sensor 11 Major Under	99	1	3
	Digital Sensor 11 Major Over	99	1	4
	Digital Sensor 11 Not Detected	99	1	5
	Digital Sensor 11 HVAC Fail	99	1	6
	Digital Sensor 11 Air Flow Below Normal	99	1	7
	Digital Sensor 11 Mate not detected	99	1	8
	Control	99	1	9-16
	Value	99	1	17-32
	Digital Sensor 12 Minor Under	99	1	33
	Digital Sensor 12 Minor Over	99	1	34
	Digital Sensor 12 Major Under	99	1	35
	Digital Sensor 12 Major Over	99	1	36
	Digital Sensor 12 Not Detected	99	1	37
	Digital Sensor 12 HVAC Fail	99	1	38
	Digital Sensor 12 Air Flow Below Normal	99	1	39
	Digital Sensor 12 Mate not detected	99	1	40
	Control	99	1	41-48
	Value	99	1	49-64
Display 11	Digital Sensor 13 Minor Under	99	1	1
	Digital Sensor 13 Minor Over	99	1	2
	Digital Sensor 13 Major Under	99	1	3
	Digital Sensor 13 Major Over	99	1	4
	Digital Sensor 13 Not Detected	99	1	5
	Digital Sensor 13 HVAC Fail	99	1	6
	Digital Sensor 13 Air Flow Below Normal	99	1	7
	Digital Sensor 13 Mate not detected	99	1	8
	Control	99	1	9-16
	Value	99	1	17-32
	Digital Sensor 14 Minor Under	99	1	33
	Digital Sensor 14 Minor Over	99	1	34
	Digital Sensor 14 Major Under	99	1	35
	Digital Sensor 14 Major Over	99	1	36
	Digital Sensor 14 Not Detected	99	1	37
	Digital Sensor 14 HVAC Fail	99	1	38
	Digital Sensor 14 Air Flow Below Normal	99	1	39
	Digital Sensor 14 Mate not detected	99	1	40
	Control	99	1	41-48
	Value	99	1	49-64
Display 12	Digital Sensor 15 Minor Under	99	1	1
	Digital Sensor 15 Minor Over	99	1	2
	Digital Sensor 15 Major Under	99	1	3
	Digital Sensor 15 Major Over	99	1	4
	Digital Sensor 15 Not Detected	99	1	5
	Digital Sensor 15 HVAC Fail	99	1	6
	Digital Sensor 15 Air Flow Below Normal	99	1	7
	Digital Sensor 15 Mate not detected	99	1	8
	Control	99	1	9-16
	Value	99	1	17-32
	Digital Sensor 16 Minor Under	99	1	33
	Digital Sensor 16 Minor Over	99	1	34
	Digital Sensor 16 Major Under	99	1	35
	Digital Sensor 16 Major Over	99	1	36
	Digital Sensor 16 Not Detected	99	1	37

	Digital Sensor 16 HVAC Fail	99	1	38
	Digital Sensor 16 Air Flow Below Normal	99	1	39
	Digital Sensor 16 Mate not detected	99	1	40
	Control	99	1	41-48
	Value	99	1	49-64

Display Mapping

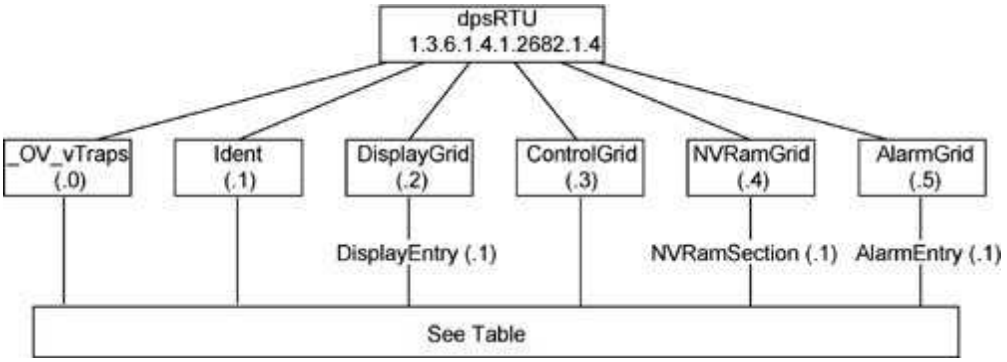
14.2 System Alarms

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

14.3 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)
Action (.5)

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

Tbl. B5 (.5) AlarmEntry points
AlarmEntry (1.3.6.4.1.2682.1.2.5.1)
Aport (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)
APntDesc (.5)*
AState (.6)
* For specific alarm points, see Table B6

14.4 SNMP Granular Trap Packets

The tables below provide a list of the information contained in the SNMP Trap packets sent by the NetGuardian 224A.

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 224A) **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 224A 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

15 Frequently Asked Questions

Here are answers to some common questions from NetGuardian 224A users. The latest FAQs can be found on the NetGuardian 224A support web page, **http://www.dpstele.com.**

If you have a question about the NetGuardian 224A, please call us at **(559) 454-1600** or e-mail us at **support@dpstele.com.**

15.1 General FAQs

Q. How do I telnet to the NetGuardian 224A?
A. You must use **Port 2002** to connect to the NetGuardian 224A. 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 224A and Port 2002. For example, to connect to the NetGuardian 224A using the standard Windows Telnet client, click Start, click Run, and type "telnet <NetGuardian 224A IP address> 2002."

Q. How do I connect my NetGuardian 224A to the LAN?
A. To connect your NetGuardian 224A 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 224A 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 224A.

Q. The LAN link LED is green on my NetGuardian 224A, 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.

15.2 SNMP FAQs

Q. Which version of SNMP is supported by the SNMP agent on the NetGuardian 224A?
A. SNMP v1, SNMPv2 and SNMPv3.

Q. How do I configure the NetGuardian 224A to send traps to an SNMP manager? Is there a separate MIB for the NetGuardian 224A? 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 224A begins sending traps as soon as the SNMP notification type is set up. The NetGuardian 224A 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 224A support MIB-2 and/or any other standard MIBs?
A. The NetGuardian 224A supports the bulk of MIB-2.

Q. Does the NetGuardian 224A SNMP agent support both NetGuardian 224A and T/MonXM variables?
A. The NetGuardian 224A SNMP agent manages an embedded MIB that supports only the NetGuardian 224A'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 224A 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 224A 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 224A and the SNMP manager are both on the network. Use the unit's ping command to ping the SNMP manager.

16 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.*

17 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

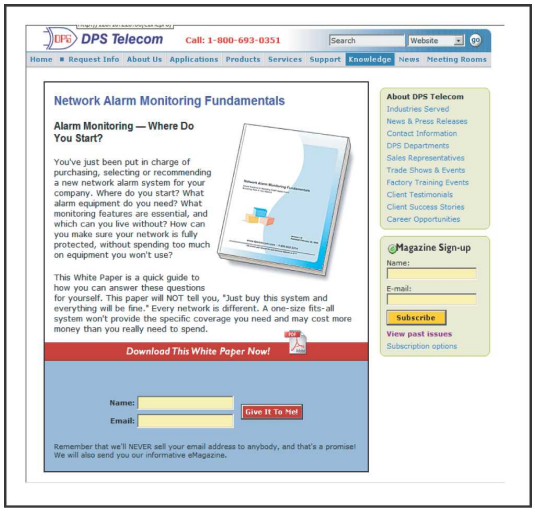
Need help with your alarm monitoring? DPS Information Services are ready to serve you … in your email or over the Web!

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

DPS Telecom
"Your Partners in Network Alarm Monitoring"

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

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