NetGuardian ENV

USER MANUAL

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

1 NetGuardian ENV Overview

The Building Access System (BAS) is a comprehensive building entry management system that provides centralized door access control utilizing your existing DPS network monitoring systems. With the system in place, managers can maintain a database of all personnel access as well as the time of day and location that access was granted.

Building access functionality typically requires an RTU to report to T/Mon and locally process entry requests made through an entry control unit (ECU). The NetGuardian ENV, however, grants or denies access on its own, performing both the RTU and ECU functions of the traditional DPS building access environment. It communicates directly with T/Mon to retrieve and report access data, stores its own access data locally, and issues control logic for a single door.

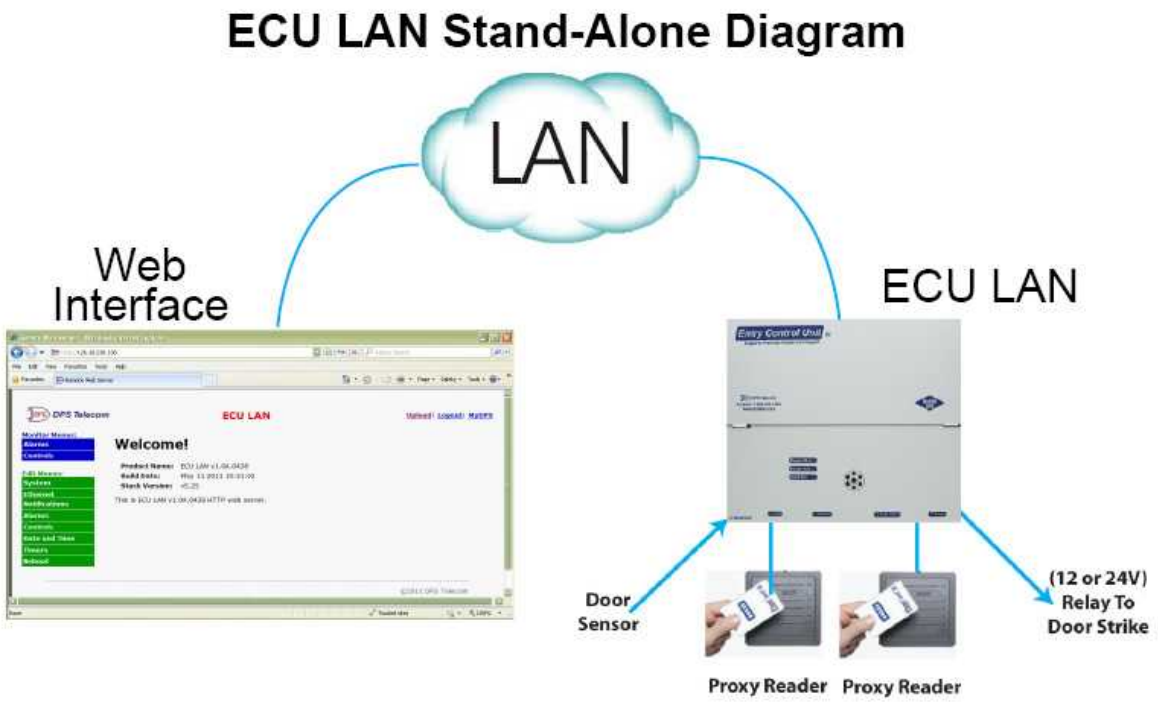
BAS Functional Diagram with NetGuardian ENV

In the Building Access System, the NetGuardian ENV operates independently of an RTU

With the NetGuardian ENV, you can cheaply and easily add individual doors to your building access system to control building access at small sites where you don't have or need an RTU. This allows you to extend building access functionality to sites that would've otherwise been unmonitored or controlled by a completely separate system.

The NetGuardian ENV:

- Controls and regulates a single door entry point.
- Stores entry data and access permissions locally so your site functions independent of the master.
- Supports a proxy reader build option.
- Is configurable through simple TTY and Web Browser interfaces
- Can run in stand-alone mode for applications without T/Mon



In "Standalone" mode, the NetGuardian ENV can control door access without receiving access information from T/Mon

Specialized Door Control Modes

"Magnetic Door Mode" - This configurable mode may be used with doors equipped with magnetic door locks. In this mode, the door will remain magnetically locked until unlocked via proxy card scan, Request-to-Exit button, or motion sensor.

NOTE: Door violations occur when the door is opened without being unlocked. Pushing a Request-to-Exit button or triggering the motion sensor after the intrusion will not cancel the violation.

"Lock When Closed Mode" - This mode causes the door to lock a few seconds after it has been detected closed, and can be usefully combined with "Magnetic Door Mode" to ensure the door closes before being locked. In this mode, if the door does not open after it has been unlocked, It will lock again after 2-3 seconds.

Accessories

Proxy Reader or Proxy/Keypad Combo (Accessory Sold Separately)
The weather-proofed proximity reader is mounted on the exterior of the building and is designed to withstand a wide temperature range. There is no amount of tampering that can be done to the proxy reader to cause the door to open. The NetGuardian ENV supports +12V RS232 card readers.

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

that could lead to major outages and system failure.

The NetGuardian ENV features:

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

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

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

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

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

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

2 Specifications

Hardware

Dimensions:	1.75" H x 17.00" W x 5.625" D	**Modem:**	33.6 K internal (Optional)
Mounting:	19" or 23" Rack 1 RU		
Weight:	2lb. 5oz. (1.063 kg)	**Discrete Alarm Inputs:**	8 (Optional build with 6 alarms and 2 controls)
		[2] Discrete Alarm Length:	200Ft. (00m) per Alarm
Power Input:	–48 VDC nominal (–36 to –72 VDC)		
	(Optional) –24 VDC nominal (–18 to –36 VDC)	**Analogs:**	8 (Optional)
	(Optional) Wide Range –24/–48 VDC (–18 to –58 VDC)	**Input Range:**	-92 to +92 VDC or 4 to 20mA
	(Optional) +24VDC (+18 to +36 VDC)	**[4] Analog Accuracy:**	± 1% of Analog Range
	(Optional) +12VDC (+11 to +18 VDC)		
	(Optional) Power Over Ethernet (POE)	**Control Outputs:**	6 (Form A) user defined NO/NC (Optional)
		Max Voltage:	60 VDC/120 VAC
[3] Current Draw:	60mA max @ 24VDC	**Max Current:**	1A AC/DC
Fuse:	Internal Resetable		
		Operating Temp:	32° to 140°F (0° to 60°C)
[1] Power Outputs:	6w	**[1] Industrial Operating Temp:**	-22° to 158°F (-30° to 70°C)
Voltage Output Options:	+12 VDC, +24 VDC	**Storage Temp:**	-40° to 185°F (-40° to 85°C)
Output Current:	0.5 A @12VDC		
Output Fuse:	Internal Resetable	**Operating Humidity:**	95% non-condensing
Audible Interfaces:	No	**MTBF:**	60 Years
Visual Interfaces:	7 Front Panel LEDs	**RoHS:**	RoHS 5 Approved
[1] Hardware Interfaces:	1 RJ45 10/100BaseT full-duplex Ethernet port	**Ordering Options:**	D-Wire Sensors
	1 USB front-panel craft port		
	1-4 RJ11 connector for D-Wire sensor network (Optional)		
	1 RJ11 Connector for Telco		

Software

Downloadable Firmware:	Yes	**[1] D-Wire Sensor Support:**	Up to 15 dwire sensors
Built-in Web Interface:	Yes		1 built-in temp sensor (Optional)
Browser Support:	IE9, IE10, Firefox		
		Ping Alarms:	32
Protocols:	DCPx, TELNET, HTTP, Email		
SNMP Support:	V1, V2c, V3	**OS Support:**	XP, Vista, 7 (32 or 64 bit)

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.

Keypad and Proxy Reader Specs

Specification	Proxy Reader
Dimensions	4.7" x 3" x 0.68"
Mounting	wall mount
Power Input	5-16 VDC
Current Draw	30 mA
Interfaces	RJ45
Protocols	UART
Temp. Range	-30° to 65°C (-22° to +150°F)
Humidity Range	0%-95% non-condensing
Fuse	N/A
Audible	Speaker
Visual	LED

Note: Proxy reader specifications are based on the ThinLine II card reader from the HID Corporation. 12VDC power is supplied to the reader by the NetGuardian ENV.

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

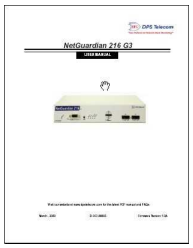
Shipping List

3 Shipping List

Please make sure all of the following items are included with your NetGuardian ENV. 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 ENV
D-PK-NGDIN

NetGuardian ENV Resource CD



NetGuardian ENV User Manual

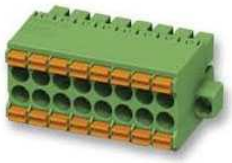
D-UM-NGDIN

6 ft. USB Download Cable

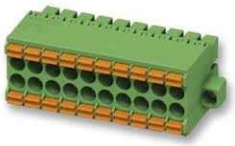
D-PR-046-10A-06

x 1
Lg. Power Connector (Main Power)
2-820-00862-02

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



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



x 1
10-Pin Alarm Connector
2-821-21035-00

x 1
Proximity Reader with Key Pad

D-PK-PROXI-12007.00001

3.1 Optional Shipping Items - Available by Request

Temp Sensor Node Node
D-PK-DSNSR-12001

Temp/Humidity Sensor

D-PK-DSNSR-12002

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

Hardware Installation

4 Hardware Installation

4.1 Site Preparation

Tools needed:

Phillips screwdriver

Wire strippers/cutter

Small standard No.2 screwdriver (1/16" for screw-lug connectors)

Materials needed:
• 1/2” conduit

Precautions
• *Pull GMT fuse before connecting ECU power feed.*
• *Always observe electrostatic discharge (ESD) precautions.*

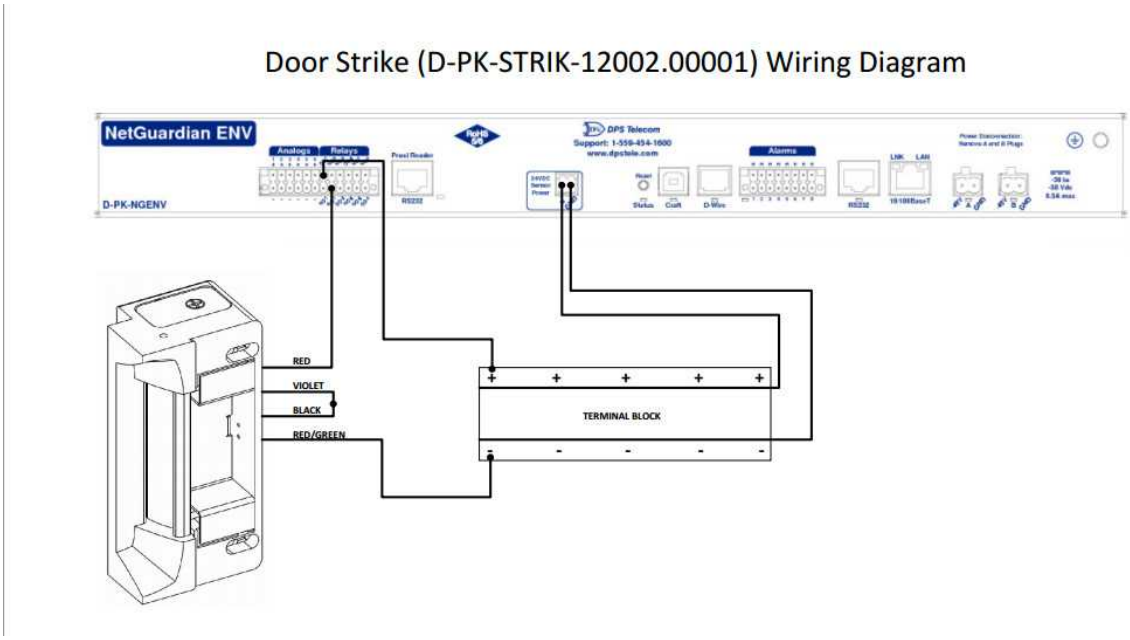
4.2 Installation Overview

1. Mount the NetGuardian ENV and the Proxy Reader.
2. Connect power to the NetGuardian ENV.
3. Connect communication lines between the NetGuardian ENV, LAN, and Proxy Reader.
4. Set the NetGuardian ENV IP address via TTY interface.
5. Customize NetGuardian ENV settings via the Web Browser Interface
6. Provision T/Mon with the appropriate information. (See the BAS software module in the T/MonXM user manual for more information)

4.3 Door Strike

When a valid password is entered on the keypad, the ENV will operate the relay to energize the door strike. The ENV will de-energize the relay if configured for magnetically controlled doors.

Follow the diagram below to connect the door strike and door sensor to the ENV.



Connect the door sensor to RTN (return) and ALM1 (opto isolated alarm for the door sensor).

4.4 Communication Lines

4.4.1 Cable Installation

Installation of the Proxy Reader consists of mounting, and connecting the cable. This document will list the steps required to connect the cable.

Parts:

Proxy Reader (D-PR-534-10A-00)	Qty. 1 (included)
Cable Fitting	Qty. 1 (included)
Cable, 8 conductor (22 AWG)	as required (up to 4000 feet)

Tools:

Flat-blade
Phillips screwdriver

Process:

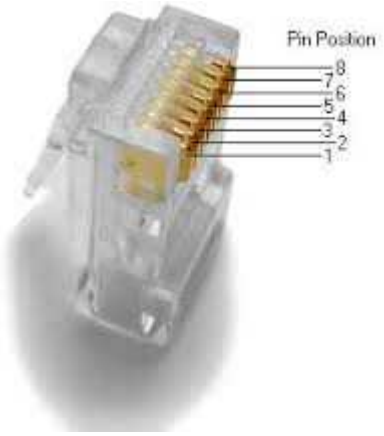
1. Route the interface cable from the proxy reader to the NetGuardian ENV.
2. Prepare the cable by cutting the cable jacket back 2 inches.

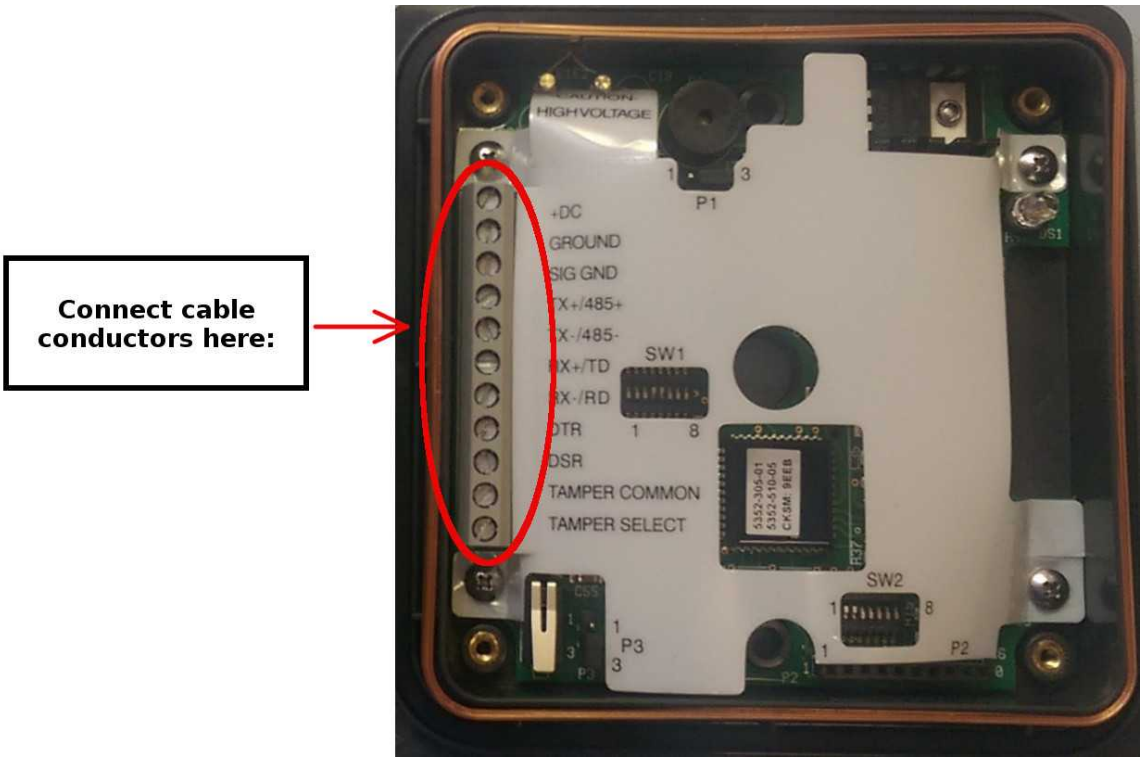
3. Strip the wires about a 1/4 inch.
4. Pry off the center face plate by placing a thin blade into the grove that outlines the face of the reader. Be careful so not to damage the proxy reader. The screws that hold the enclosure pieces together will now be exposed.

5. Loosen the four screws to open the enclosure (the enclosure screws are captive in the cover).

6. Installation of the cable fitting is optional. If the cable fitting is installed it can accommodate a cable with an outer diameter of .300 inches (nominally). To install the cable fitting just screw it to the rear of the reader and feed your cable through it.
7. Dress the cable conductors and connect them to **DC +, GROUND, SIG GND, RX+/ TD** and **RX-/RD**. The following pin-out must be used:

Proxy P7 Pin	Description	RJ45/ENV
1	DC +	1
2	GROUND	8
3	SIG GND	4
4	TX+/485+	N/C
5	TX-/485-	N/C
6	RX+/TD	3
7	RX-/RD	6
8	DTR	N/C
9	DSR	N/C
10	TAMPER COMMON	N/C
11	TAMPER SELECT	N/C





8. Test to make sure the proxy reader is working properly.

Installation

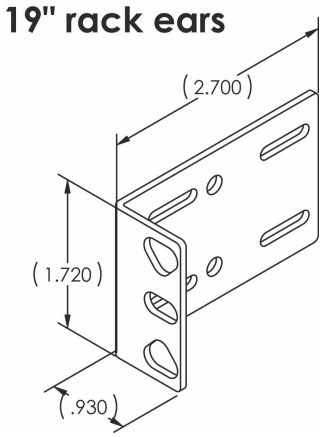
5 Installation

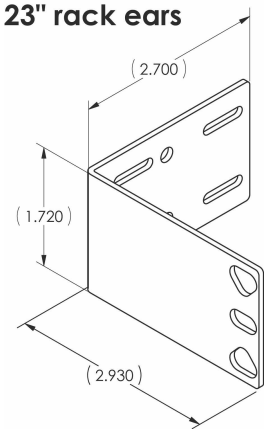
5.1 Mounting

The NetGuardian ENV can be flush or rear-mounted

The compact NetGuardian ENV occupies only the width of a standard rack unit. The NetGuardian ENV mounts in a 19" or 23" rack, and can be mounted in the flush-mount or rear mount locations, as shown in above.

The rack ears can be rotated 90° for wall mounting or 180º for other mounting options.

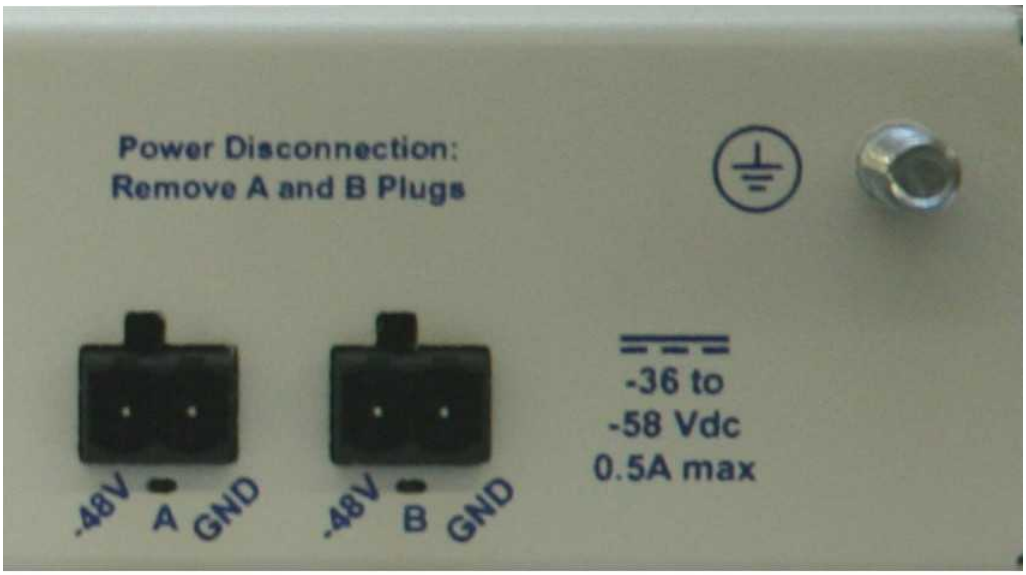




Use the included wall mount brackets to mount the NetGuardian ENV on the wall.

5.2 Power Connection

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



NetGuardian ENV Power Terminal

To connect the NetGuardian ENV to a power supply:

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

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

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

6 NetGuardian ENV Front Panel

NetGuardian ENV Front Panel

LED	Status	Description
Status	Flashing Green	Application Running
	Flashing Red	Bootloader Running
Craft	Flashing Green	Transmit over craft port
	Flashing Red	Recieve over craft port
D-Wire	Solid Green	At least 1 D-Wire enabled, no alarm
	Solid Red	New Alarm
	Off	No D-Wire Sensors attached.
Alarms	Flashing Red	New Alarm
	Solid Red	Standing Alarm Acknowledged via DCP poll
	Off	No Alarms
Power (A or B)	Solid Green	Has power
	Off	Does not have power or polarity reversed.
RS232/BAS	Flashing Green	Transmit over port
	Flashing Red	Receive over port

Front Panel LED Descriptions

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

Basic Unit Configuration

7 Basic Unit Configuration

To configure your NetGuardian ENV, you must first provision the unit with an IP Address. You will configure the unit's IP address, subnet mask, and gateway, via the NetGuardian ENV's TTY interface, accessed via HyperTerminal (or a similar terminal emulator) over a serial connection.

The NetGuardian ENV Craft Port

To begin configuring the unit, connect the DB9 male to female cable that came with your ECU to the unit's craft port and your PC's serial port.

7.1 Provisioning an IP Address

You must be connected via craft port or Telnet to use the TTY interface. We'll be using HyperTerminal to connect to in the following example - however, most terminal-emulating programs should work.

To Configure your NetGuardian ENV's IP Address:

To access HyperTerminal using Windows:

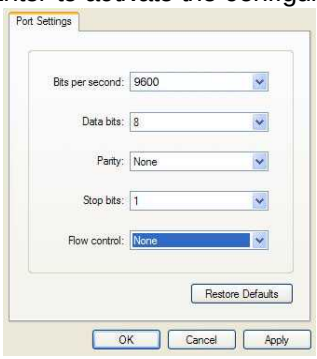
1. Click on the **Start** menu **>** select **Programs** > **Accessories** > **Communications** > **HyperTerminal.**

2. At the Connection Description screen, enter a name for this connection. You may also select an icon. The name and icon do not affect your ability to connect to the unit.

3. At the Connect To screen, select Com port you using from the drop down and click OK. (COM1 is most commonly used.)

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

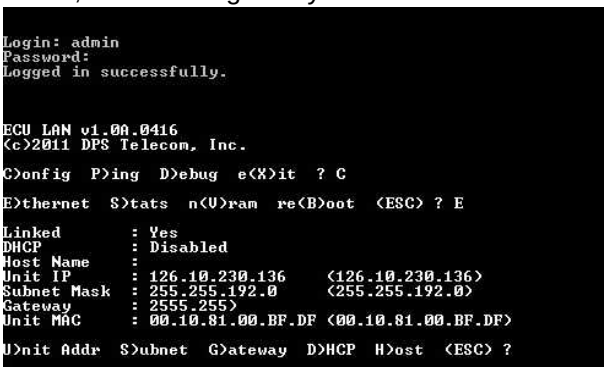
   Once connected, you will see a blank, white HyperTerminal screen. Press Enter to activate the configuration menu.



5. When prompted, enter the default username **ad** and password **dpstelecom**. NOTE**:** If you don't re prompt for the username, try pressing **Enter** to re the prompt. If that doesn't work, check the Com p are using on your PC and make sure you are usi cable provided.

Additional cables can be ordered from DPS Tele
Part number D-PR-045-10A-04

6. The NetGuardian ENV'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.



7. ESC to the main menu. When asked if you'd lik save your changes, type Y for Y)es. Reboot the NetGuardian ENV to save its new configuration.

8 Speaker Operation

The NetGuardian ENV offers the following audible notification of specific events:
*Configurable in the Provisioning > Timers page under Door Warning Beep.
**Configurable in the Provisioning > Timers page under Time Before Door Violation.

Normal Entry Operation
After entering a valid "Entry" password or card scan and the door strike has been energized, users have approximately 55 seconds** to enter through the door and close the door behind them before an alarm condition occurs. Once a valid "Entry" password is accepted by the NetGuardian ENV, a 25-second* silent time-lapse will occur followed by a 30-second slow (warning) beep, during which time the user must enter through the door and close it behind them. An alarm condition will occur after 55 seconds** and will be indicated by a faster beep.

Normal Exit Operation
Upon exiting through the door, users must enter a valid "Exit" password or card scan within 30 seconds of
opening the door. A 30-second slow (warning) beep will sound during which time the user must close the door
and enter valid "Exit" password before an alarm condition occurs.

Normal Exit Operation (With Request-to-Exit)
An optional motion sensor can be tied to ALM2 to signal a request-to-exit scenario. You would do this if you
don't want to enter a password or card scan during exit. During a request-to-exit, the person exiting has approximately 55 seconds** to close the door behind them before an alarm condition occurs. A 25-second*
silent time-lapse will occur followed by a 30-second slow (warning) beep, during which time the user must
exit through the door and close it behind them. An alarm condition will occur after 55 seconds** and will be
indicated by a faster beep.

Door Alarm
A fast beep indicates a door alarm has occurred. The user must re-enter or re-exit (with a valid password or
card scan) in order for the alarm to clear. While the door alarm remains standing (uncleared), the speaker will
cycle between 12 minutes on (fast beep) and 3 minutes off. Because a fast beep indicates a door alarm, open
door lockout will be canceled, and the keypad or reader will be enabled, even if the door is open. A T/Mon administrator can also cancel the door alarm by issuing a MOM door unlock command.

Propped Door Mode
T/MonXM can issue a "Propped Door Mode" by issuing a MOM control command to point 21,which will allow
the door to be held open without an alarm for up to 15 minutes. The speaker will not sound while the "Propped Door Mode" is active. Door violation alarms will not post while the "Propped Door Mode" is active.
However, users should continue to submit passwords as they enter and exit the building.
A beep indication will be given during the last 2 minutes if the door is open to show the command is about
to expire. See the Building Access System software module in the T/Mon user manual for information regarding issuing a "Propped Door Mode" command.

Extended Propped Door Mode

The "Extended Propped-Door Mode" feature can be engaged by remotely issuing an OPR control command from
the T/Mon to point 22. The door may be opened and closed freely with no door violations for an indefinite
period of time. The door will be locked when closed. With the door closed, exit this mode by remotely issuing
an RLS control command to point 22.

Caution: Extended propped-door mode will not auto-expire.

Stay-Open Door Mode
You can enter "Stay-Open Door Mode" in one of two ways:

i. Scan any card defined in T/Mon for that door with Stay-Open parameter set to 'Yes'
ii. Remotely issue an OPR control command for both points 17 and 22

Points 17 and 22 will be active during Stay-Open Mode. The door will be unlocked and no door violations
will occur.

With the door closed, you can exit Stay-Open mode in one of two ways:

i. Scan any card defined in T/Mon for that door with Stay-Open parameter set to 'Yes'
ii. Remotely issue RLS control command to point 22. Point 17 will automatically clear, which will lock the door.

Caution: Stay-Open mode will not auto-expire.

Quick Start: How to Connect to the NetGuardian ENV

9 Quick Start: How to Connect to the NetGuardian ENV

Most NetGuardian ENV 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 ENV and access its Web Browser.

9.1 ...via LAN

NetGuardian ENV Ethernet Port

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

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

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

NetGuardian ENV Craft Port

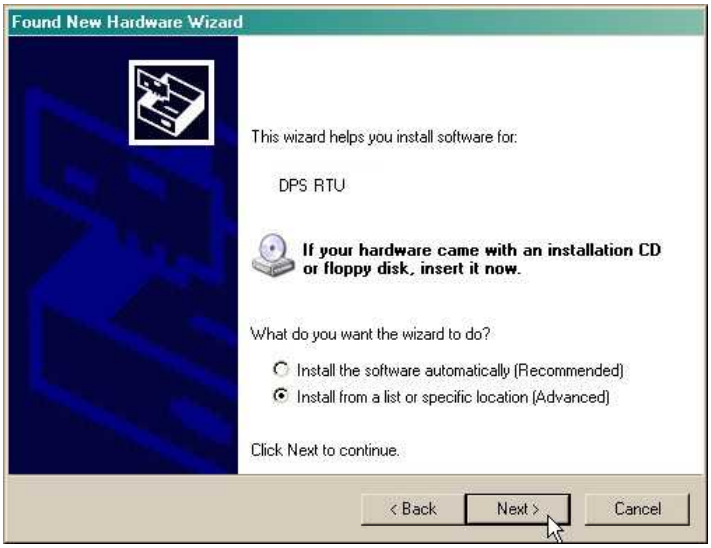
Use the front panel craft port to connect the NetGuardian ENV to a PC for onsite unit configuration. To
use the craft port, connect the included DB9 download cable from your PC's COM port to the craft port.

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

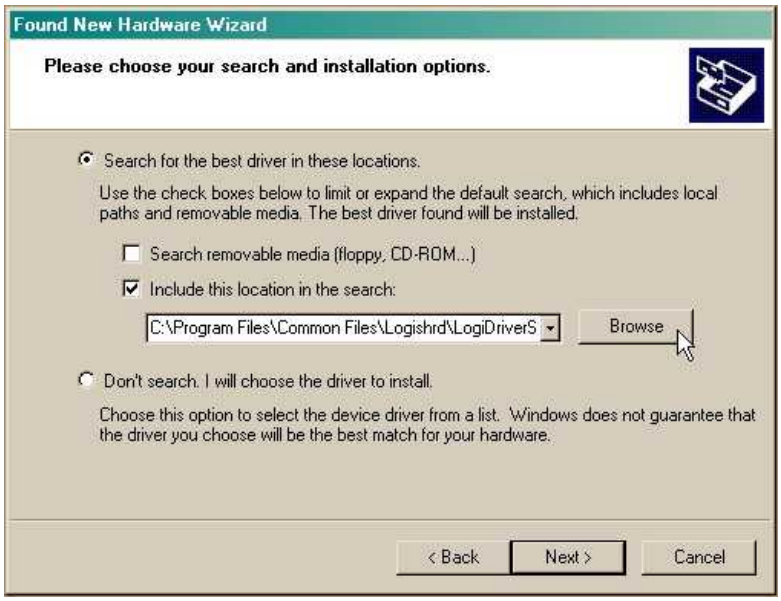
The following steps will occur the first time any DPS USB equipment is used on this PC. If you've used a different DPS USB device before and have installed the DPS USB drivers, then **skip to Step 9**.

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

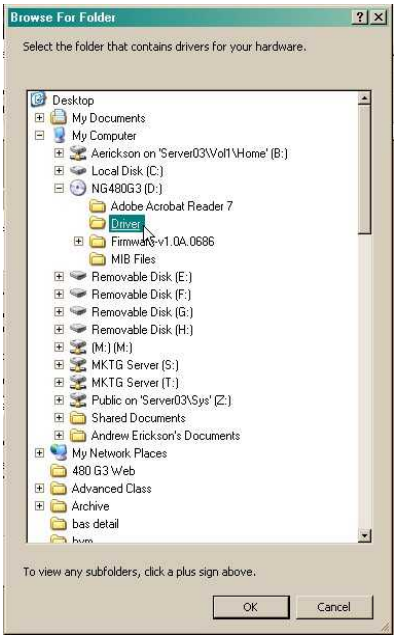
1. Click the "Found New Hardware" message/icon to launch the "Found New Hardware Wizard".



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

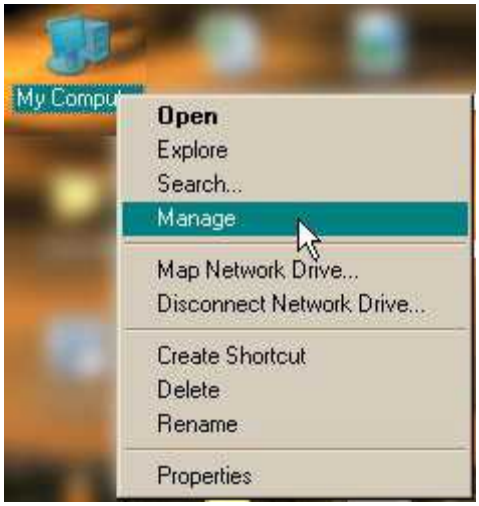


7. Select the "Driver" folder of your NetGuardian ENV Resource Disc Disc (CD) and click "OK"

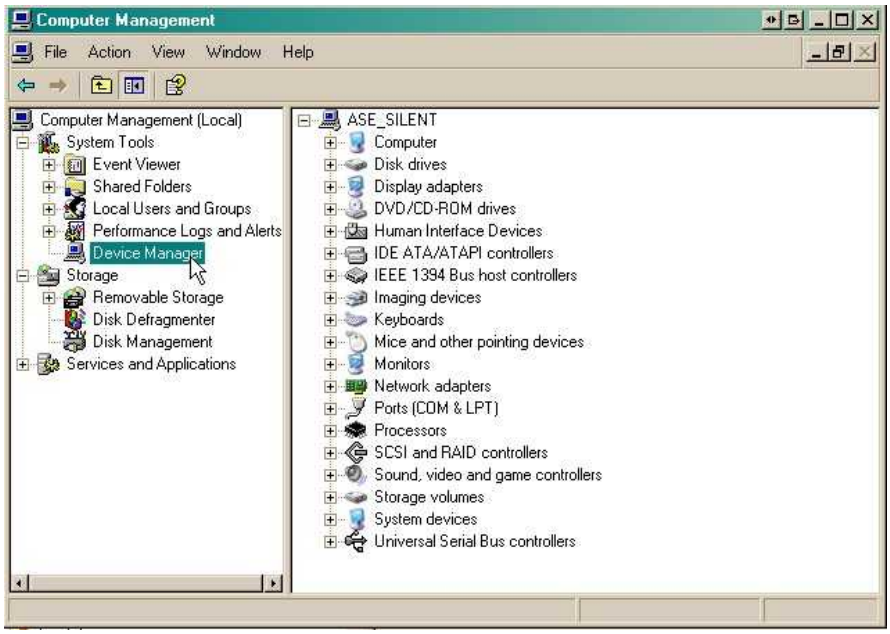
The following message will confirm installation of a new "USB Communications Port"

8. Click "Finish" to close the Wizard.

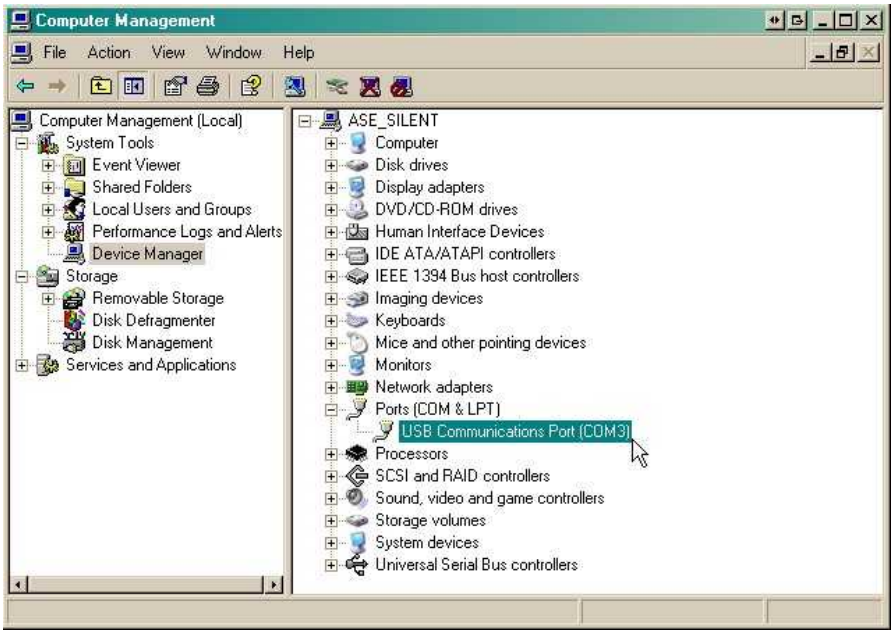
Now that the driver has been installed, a new COM port is being emulated on your PC. Before using hyperterminal, you must confirm the identity of that new COM port (COM1, COM2, COM3...) in the Windows Device Manager.



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).

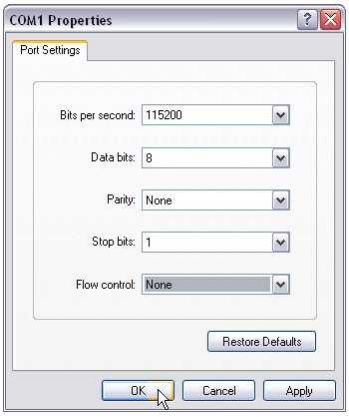
12. Click on the **Start** menu **>** select **Programs** > **Accessories** > **Communications** > **HyperTerminal.**

13. At the Connection Description screen, enter a name for this connection. You may also select an icon. The name and icon do not 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**

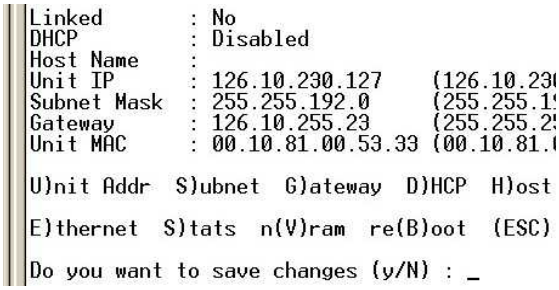
    Once connected, you will see a blank, white HyperTerminal screen. Press Enter to activate the configuration menu.



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 ENV'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 ENV 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.

10 TTY Interface

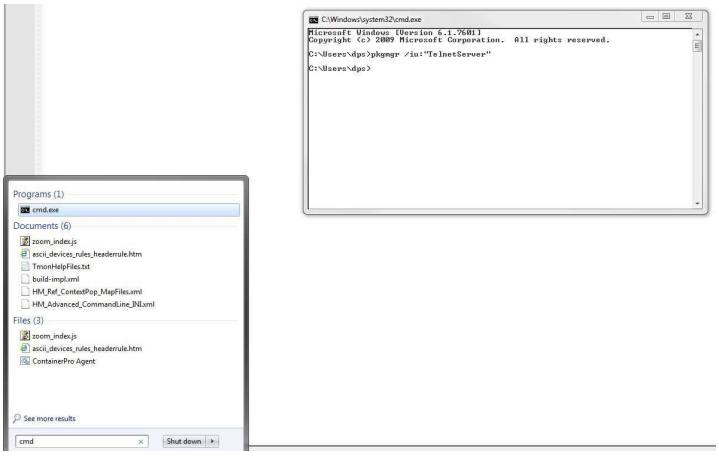
The TTY interface is the NetGuardian ENV's built-in interface for basic configuration. From the TTY interface, you can:

- 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.

11 Determining Proximity Card Number

To obtain the number of your proximity card that should be databased in your T/Mon or NetGuardian ENV web browser in order to grant access privileges:

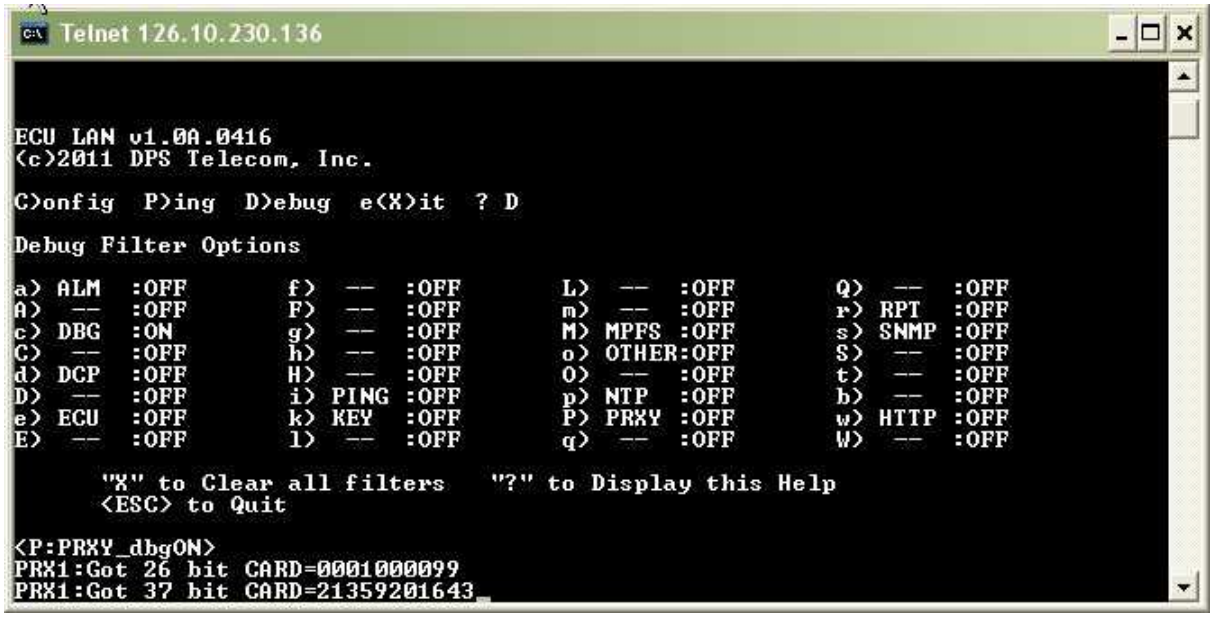
1. Telnet into the NetGuardian ENV using port **2002** (or create a serial craft connection at 9600 baud)

2. Login using your username and password.

3. Select the **(D)ebug** option:

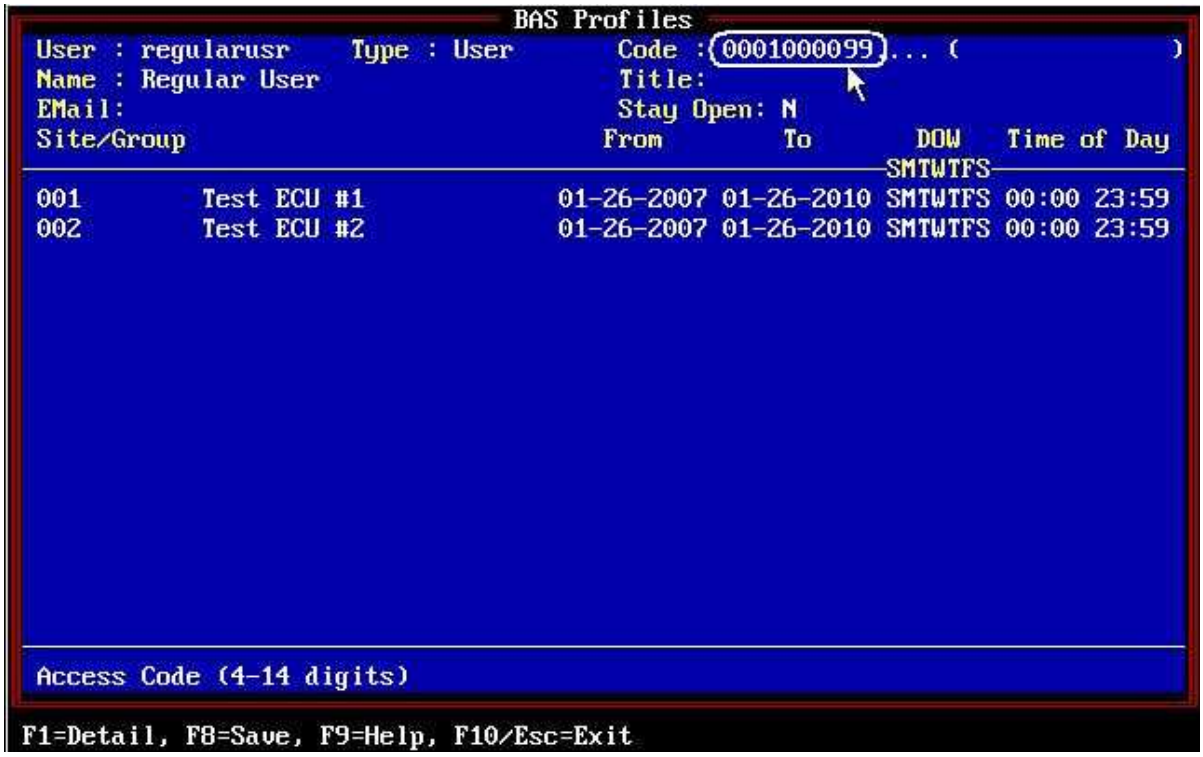
4. In the **(D)ebug** menu, select the **(P)roxy** option:

5. Once Proxy filter debug is set to **ON**, you can capture your card number. Swipe the undatabased card in front of the reader, and the card number will appear for you to catalog. The screen below shows examples of card numbers (access codes).



A Telnet screen showing both 26 and 37-bit card number captures

6. Having captured the card number, you are now ready to database it into the T/Mon. From the T/Mon Master Menu, navigate to **Files/Utilities/Building Access/Profiles** and enter the code in the area shown:



Database valid user access codes captured via debug in T/Mon

12 T/Mon Configuration

To incorporate the NetGuardian ENV into your Building Access System, you must configure the device in T/Mon. Once the device is configured in T/Mon, you will be able to determine access rights by user, day, time, and during what dates, a user will have access to the door controlled by the NetGuardian ENV.

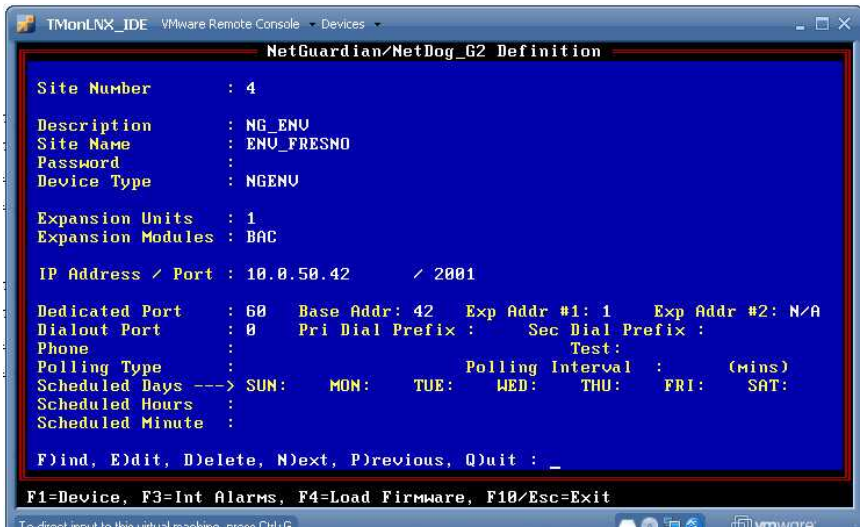
To configure your NetGuardian ENV in T/Mon:

1. Set up a Remote Port Polling Job

- From the T/Mon main menu, select **Parameters>Remote Parameters**
- Select a halted job greater than 49 and Create a **DCP(F) Interrogator Job**.
  - If unsure of settings when creating the DCP(F) Interrogator job, see section M1 of your T/Mon XM manual or simply use default settings.
- Define the data connection for your job
  - Press F6 to reach the Data Connection screen
  - Press F1 to open the Ethernet TCP Port Definition screen and define the data connection (IP Port) for your Building Access Job.

Configuring the DCP(f) Job in T/Mon

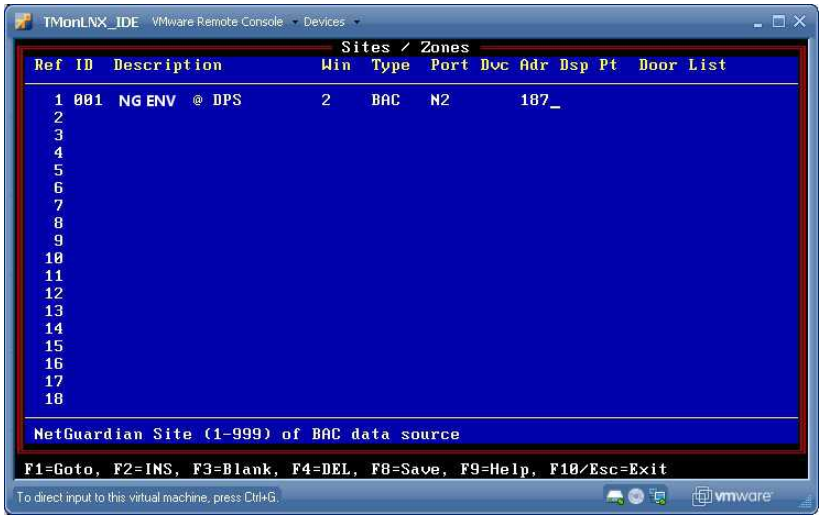
2. Once you've configured the remote port job, you must **Define the NetGuardian ENV Device**.
   - Return to the Master Menu and select **File Maintenance>LAN-Based Remotes>NetGuardian/ NetDog_g2**. From here, you will configure the NetGuardian ENV device.



Defining the NetGuardian ENV in T/Mon

- In the **Device Type** field, select **NetGuardian ENV.**
- In the **Expansion Modules** field, select **BAC**.
- In the **IP Address / Port** field, enter the IP Address you configured for the unit via the TTY interface. The NetGuardian ENV defaults to port 2001, but can be changed from the Web Browser interface.
- In the **Dedicated Port** field, enter the number of the Port Job you used for the DCP(F) Interrogator job you created in the previous step.
- For all other settings, you may use defaults. Or, if you are unsure of any settings, see section M22 of your T/MonXM manual for field descriptions in the device definition screen.

3. Once you've defined the NetGuardian ENV device, you must define the site.
   - Return to the T/Mon Master Menu, and select **Files>Building Access>Sites/Zones**



Defining the ENV site in T/Mon

- From the site definition screen, you can define the door controlled by your NetGuardian ENV.
  - Set the site ID (001-999 - there are no restrictions as to the order of your sites)
  - For the **Type**, enter **BAC**
  - Under **Port**, enter **N2**
  - For **Adr**, enter the number you input for the **Site Number** field in the previous step

- Under **Door List**, enter 1

Once your device is defined and properly configured in T/Mon, you may determine which users may access the door at what times. For more information on users and profiles, see section M22 of your T/Mon Manual.

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

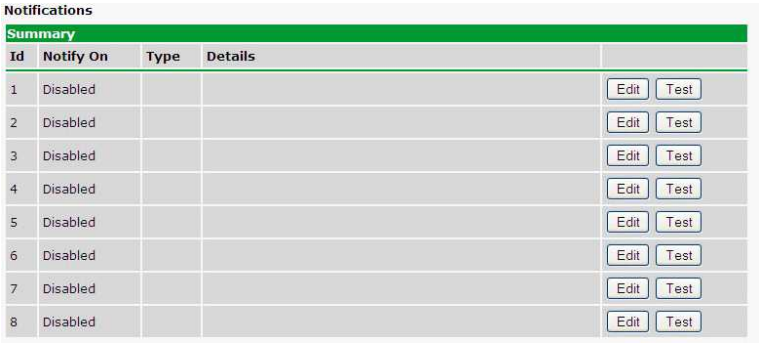
Quick Turn Up

13 Quick Turn Up

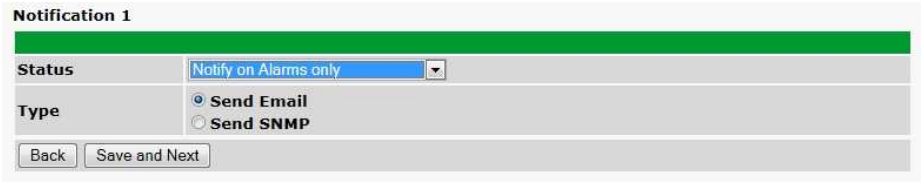
The next sections of this manual will walk you through some of the most common tasks for using the NetGuardian ENV. You will learn how to send email notifications, and send SNMP traps to your alarm master - all using the Web browser. For details on entering your settings into each Web browser menu, the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

13.1 How to Send Email Notifications

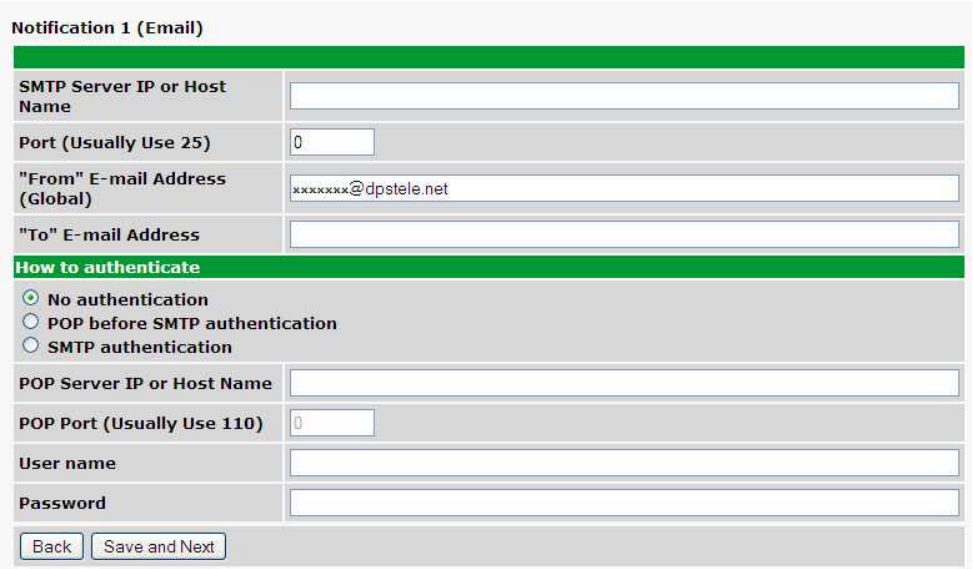
1. Click on the **Notifications** button in the **Provisioning** menu. You can setup as many as 8 different notifications. Begin the setup "wizard" by clicking **Edit** for a notification number. In this example, we'll setup Notification 1 to send emails.



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**.



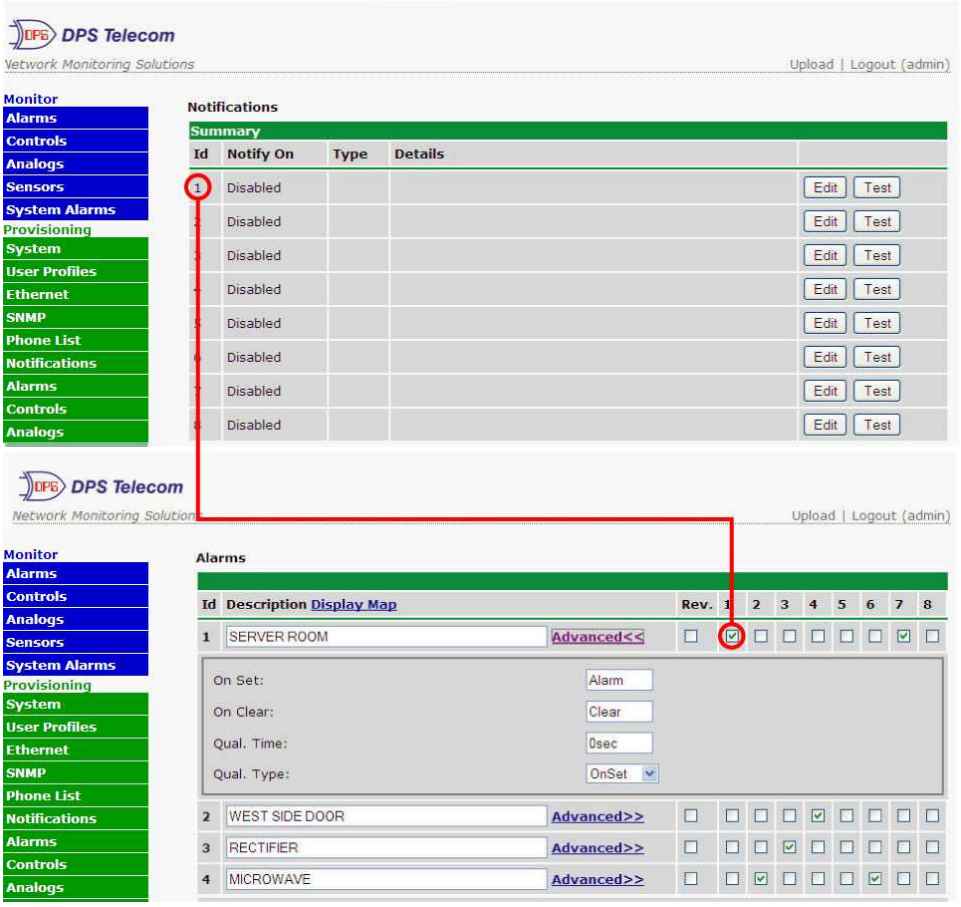
3. At the **Email Notification** screen, you'll enter your email server settings. Enter the **IP address** or **Host Name** of your email server. Enter the **Port Number** (usually 25) and the **"To" Email Address** of the technician that will receive these emails. If authentication is required, chose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

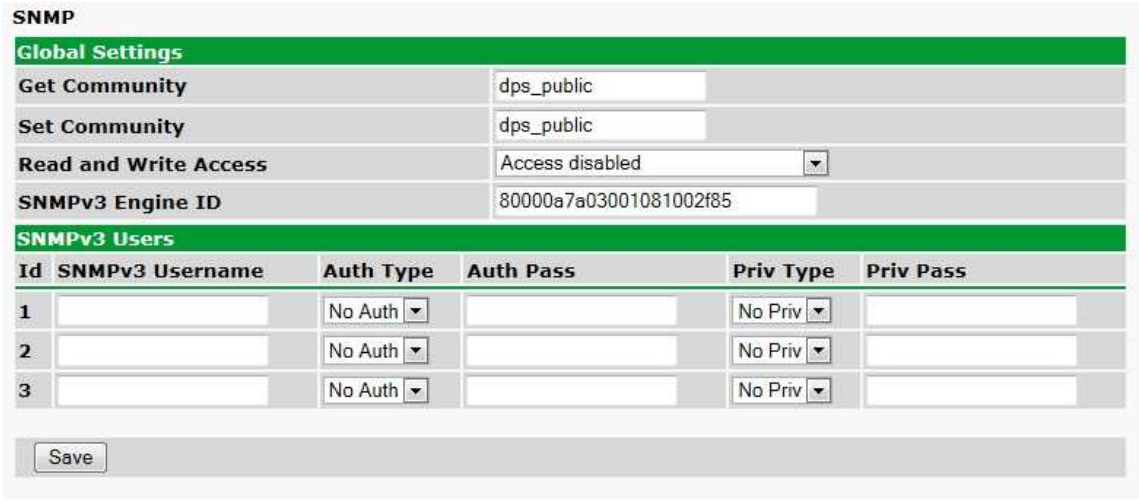
5. If you chose to test the email notification you've just setup, you will prompted with a pop up . Click **OK** to send a test email alarm notification. Confirm all your settings by checking your email to see if you've received it. **NOTE:** This test only means that your notification settings are correct,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



13.2 How to Send SNMP Traps

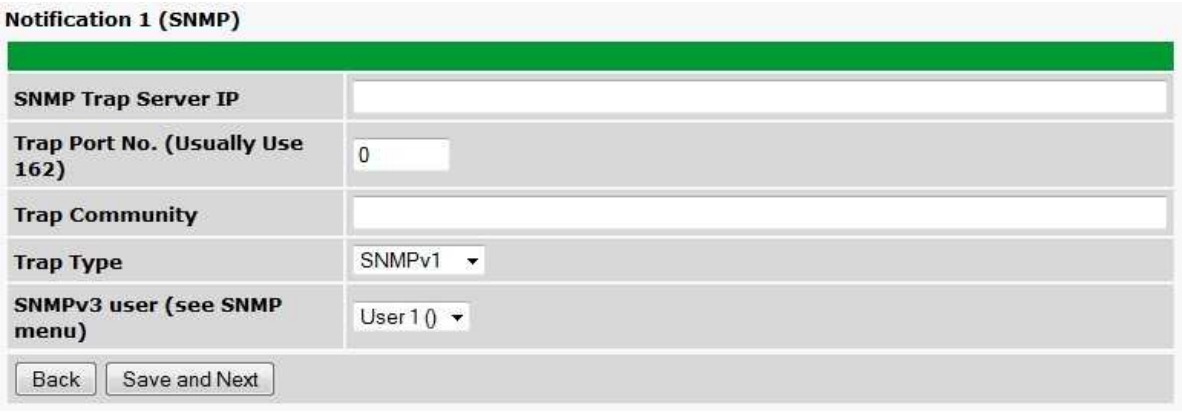
1. Click on the **SNMP** button in the **Provisioning** menu. Enter the **SNMP GET** and **SNMP SET** community strings for your network, then click **Save**. The typical SNMP SET and GET community strings for network devices is "public". As an added security measure, we've made our default "dps_public".



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.

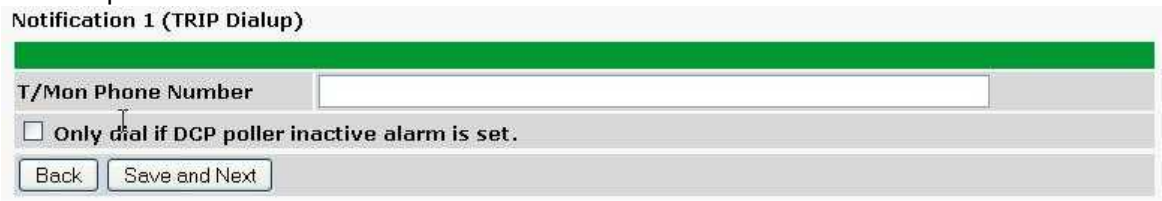
NOTE: This test only means that your notification settings are correct, but you still need to assign the notification to an alarm point. See Step 6 in "How to Send Email Notifications" for more detail.

13.3 How to Send TRIP Notifications

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

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

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



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

6. Click **Test** to send a test voice notification. **NOTE:** This test only means that your notification settings are correct, but you still need to assign the notification to an alarm point (See step 6 of the "How to Send Email Notifications" section).

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

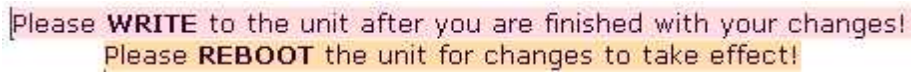
Provisioning Menu Field Descriptions

14 Provisioning Menu Field Descriptions

NetGuardian ENV 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 ENV:
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.

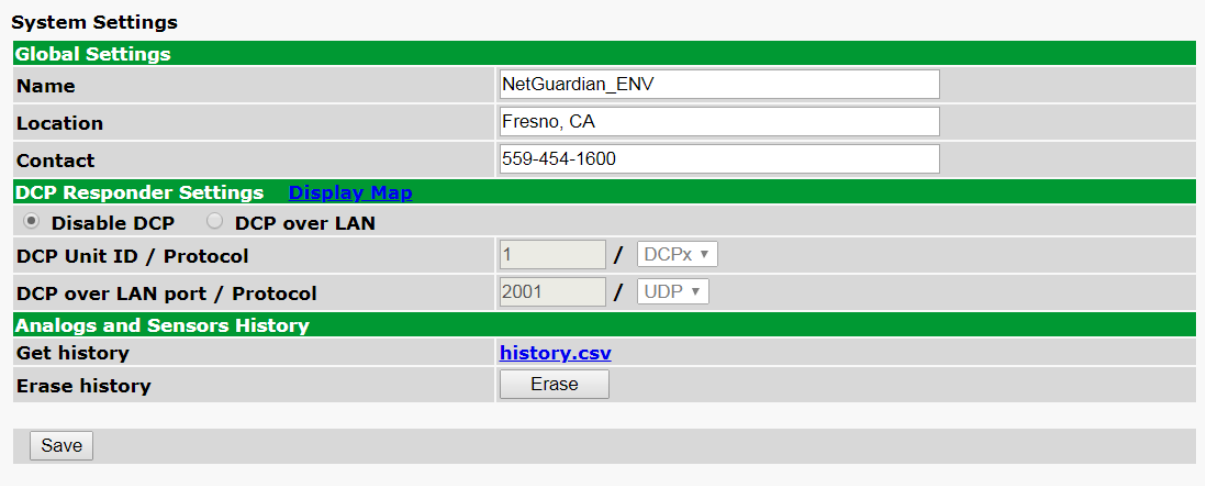


Status messages on the NetGuardian ENV Device Access menu, inform you how to implement your changes

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

14.1 System

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

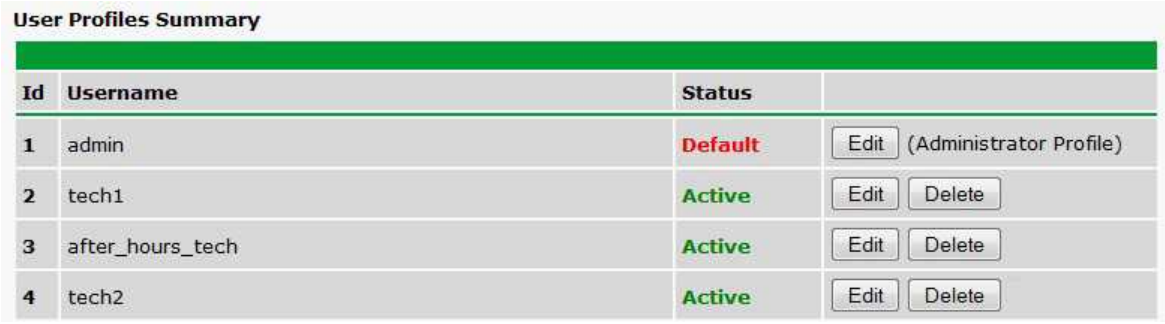


The Provisioning > System menu

Global System Settings	
Name	A name for this NetGuardian ENV unit. {Optional field)
Location	The location of this NetGuardian ENV unit. {Optional field)
Contact	Contact telephone number for the person responsible for this NetGuardian ENV 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
Sensors History	
Get History	Download a log of all configured analog and sensor values.
Erase History	Erase the log of all configured analog and sensor values.

14.2 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 7 additional unique user profiles, each with different access rights to the NetGuardian ENV's web interface.



Configure access privileges for users in the User Profile screen

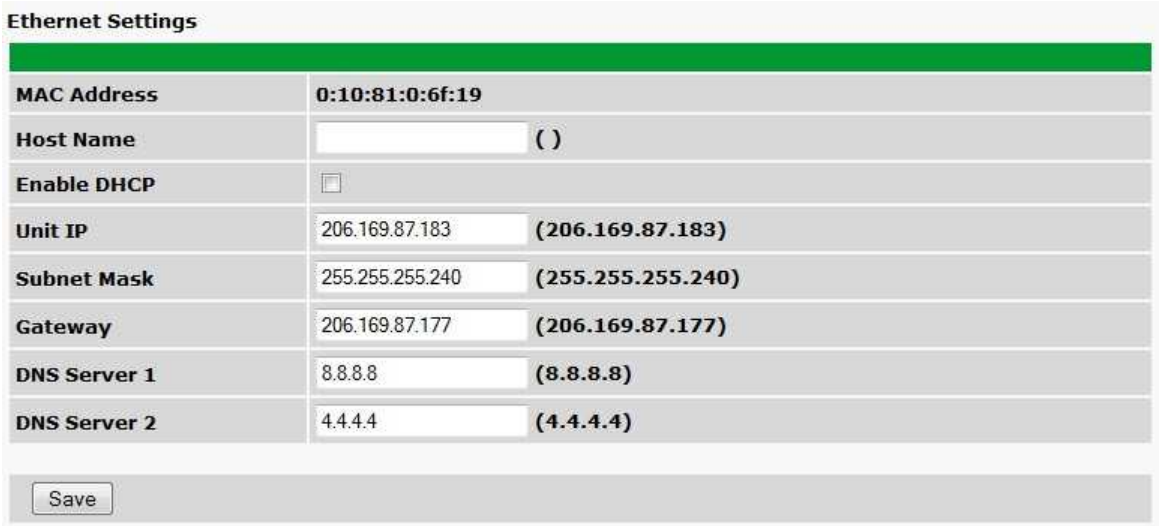
To create or edit any of the 8 user profiles (including the Admin), click the **Edit** button. From there, you can change all configurable settings for a user profile.

User Profile	
Suspend this Profile	If this box is checked, the profile will not be able to access the NetGuardian ENV.
Username	Enter a username or a user description
Password	Enter a unique user password **Note:** All passwords are AES 128 encrypted.
Confirm Password	Re-enter the password.
Access Rights	
Check all	Enables all Access Rights
Edit logon profiles	Enables the user to add/modify user profiles and password information.
Write Config (change unit configuration)	Enables the user to change the unit config by accessing the **Write** feature in the control menu.
View monitor pages	Allows the user to access Monitor menu options.
Send relay commands	Allows the user to send commands to operate the device's control relays.
TTY access (access via Craft port or via Telnet)	Grants the user access to the unit via TTY interface (via craft or telnet).
Initialize config to factory defaults	Allows the user to use the **Initialize** option in the **Device Access** menu, resetting the NetGuardian ENV 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

14.3 Ethernet

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



The Provisioning > Ethernet menu

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

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

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

14.4 RADIUS

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

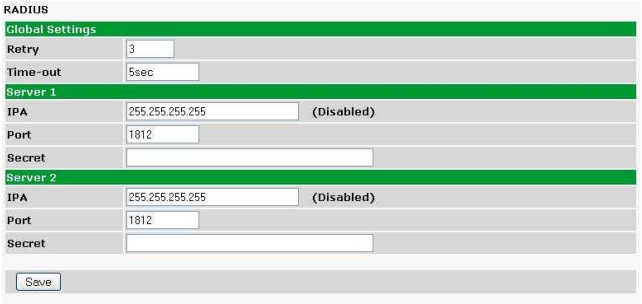


Fig. 2.1. *RADIUS configuration screen*

Fig. 2.2. *RADIUS server prompt for Username **and** Password.*

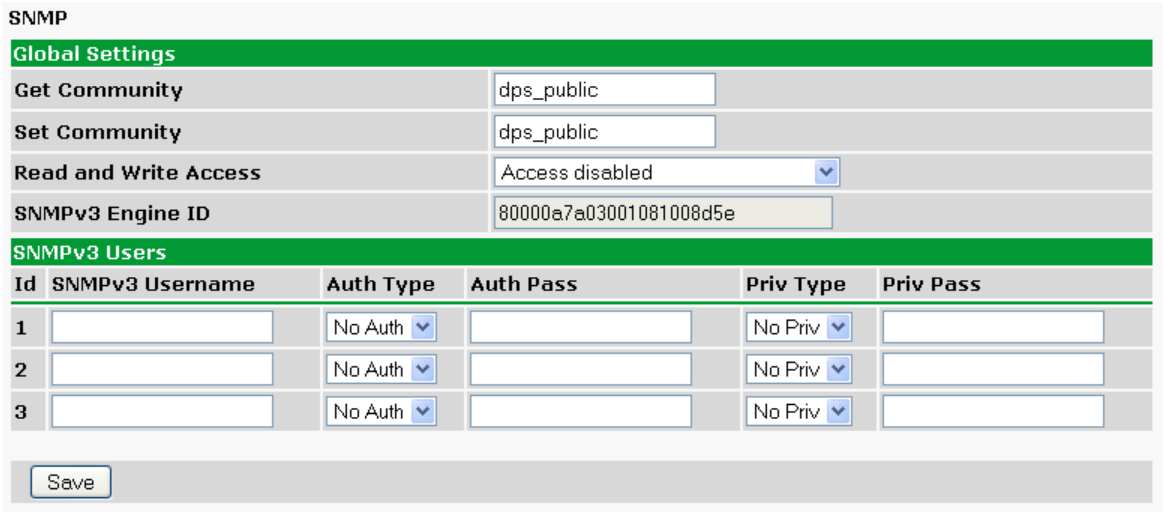
Global Settings	
Retry	Enter the number of times the RADIUS server should retry a logon attempt
Time-out	Enter in the number of seconds before a logon request is timed out
Servers 1 / 2	
IPA	Enter the IP address of the RADIUS server
Port	Port 1812 is an industry-standard port for using RADIUS
Secret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

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

RADIUS logons **are** case-sensitive. If the RADIUS server is unavailable or access is denied, the master password will work for craft port access only. Also, the "dictionary.dps" files (included on the Resource Disk) needs to be loaded on the RADIUS server for access-right definition. If RADIUS is enabled on the NetGuardian, the local authentication will not be valid.

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

Fields in the Provisioning > SNMP settings

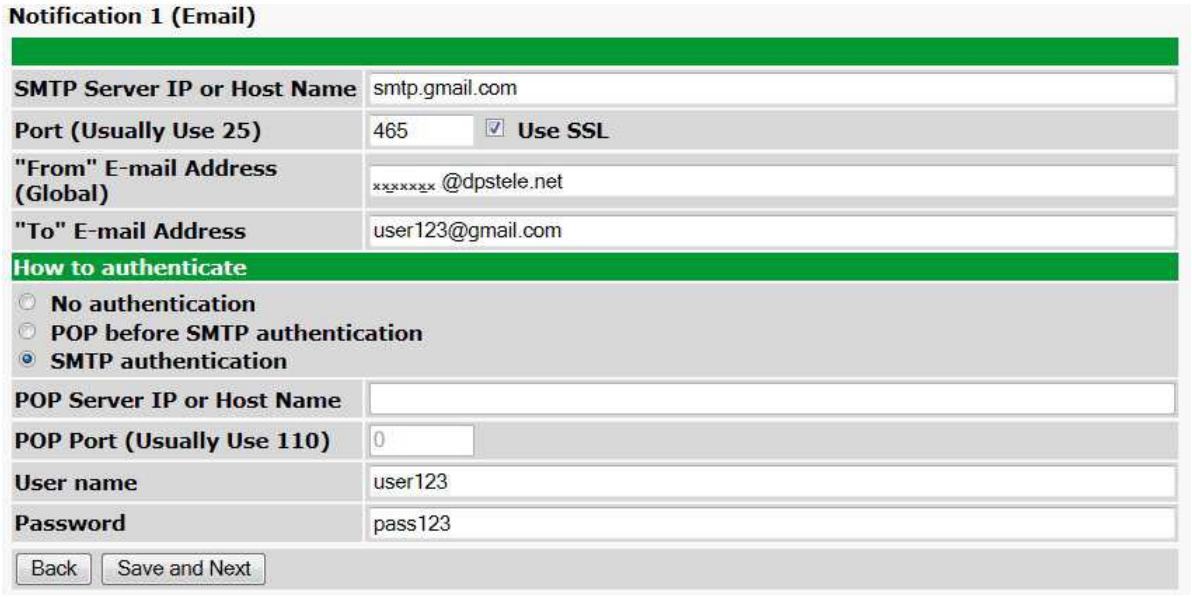
14.6 Notifications

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).

14.6.1 Notification Settings

Email Notification Fields

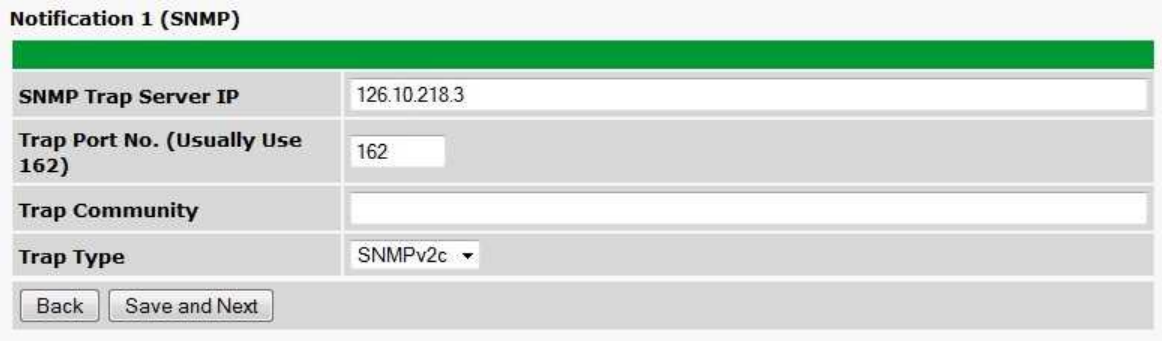


Editing Email Notification Settings

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

TRIP Dialup (T/Mon) Notification Fields

Editing Call notification settings

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

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

14.6.2 Schedule

The notifications scheduling menu is where you will tell the NetGuardian ENV 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.

14.7 Alarms

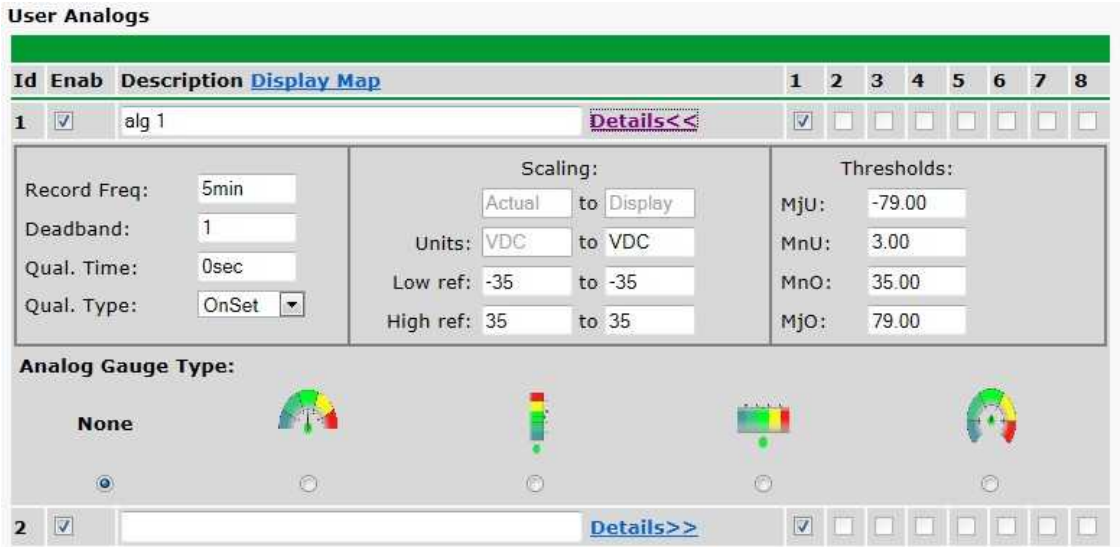
Discrete alarms are configured from the **Provisioning** > **Alarms** menu. Descriptions for the alarm points, polarity (normal or reversed) and notification type(s) are defined from this menu. You also have the option to use **Basic** or **Advanced** configuration methods, explained in this section.

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 f that alarm point.
Advanced Alarm Configuration (Advanced>>)	
On Set	User-definable description (condition) that will appear for the discrete alarm input on S 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 Se Clear, or Both.

14.8 User Analogs

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



The Provisioning > User Analogs menu

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

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

14.9 Controls

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

The Provisioning > Controls screen

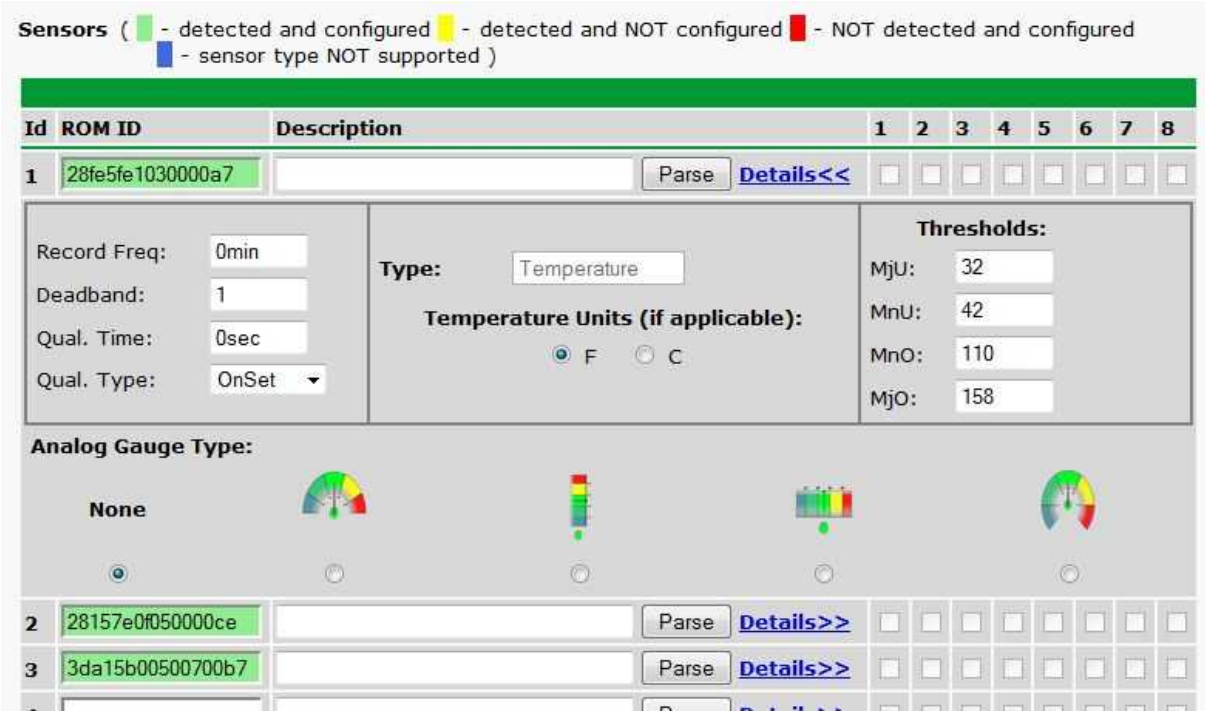
Basic Controls Configuration	
ID	ID number for the control relay.
Description	User-definable description for the NetGuardian ENV's control relay.
Derived Description	Formula to control relay operation. Control relays and virtual alarms can be created from derived formulas using the following operations: **_OR** : Set the current operation to OR. **_AN** : Set the current operation to AND. **_XR** : Set the current operation to XOR. **D** : Tag to change the active display number. . : Used like a comma to delimit numbers. - : Used to specify a range of points.
Momentary Time	Control on time (in milliseconds) when you execute the MOM command. Max limit of 6 seconds.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications f the control relay.

14.10 Sensors

D-Wire Sensors
The NetGuardian ENV supports up to 32 daisy-chained D-Wire sensors via its D-Wire input. Sensors connected to the NetGuardian ENV 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 ENV'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 ENV'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 NetGuardia ENV will automatically detect the sensor ID when you plug a sensor into the unit. The 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 configu fields and click **Save** to configure the sensor). **Red** - The sensor is not detected and configured (i.e. a previous configured sensor is longer connected). **Blue** - The sensor is not supported by the NetGuardian ENV. To reconfigure or disable the Sensor ID, simply delete any data in this field and click **S** 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 f 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 Se Clear, or Both.
Thresholds	These settings are set to indicate the severity of the alarm depending on which thresho values have been passed. Enter values for Major Under (MjU), Minor Under (MnU), Mi Over (MnO), and Major Over (MjO).
Analog Gauge Type	Select the color-coded gauge that best represents your data. Selecting **None** will disa the analog gauge and only a numerical representation of the value will be displayed un **Monitor** > **Sensors**.

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

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

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

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

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

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

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

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

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

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

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

Example of how an equation is evaluated:

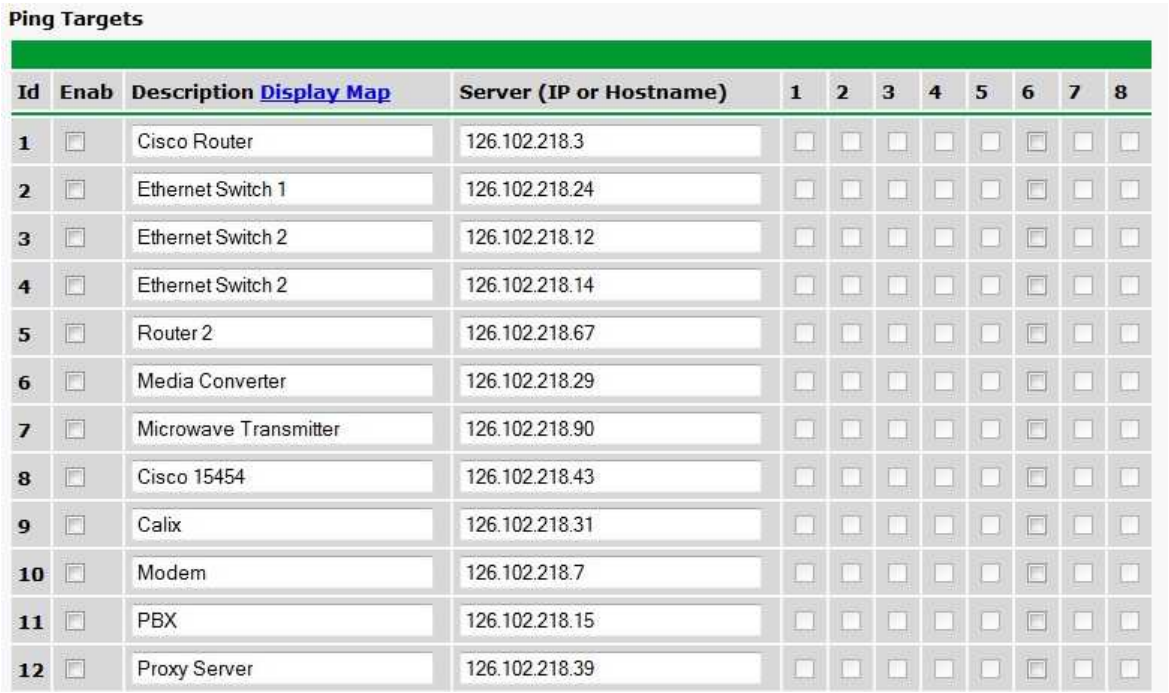
Equation: a8 a5 a6 + * a4 -

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

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

14.11 Ping Targets

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

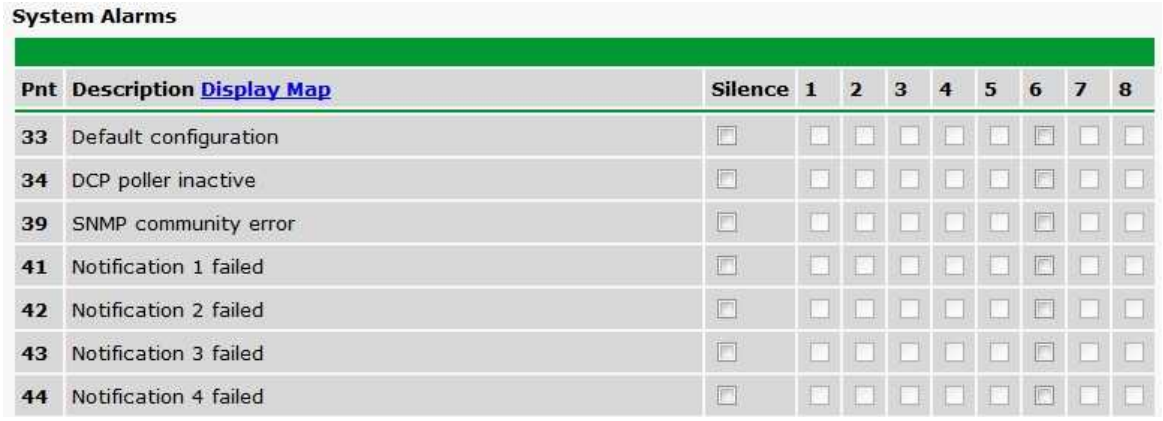


The Provisioning > Ping Targets menu

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.

14.12 System Alarms

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



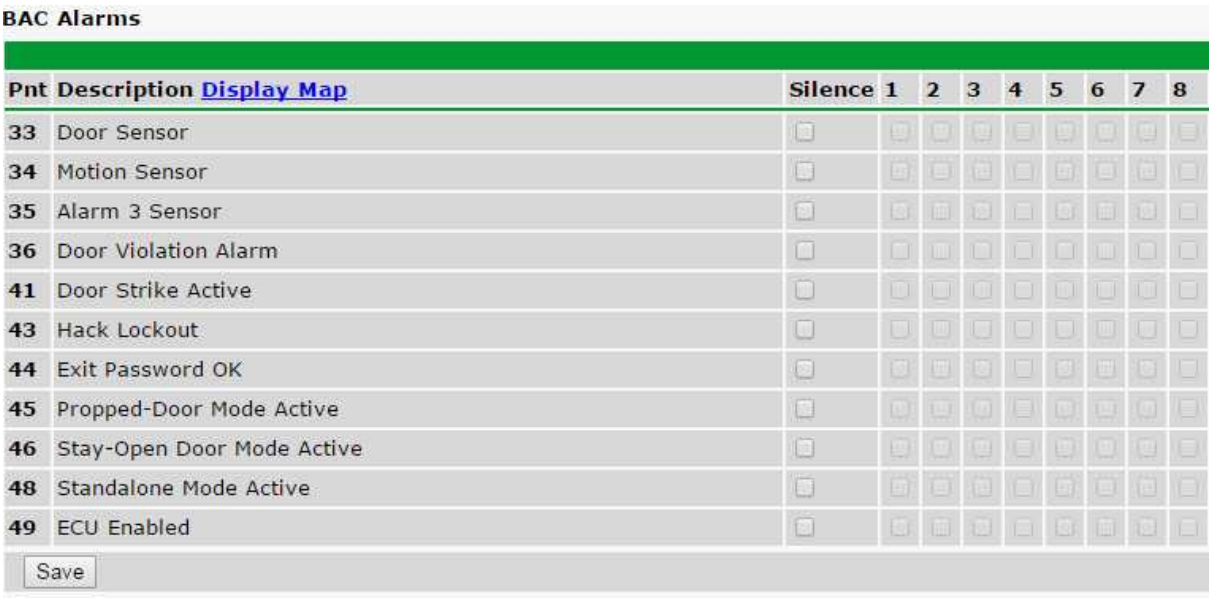
System Alarms

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

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.

14.13 BAC Alarms



BAC Alarms

Pnt	Description Display Map	Silence	1	2	3	4	5	6	7	8
33	Door Sensor									
34	Motion Sensor									
35	Alarm 3 Sensor									
36	Door Violation Alarm									
41	Door Strike Active									
43	Hack Lockout									
44	Exit Password OK									
45	Propped-Door Mode Active									
46	Stay-Open Door Mode Active									
48	Standalone Mode Active									
49	ECU Enabled									

Save

14.14 BAC Globals

From the **BAC Globals** menu, you can configure the DCP responder settings for communicating with T/Mon, how your NetGuardian ENV will validate access, and enable special door-control behaviors.

From the BAC Globals screen, you can determine building access functionality for your door

DCP Responder Settings *(For use with T/Mon)*	
DCP over LAN	Enables DCP transmissions over LAN (Enabled by default)
DCP Unit ID/Protocol	User-definable ID number for the NetGuardian ENV (DCP Address), and the DCP protocol being used (DCPx or DCPf).
DCP over LAN port/Protocol	Enter the DCP port for this NetGuardian ENV (UDP/TCP port).

The **BAC Settings** allow you to configure NetGuardian ENV profile validation and door control behavior

- **Alarm Controller Speaker**, when configured, will trigger the control for the speaker when the alarm point configured becomes active.
- **Max Key Presses** - Maximum limit to the number of keypad keys that can be entered before the ENV will process the entry.

The radio buttons determine the method the NetGuardian ENV will use to authenticate door access.

- **Use internal profiles only when TMon profiles are not available** set's the NetGuardian ENV to use profiles from T/Mon to validate door access unless the T/Mon database has been purged (see the **System** section for details on purging the BAC database), corrupted, or has not yet been downloaded from T/Mon. **This is the default setting.**
- **Use internal profiles only, and ignore TMon profiles** sets the NetGuardian ENV to work in **Standalone** mode. In this mode, the ECU controls door access with its own internally databased access profiles. It will **not** use access information from T/Mon to make entry decisions. (**Note:** the

ECU can still report door violations and access if being polled by T/Mon.)

- **Do not use internal profiles, and use TMon profiles only** configures the NetGuardian ENV to ignore its internal profiles. If T/Mon's database has not yet been downloaded, been purged (see the **System** section for details on purging the BAC database), or corrupted, an ECU operating in this mode will essentially make a door inaccessible.

The checkboxes in the BAC Settings section determine any special behaviors for the door.

- **Using magnetic door lock (uncheck if using door strike)** configures the NetGuardian ENV to operate in **Magnetic Door Mode**. In Magnetic Door Mode, the door will remain magnetically locked until unlocked via proxy card scan, Request-to-Exit button, or motion sensor. Enabling magnetic door mode reverses the relay energize state from normally open to normally closed, keeping the electromagnetic lock powered (locked) until access is granted.
- **Enable request to exit when using door strike.** Door will remain locked until a proxy card scan, Request-to-Exit or motion sensor trigger is detected.
- **Keep door unlocked until close detected** sets the door to lock a few seconds after it has been detected closed, and can be usefully combined with "Magnetic Door Mode" to ensure the door has closed first before the lock is applied. In this mode, if the door does not open after it has been unlocked, It will lock again after 2-3 seconds.
- **Enable direction logic for logging in/out activity** enables the unit's in-out clocking function. In this mode, T/Mon will log whether a user is entering or exiting the door (by keypad, following a passcode, a user will enter 1 for "in" or 4 for "out")

Click **Save** at the bottom of the screen to commit your changes to the NetGuardian ENV.

Building Access Unit Mode (BAU):
In BAU mode the NetGuardian does not use a relay and key code combination to control facility access for the purpose of determining door violations. In this mode of operation no codes are stored in the local BAC profile database and access to the site is granted by issuing an OPR command to Display 2 point 46 "Extended Propped Door Mode". If access to the facility has not been granted using this method and a door is opened, a door warning period will begin, followed by a door violation.

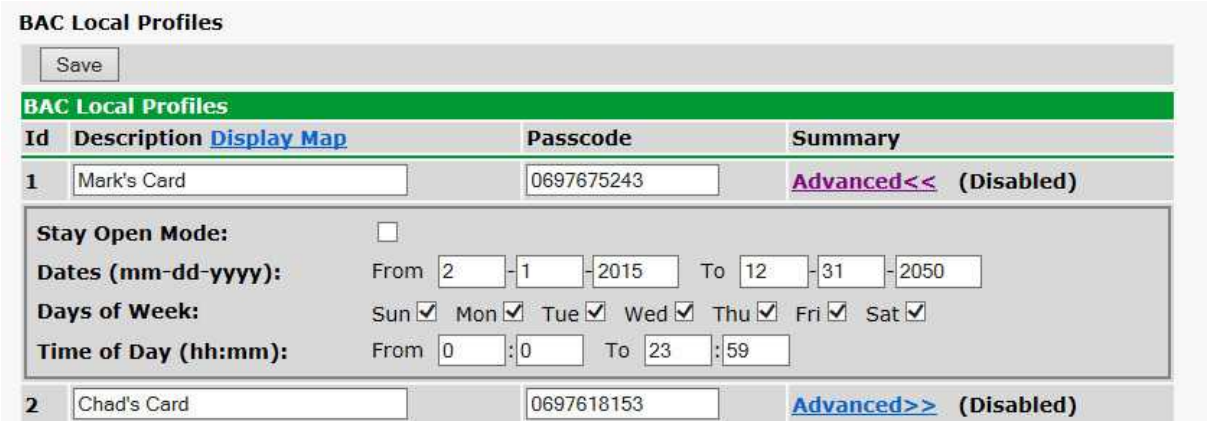
Clearing the Door Violation alarm:
- Sending an OPR command to Display 2, Point 46 from T/Mon will enter "Extended Propped Door Mode" and will suppress the speaker sounding under an alarm condition. The OPR command will also clear a “Door Violation” alarm status. To cancel this mode send a RLS command from T/Mon to Display 2, Point 46.
- Sending a MOM command to Display 2, Point 46 from T/Mon will clear a Door Violation Alarm Status and reset the speaker progression.

BAU Mode Setup:
1. Set Provisioning > BAC Globals > BAC ID to 0
2. Set the Provisioning > BAC Globals > Speaker Sound Control ID to the Control Id that is connected to the external speaker.
3. For the Control Id chosen as the Speaker Sound Control ID, set the Provisioning > Controls > Details > Derived Description to "_ORD1.1-N", where N is the max number of discrete alarms supported.

14.15 BAC Profiles

From the **BAC Profiles** screen, you can manage up to 32 internal profiles for valid door access.

Note: By default, the NetGuardian ENV's internal profiles will be used to validate door access only when not configured with T/Mon. These profiles are **not** databased in T/Mon unless you do so manually. You can alter the NetGuardian ENV's behavior for determining when to utilize its own internal profiles to validate door access from the **BAC Globals** screen.



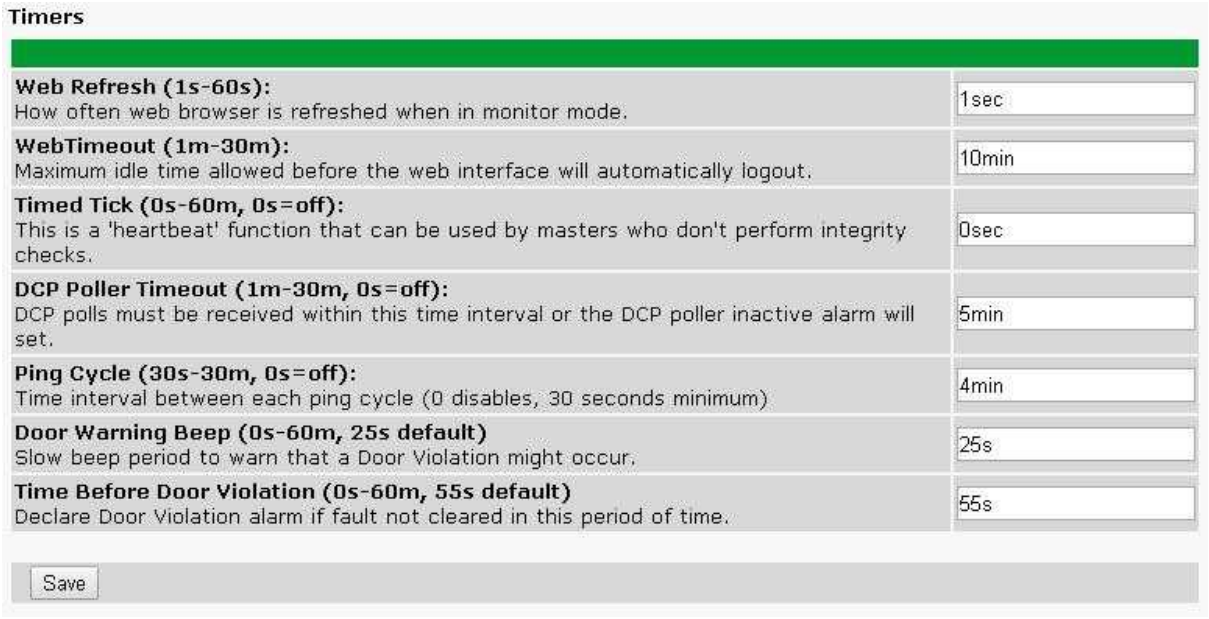
The BAC Profiles Screen

To configure profiles:

1. Enter a **Description** for the profile (typically, the name or the purpose of the profile)
2. Enter the **Passcode** that will be used to authenticate door access, either a code that will be entered manually on the keypad or a code associated with a proxy card. If using a proxy card, you can read the passcode associated with the card by placing the unit in debug mode. See the section of this manual titled **Determining Proximity Card Numbers** for more information.
3. Set Date and Time restrictions for the profile. The **Summary** field will show any access restrictions for a profile by Date, day of the week, or time. By default, a profile is set to be able to access a door without date or time restrictions. To configure access restrictions for any profile, click **Advanced<<**.
   - o Enable **Stay Open Mode** if you want the door to remain unlocked after the passcode is entered. In this mode, you can lock the door again by re-entering the passcode (by proxy or keypad), or by logging into the NetGuardian ENV and issuing a RLS command to point 22. This mode is disabled by default.
   - o Enter **Dates** for valid use of the profile. By default, profiles are set with virtually no expiration date.
   - o Enter **Days of the Week** during which the profile will be valid.
   - o Enter the **Time of Day** during which the profile can access the door. All times are set in military. By default, there is no time restriction (the Time of Day fields are set to 00:00 and 23:59)
4. Repeat the above steps for any profiles you wish to configure. When you are finished, click **Save** at the bottom of the screen to commit the profiles to the NetGuardian ENV.

14.16 Timers

The **Timers** menu allows you to change how often certain NetGuardian ENV specific events occur.



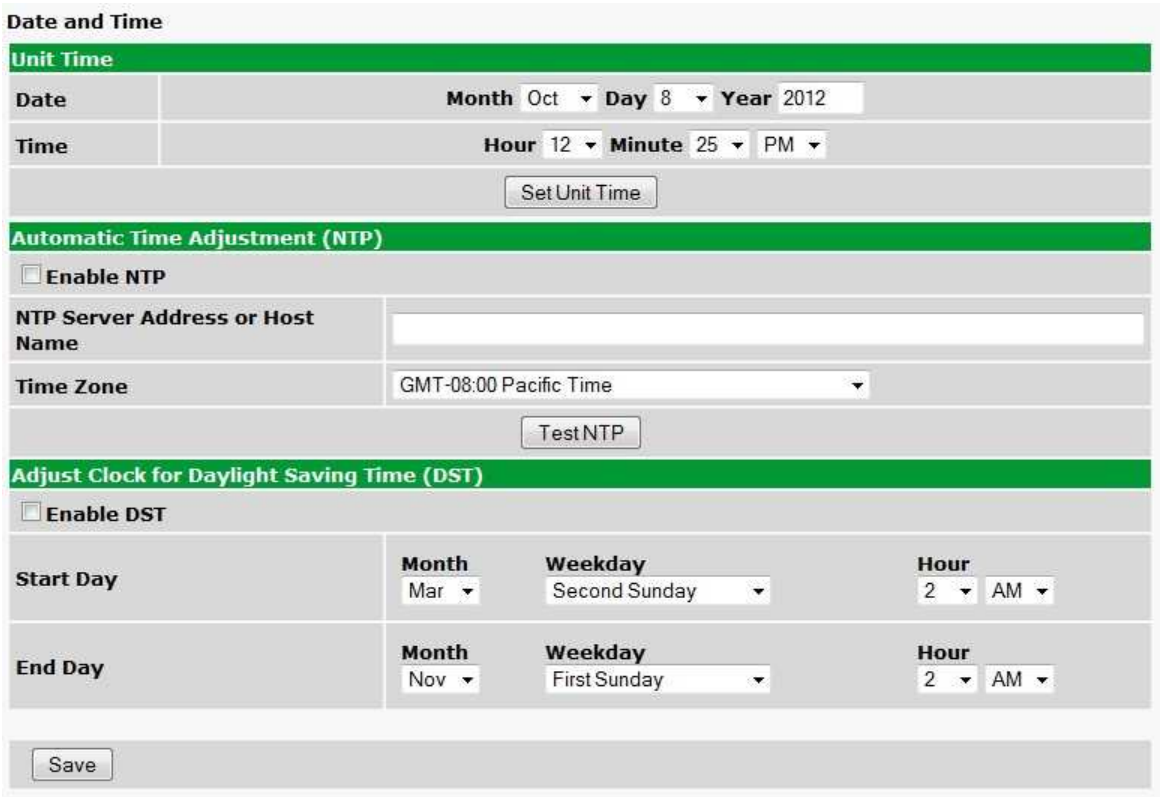
The Edit > Timers menu

Timers	
Web refresh	How often the web browser is refreshed when in monitor mode.
WebTimeout	Maximum idle time allowed before the web interface will automatically logout.
Timed Tick	The "hearbeat" function that can be used by masters who don't perform integrity checks.
DCP Poller Timeout	DCP polls must be received within this time interval or the DCP poller inactive alarm will s
Ping Cycle	Time interval between each ping cycle (0 disables, 30 seconds minimum).
Door Warning Beep	The amount of time after the door is unlocked before a slow beep will occur to alert the pe entering or exiting that a door violation is about to occur. **Note:** Set the Door Warning Be some number of seconds less than the Time Before Door Violation, otherwise you will not receive warning for potential door violations.
Time Before Door Violation	The time after which a violation will occur if a fault has not been cleared.

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

The Provisioning > Timers menu

14.17 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 h 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 ENV 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.

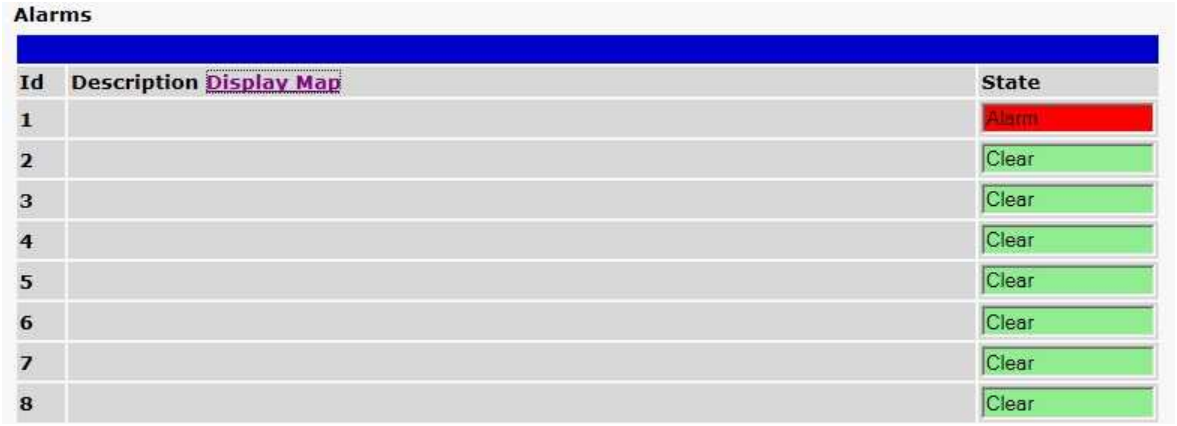
This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

Monitoring via the Web Browser

15 Monitoring via the Web Browser

15.1 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.



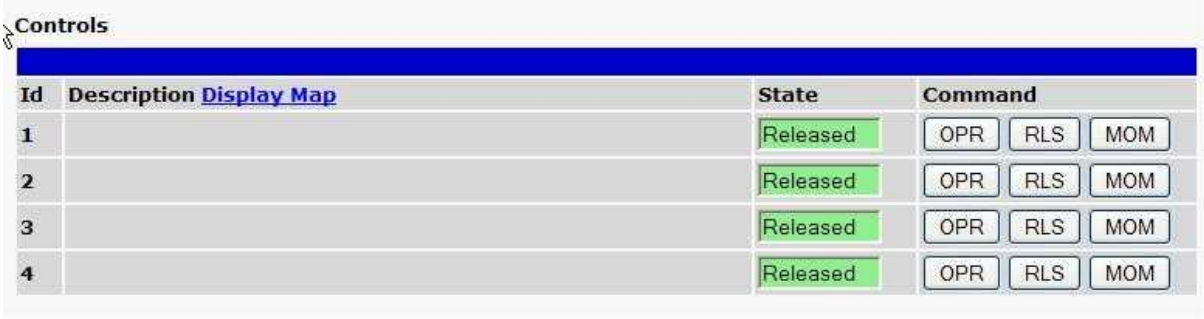
Click on Alarms in the Monitor menu to see if any base alarms (1-8) have been triggered.

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)

15.2 Controls

Use the following rules to operate the NetGuardian ENV's control:

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

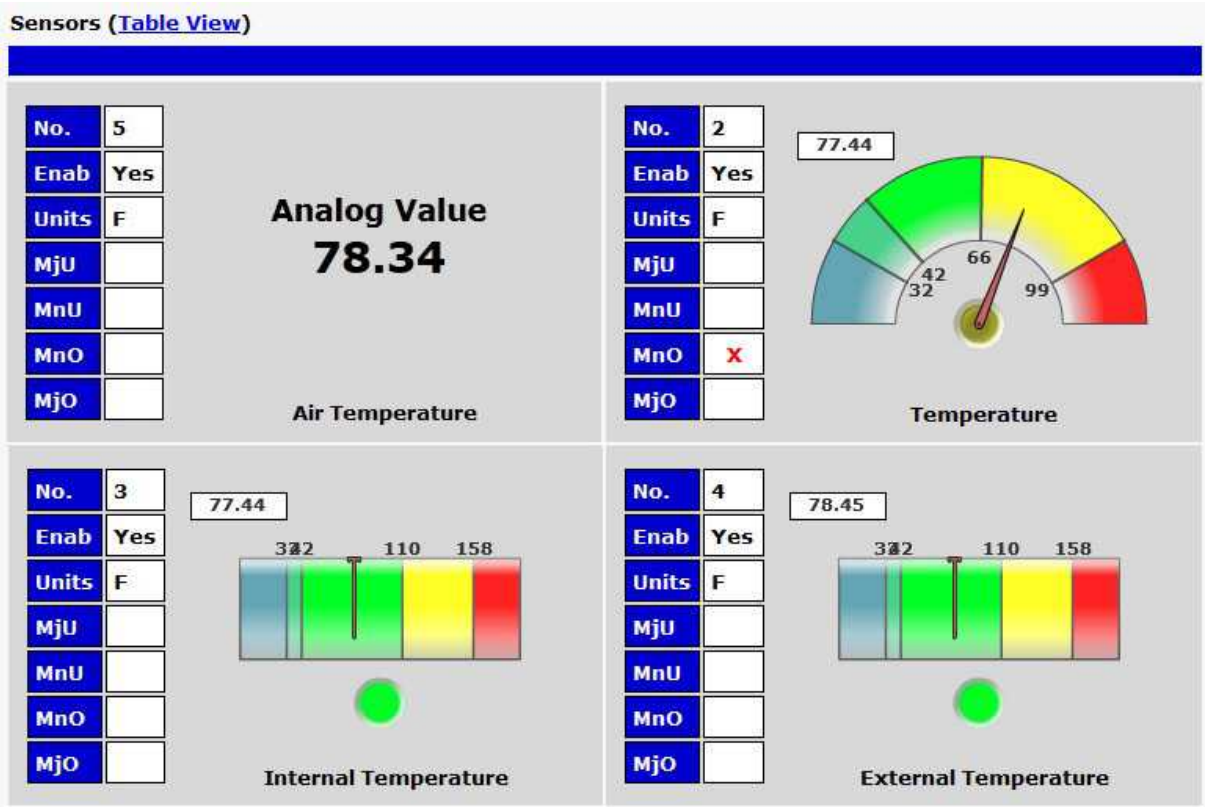


View and operate control relays from the Monitor > Controls menu

Control Relay Operation	
ID	ID number for the control relay.
Description	Description for the NetGuardian ENV'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 the latch is defined in the Provisioning > Controls menu.

15.3 Sensors

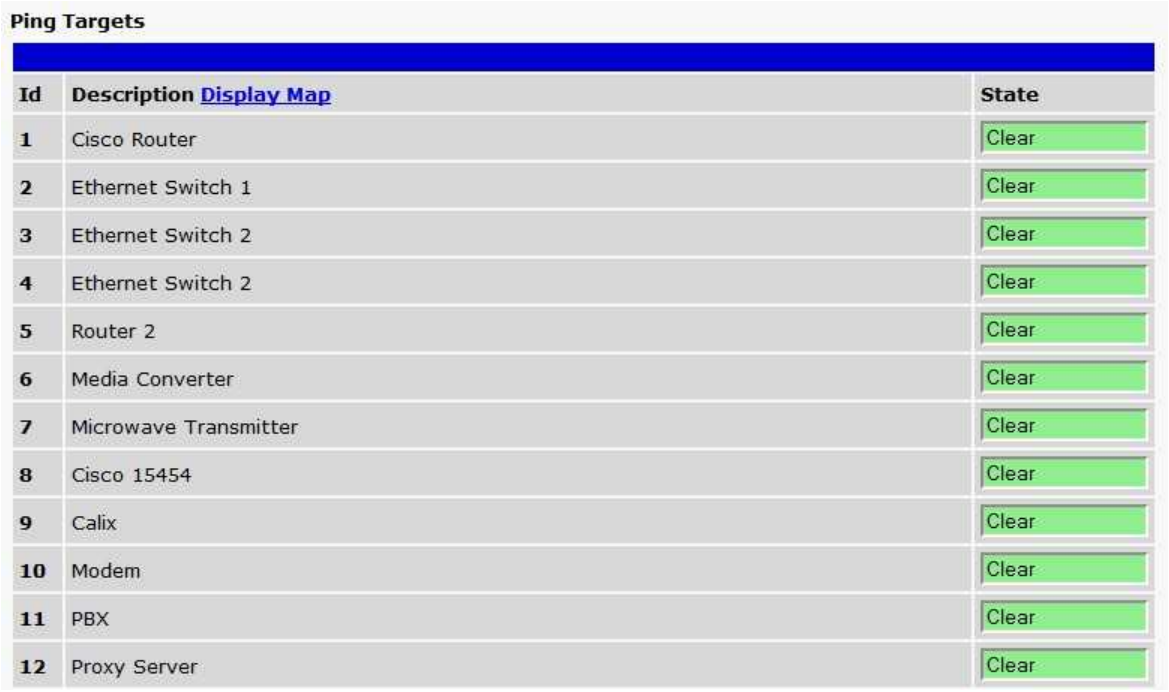
This selection provides the status of the system's analog channels by indicating if an alarm has been triggered. The **Monitor** > **Sensors** screen provides a description of each analog channel, the current reading, the units being read, and alarm conditions (major under, minor under, major over, minor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

15.4 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.



Ping Targets

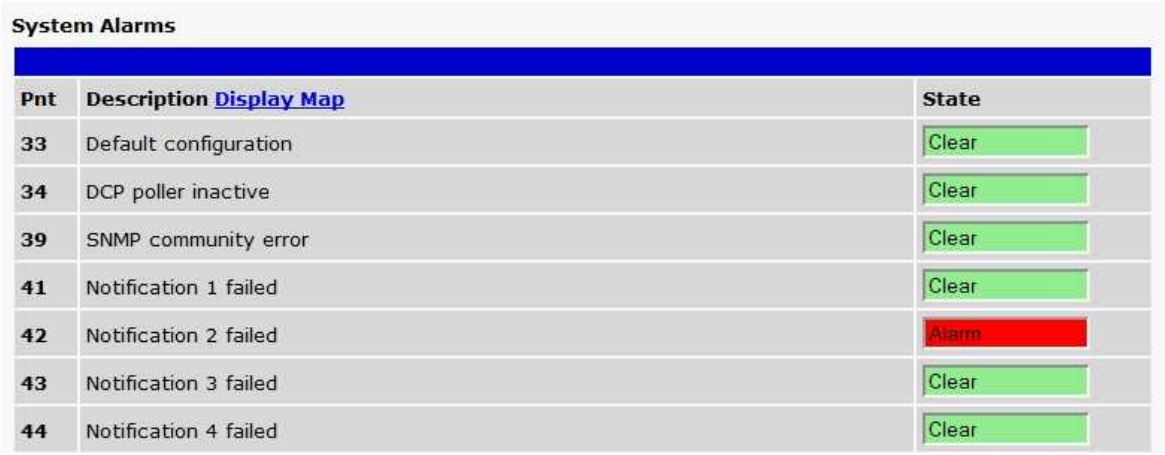
Id	Description Display Map	State
1	Cisco Router	Clear
2	Ethernet Switch 1	Clear
3	Ethernet Switch 2	Clear
4	Ethernet Switch 2	Clear
5	Router 2	Clear
6	Media Converter	Clear
7	Microwave Transmitter	Clear
8	Cisco 15454	Clear
9	Calix	Clear
10	Modem	Clear
11	PBX	Clear
12	Proxy Server	Clear

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

15.5 System Alarms

System alarms are not-editable, housekeeping alarms that are programmed into NetGuardian ENV. 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	DCP poller inactive	Clear
39	SNMP community error	Clear
41	Notification 1 failed	Clear
42	Notification 2 failed	Alarm
43	Notification 3 failed	Clear
44	Notification 4 failed	Clear

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

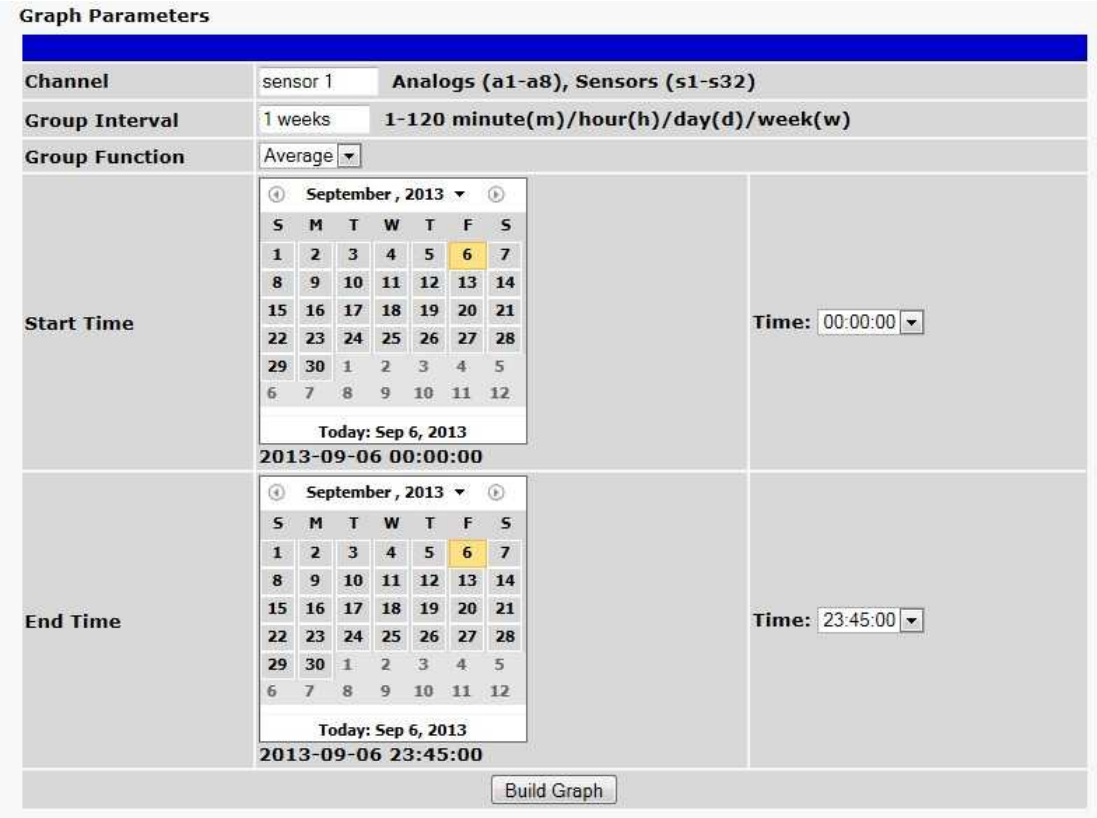
15.6 BAC Alarms

BAC Alarms

Pnt	Description Display Map	State
33	Door Sensor	Clear
34	Motion Sensor	Clear
35	Alarm 3 Sensor	Clear
36	Door Violation Alarm	Clear
41	Door Strike Active	Clear
43	Hack Lockout	Clear
44	Exit Password OK	Clear
45	Propped-Door Mode Active	Clear
46	Stay-Open Door Mode Active	Clear
48	Standalone Mode Active	Clear
49	ECU Enabled	Clear

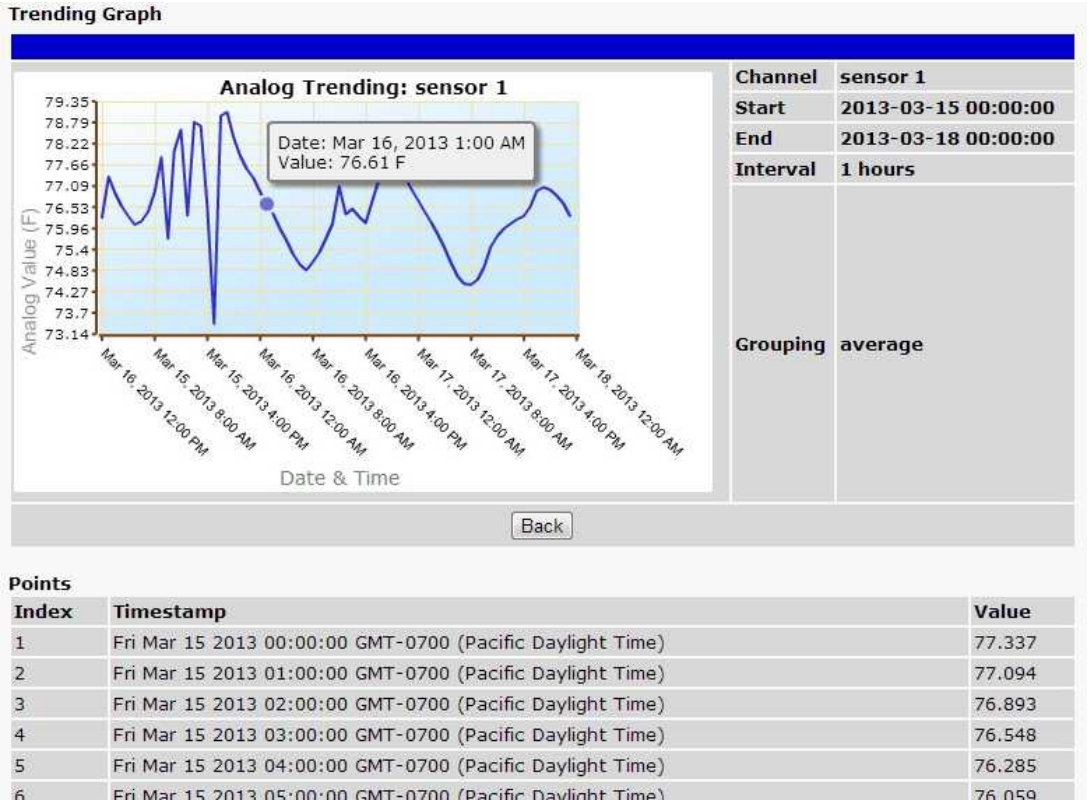
15.7 Graph

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.

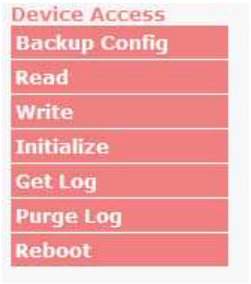
Your graph will appear on the next screen. This graph is Adobe Flash-based and allows you to mouse over the lines to quickly view measurements (date, time, and value) within their context of the overall graphing trend. Below the graph is a full textual list of all indexed points with their dates and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



Specify your parameter values and build an interactive graph based on the alarm point history.

16 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 ENV'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 ENV's non-volatile m
Initialize	Sets the unit's configuration to factory default values
Get Log	Opens the NetGuardian ENV's event log in Notepad (or another plain text editor).
Purge Log	Deletes the NetGuardian ENV's event log history.
Reboot	Reboots the NetGuardian ENV.

17 Backup Configuration

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

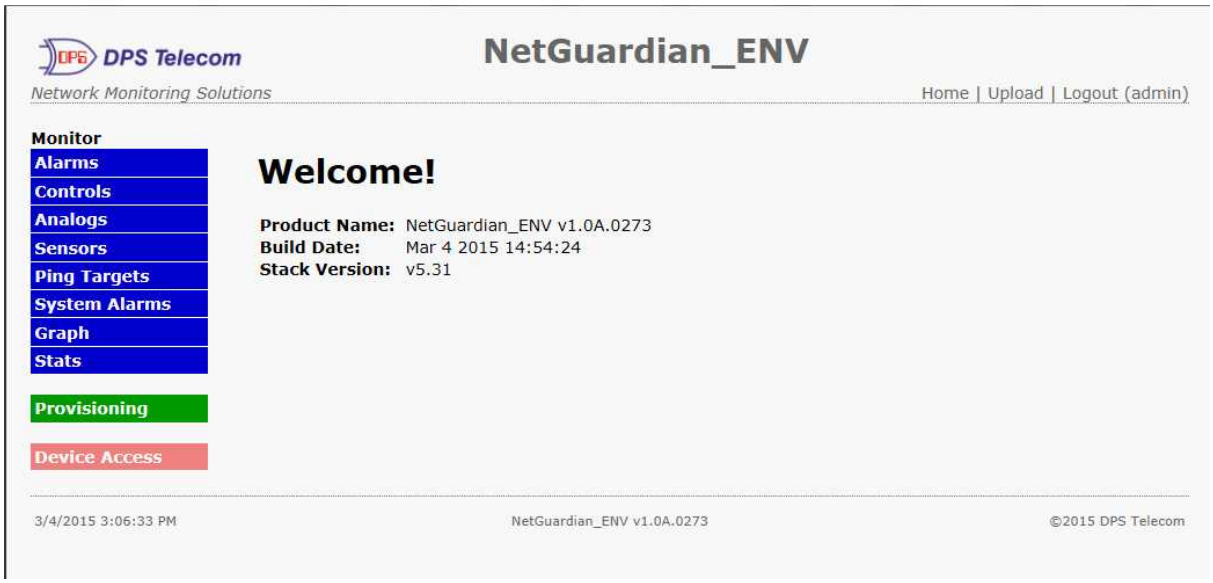
*To upload your configuration file, click on **Upload** on the top right corner of the web interface*

How to upload a saved configuration:

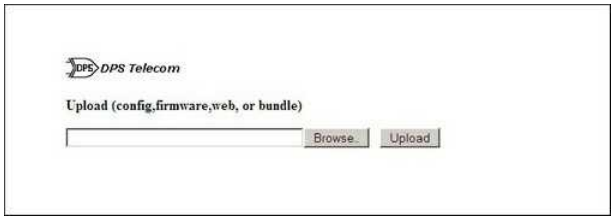
1. Click the upload button at the top right corner of the Welcome screen.
2. Click the Browse... button
3. Browse to the location of the .bin file from the steps above.
4. Select that .bin file and press the Upload button.
5. You should now have the same configuration settings loaded from when you saved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

18 Firmware Upgrade

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 **Upload**.



Browse for downloaded firmware upgrade

Reference Section

19 Reference Section

19.1 Display Mapping

Display Mapping

Display	Point	Description
Display 1	1-8	Discrete Alarms 1-8
	9-16	Undefined
	17-22	Controls 1-6
	23-32	Undefined
	33	Default configuration
	34	DIP Switch Config
	35	MAC Address Not Set
	36	IP Address Not Set
	37	LAN Hardware Error
	38	SNMP Processing Error
	39	SNMP community error
	40	LAN TX packet drop
	41	Notification 1 failed
	42	Notification 2 failed
	43	Notification 3 failed
	44	Notification 4 failed
	45	Notification 5 failed
	46	Notification 6 failed
	47	Notification 7 failed
	48	Notification 8 failed
	49	NTP failed
	50	Timed tick
	51	Serial RCV Q
	52	Dynamic Mem Full
	53	Unit Reset
	54	DCP Poll Inactive
	55	Reserved
	56	Reserved
	57	Reserved
	58	Reserved
	59	Reserved
	60	Reserved
	61	Reserved
	62	Reserved
	63	Reserved
	64	Reserved

Display	Point	Description
Display 2	1-32	Ping Alarms 1 - 32
	33	Door Sensor(Alarm 1)
	34	Motion Sensor (Alarm 2)
	35	Alarm 3 Sensor
	36	Door Violation Alarm
	37 - 40	Unused
	41	Door Strike Active (relay #1)
	42	Relay #2 Active
	43	Hack Lockout
	44	Exit Password OK

	45	Propped-Door Mode Active
	46	Stay-Open Door Mode or Extended Propped-Door Mode Active
	47	Standalone Mode Active
	48	ECU Enabled
	49 - 64	Unused

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

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

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

Display	Point	Description
Display 6	1	Analog 7 Minor Under
	2	Analog 7 Minor Over
	3	Analog 7 Major Under
	4	Analog 7 Major Over
	9-16	Control
	17-32	Value
	33	Analog 8 Minor Under

	34	Analog 8 Minor Over
	35	Analog 8 Major Under
	36	Analog 8 Major Over
	41-48	Control
	49-64	Value

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

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

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

Display	Point	Description
Display 10	1	Digital sensor 7 Minor Under

	2	Digital sensor 7 Minor Over
	3	Digital sensor 7 Major Under
	4	Digital sensor 7 Major Over
	5	Digital sensor 7 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 8 Minor Under
	34	Digital sensor 8 Minor Over
	35	Digital sensor 8 Major Under
	36	Digital sensor 8 Major Over
	37	Digital sensor 8 Sensor not detected
	41-48	Control
	49-64	Value

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

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

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

	35	Digital sensor 14 Major Under
	36	Digital sensor 14 Major Over
	37	Digital sensor 14 Sensor not detected
	41-48	Control
	49-64	Value
Display	Point	Description
Display 14	1	Digital sensor 15 Minor Under
	2	Digital sensor 15 Minor Over
	3	Digital sensor 15 Major Under
	4	Digital sensor 15 Major Over
	5	Digital sensor 15 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 16 Minor Under
	34	Digital sensor 16 Minor Over
	35	Digital sensor 16 Major Under
	36	Digital sensor 16 Major Over
	37	Digital sensor 16 Sensor not detected
	41-48	Control
	49-64	Value
Display	Point	Description
Display 15	1	Digital sensor 17 Minor Under
	2	Digital sensor 17 Minor Over
	3	Digital sensor 17 Major Under
	4	Digital sensor 17 Major Over
	5	Digital sensor 17 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 18 Minor Under
	34	Digital sensor 18 Minor Over
	35	Digital sensor 18 Major Under
	36	Digital sensor 18 Major Over
	37	Digital sensor 18 Sensor not detected
	41-48	Control
	49-64	Value
Display	Point	Description
Display 16	1	Digital sensor 19 Minor Under
	2	Digital sensor 19 Minor Over
	3	Digital sensor 19 Major Under
	4	Digital sensor 19 Major Over
	5	Digital sensor 19 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 20 Minor Under
	34	Digital sensor 20 Minor Over
	35	Digital sensor 20 Major Under
	36	Digital sensor 20 Major Over
	37	Digital sensor 20 Sensor not detected
	41-48	Control
	49-64	Value
Display	Point	Description
Display 17	1	Digital sensor 21 Minor Under

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

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

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

Display	Point	Description
Display 20	1	Digital sensor 27 Minor Under
	2	Digital sensor 27 Minor Over
	3	Digital sensor 27 Major Under
	4	Digital sensor 27 Major Over
	5	Digital sensor 27 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 28 Minor Under
	34	Digital sensor 28 Minor Over

	35	Digital sensor 28 Major Under
	36	Digital sensor 28 Major Over
	37	Digital sensor 28 Sensor not detected
	41-48	Control
	49-64	Value

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

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

19.2 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

19.3 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

19.4 SNMP Granular Trap Packets

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

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 ENV) **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 ENV 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

Frequently Asked Questions

20 Frequently Asked Questions

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

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

20.1 General FAQs

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

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

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

20.2 SNMP FAQs

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

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

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

21 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.*

22 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.

- A -

- C -

- D -

- F -

- I -

- L -

- M -

- N -

- O -

- P -

- R -

- S -

- T -