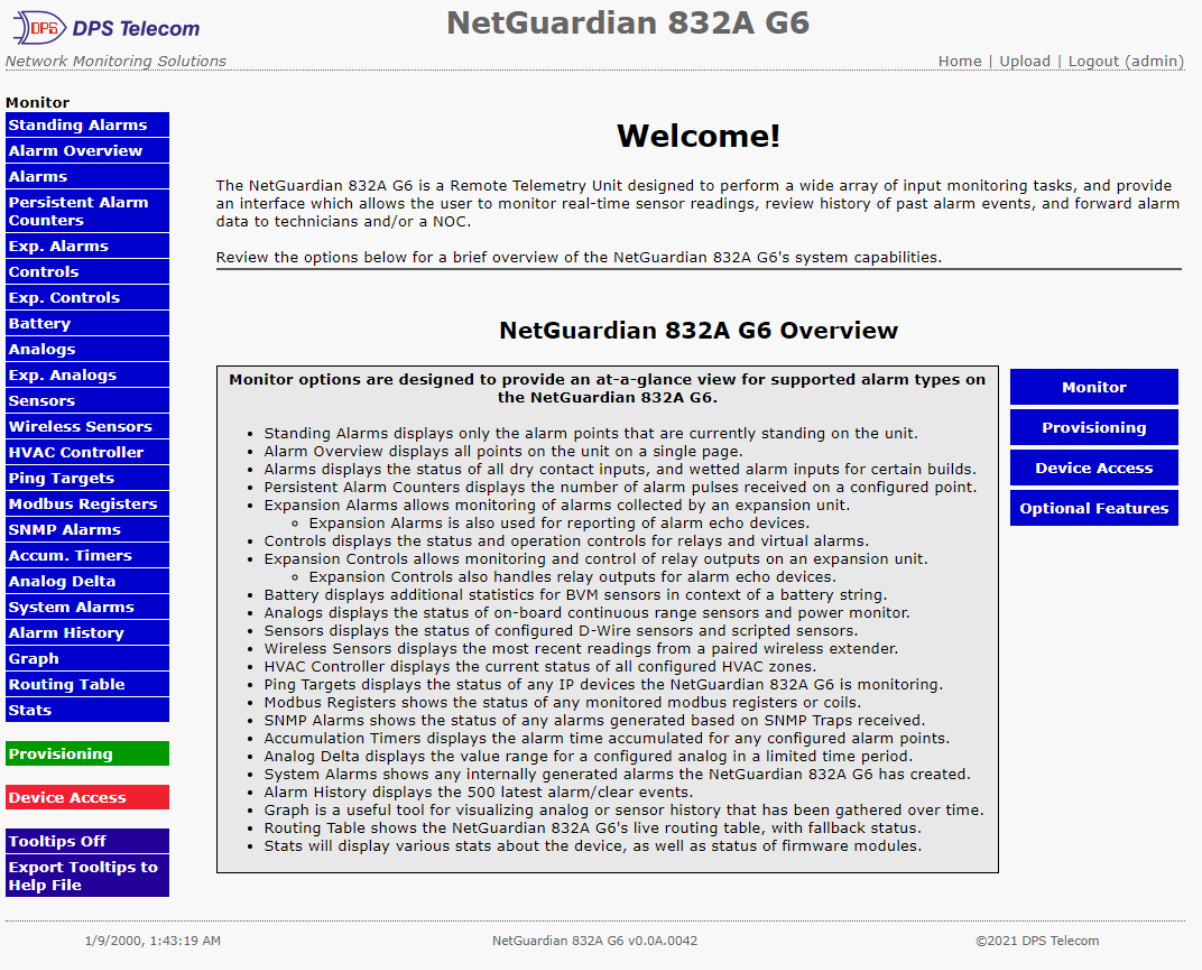
DPS Telecom
"Your Partners in Network Alarm Monitoring"

NetGuardian G6 832A/864A Web Browser

USER MANUAL



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

November 17, 2021 **D-UMW-NG832.6** **Firmware Version v.5.6D**

Revision History

November 24, 2021 First Edition

Notice

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

Contents

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

1 Overview

NetGuardian 832A G6 monitors alarms, pings network elements, and reports via SNMP or email.

1.1 Introduction

The NetGuardian's Web Browser Interface lets you manage alarms and configure the unit through the Internet or your Intranet. You can quickly set up alarm point descriptions, view alarm status, issue controls, and configure paging information, and more. The NetGuardian supports nearly all latest versions of any web browser you choose.

NetGuardian 832A G6 can monitor both legacy and contemporary devices via traditional contact closures and analog voltages/currents, IP-based protocols (ex. MODBUS). Once collected, alarms can trigger email or SMS-via-email notifications, SNMP traps, or reporting to a T/MON control alarm master.

1.2 What's New in NetGuardian G6

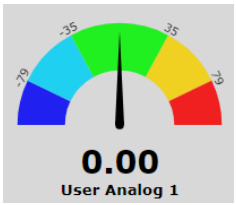
The NetGuardian 832A G6 has many new features above and beyond our preceding RTUs, some which are highlighted here:

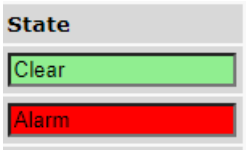
The new G6 includes many enhancements over previous models:

- Elimination of web page loading: The web interface will now load only once when you first access it. Once the page is loaded, alarm data updates several times per second, so there's no waiting to see alarm status or for a long page to reload. This provides a superior experience when monitoring the G6 from its built-in web interface.
- Much larger capacity for recording event history and analog sensor readings: Earlier models were limited to only 100 alarm events, intended only as a small buffer to protect against momentary losses of connectivity back to the central alarm master. The G6 now has enough storage to be a viable standalone monitoring system in all but the busiest environments.
- Analog gauges for fast visual review of important levels: For several years, small and medium NetGuardian models have included animated analog gauges. This feature is now incorporated in the flagship 832A model of the NetGuardian.

The G6 maintains fundamental long-term features of the NetGuardian RTU line:

- Expansion Alarms offer the ability to monitor and control via an expansion shelf.
- SNMP Alarms show the statuses of any alarms generated based on SNMP traps received.
- System Alarms show any internally generated alarms the NetGuardian 832A G6 has created (ex. "SNMP trap failed to send!").
- Routing Table shows the NetGuardian 832A G6's live routing table, with fallback status.
- Alarm lists and color-coded status indicators give you the ability to quickly see alarm states and status levels of your connected devices and/or sensors.





The green "Edit" menu is now "Provisioning":

- User Profiles are now used to configure passwords and access permissions for users who access the NetGuardian 832A G6.
- The Ethernet section provides options for configuring network interfaces, including static routes.
- SNMP is used to designate options for the NetGuardian 832A G6's SNMP agent (including SNMPv3 users & authentication/privacy)

2 Shipping List

While unpacking the NetGuardian, please make sure that all of the following items are included. If some parts are missing, or if you ever need to order new parts, please refer to the part numbers listed and call DPS Telecom at **(800) 622-3314**.

NetGuardian 832A G6: D-PK-NG832-6...
NetGuardian 864A G5: D-PK-NG864-6...

NetGuardian G6 Resource CD
(includes manual, MIBs, and software)

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

Two Ethernet Cables 14 ft.
D-PR-923-10B-14

Telephone Cable 6 ft.
D-PR-045-10A-01

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

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

Eight 3/8" Ear Screws (F)
2-000-60375-05

Four Standard Rack Screws (H)
1-000-12500-06

Four Metric Rack Screws (G)
2-000-80750-03

Three 3/4-Amp GMT Fuses (B)
2-741-00750-00

Two Large Power Connector Plugs for Main Power (C)
2-820-00862-02

Four Cable Ties
(Sixteen with hinged panel)

4 Pin Analog Connector (D)
2-820-00814-02

Pads (E)
2-015-00030-00

A B C D E F G H

Optional

Screws and connectors are packaged in a sealed hardware kit, shown above

(Hardware kit containing a WAGO connector)

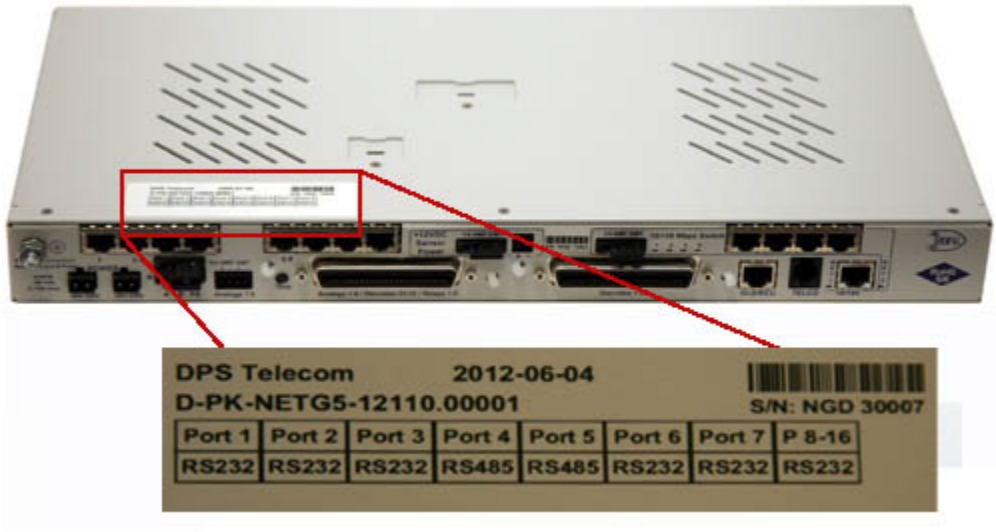
Optional Items

Two 3/4-Amp GMT Accessory Fuses (A)
2-741-00250-00

One Small Connector for Sensor Output
2-820-00812-02

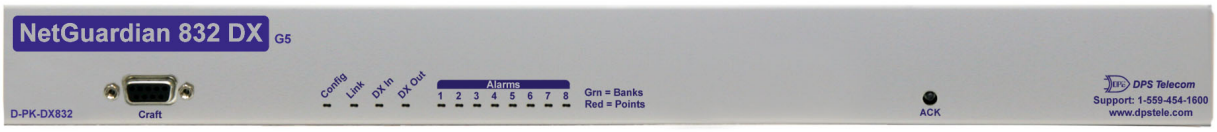
2.1 Port Allocation

Located on the top of the unit in the back left corner is the Port Allocation Sticker. This sticker includes your part number (D-PK-NETG5-#####.#####), which specifies your build option. The table below it lists your port allocation. This label displays serial electrical information about each of the ports, for example if the port hardware is configured for RS232, RS485, 202, etc.

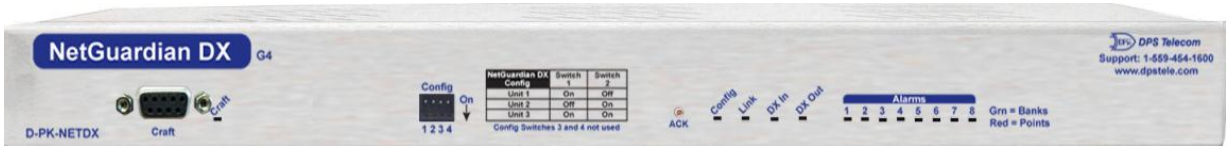


2.2 Optional Accessories

You can extend the capabilities of the NetGuardian through accessory units that provide greater discrete alarm capacity, remote audiovisual alarm notification, visual surveillance of remote sites, and other options. If you would like to order any of these accessories, or if you would like more information about them, call DPS Telecom at **(800) 622-3314**.



NetGuardian Expansion (NetGuardian 832A/864A DX G5)
D-PK-DX832/D-PK-DX864
The NetGuardian G5 expansions provide and additional 32 alarms for your NetGuardian 832A model or 64 points for your 864A, providing a total of 128 or 256 alarms with 3 expansion units. Each expansion comes standard with an additional 8 control relays and 8 analog inputs, and is available with an optional 8 port hub. (Optional builds are also available without controls, analogs, or both.)



NetGuardian Expansion (NetGuardian DX G4)
D-PK-NETDX-12022.00001
The NetGuardian Expansion G4 provides an additional 48 discrete and 8 relay controls. Up to three NetGuardian Expansions can be daisy-chained off one NetGuardian, providing a total of 176 discrete and 32 analog alarm points.

NetGuardian Expansion
The NetGuardian 480 (NG480) Expansion provides an additional 80 alarms and 4 relays. With 80 discrete alarm inputs, you can easily forward all the alarms of a small to medium-sized site.

NetGuardian E16
D-PK-DXE16
Adding the NetGuardian E16 provides an additional 16 alarm points and 16 controls. One NetGuardian E16 unit may be used per NetGuardian 832A/864A G5 remote. In this configuration, the E16 must be the last unit in the chain. Having only 1 serial port, it cannot forward traffic to a subsequent RTU.

General LCD Display (GLD)
D-PK-GLDRJ-12001.00001

The General LCD Display (GLD) is a small wall-mounted remote terminal for the NetGuardian. The LCD display shows system status and alarm messages, and the built-in speaker gives an audible notice of alarms. Up to 12 GLDs can be daisy-chained off the NetGuardian.

Hinged Wire-Wrap Back Panel

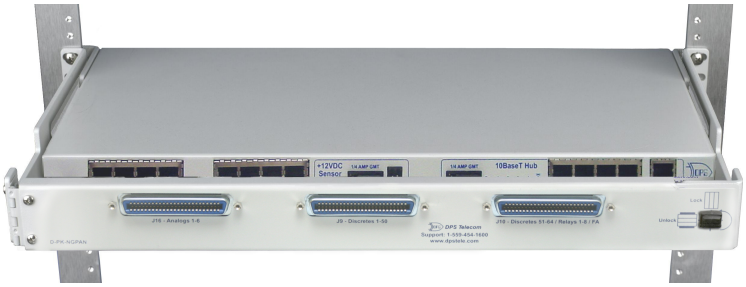
For 19" rack: D-PK-NGPAN-12002 **For 23" rack: D-PK-NGPAN-12006**

The hinged wire-wrap back panel provides wire-wrap connections for the NetGuardian's alarms and control relays.

Pluggable Barrier Panel

For 19" rack: D-PK-NGPAN-12021 **For 23" rack: D-PK-NGPAN-12007**

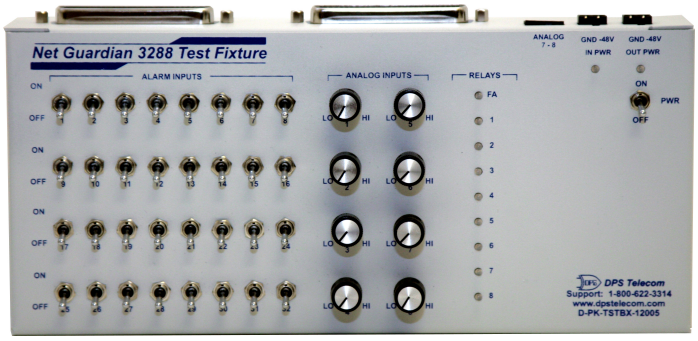
The pluggable barrier panel provides screw-lug barrier plug connections for the NetGuardian's alarms and control relays.



Hinged Amphenol Back Panel

For 19" rack: D-PK-NGPAN-12027 **For a KDA864 GOB option**
D-PK-NGPAN-12047 **For a KDA 864 with GOB-L option**

The Hinged Amphenol Back Panel easily allows for Upgrades from a KDA864 to a NetGuardian 864.



NetGuardian 3288 Test Fixture

D-PK-TSTBX-12005.00001

Every DPS product is rigorously tested before shipping, and the NetGuardian Test Box allows technicians to verify every discrete alarm input, control relay, and voltage-based analog alarm input on a NetGuardian G5. This time-tested tool is now available to you as the NetGuardian 3288 Test Fixture (known casually as the "NetGuardian Test Box"). With 32 discrete alarm toggles, 8 analog knobs, and 8 control relay LEDs, you can verify every alarm input and control output on your NetGuardians in a controlled way.

2.3 Specifications

Discrete Alarm Inputs:	32 (expandable to 80, 128, or 176 in 832A model) 64 (expandable to 112, 160, or 208 in 864A model)
Analog Alarms:	8
Analog Input Range:	(–94 to 94 VDC or 4 to 20 mA)
Analog Accuracy:	+/- 1% of Analog Range (See **Analog Step Sizes**)
Control Relays:	8 Form C (expandable to 16, 24, 32)
Maximum Voltage:	110 VDC/125 VAC
Maximum Current:	0.3 Amp at 125VAC, 1A at 30VDC
Ping Alarms:	32
Protocols:	SNMPv1, SNMPv2c, SNMPv3, DCPx, DCPf, TRIP, SNPP SMTP, TAP, HTTP, FTP, TELNET, ICMP, RADIUS, SSH, HTTPS
Interfaces:	9 RJ45 10/100 full-duplex Ethernet ports (1 port tied internally to switch - if switch option is purchased 1 RJ11 telco jack 5 D-Wire Ports (4 Front, 1 Rear. Rear uses modem jack) 2 50-pin amphenol connectors (discretes, controls, and analogs) 1 4-pin screw connector (analogs) *With Fiber top-board build option:* 4 10/100/1000 copper Ethernet ports **AND** 2- 1000 Base-X SFP Fiber ports *With WAN top-board build option:1 Rj45 WAN port*
Physical Dimensions:	1.720"H x 17.026"W x 8.386"D (NetGuardian 832A) (11.250"D with hinged Wire Wrap Adapter) 1.720"H x 17.026"W x 9.636"D (NetGuardian 864A) (12.750"D with hinged Wire Wrap Adapter)
Weight:	6 lbs. 3 oz. (2.8 kg)
Mounting:	19" or 23" rack
Power Input	
Voltage Options Include:	–48 VDC nominal (–18 to –60 VDC) (Optional) –24 VDC nominal (–18 to –36 VDC) (Optional) –24 VDC nominal (–18 to –36 VDC) (Optional) +24VDC (+18 to +36 VDC) (Optional) +12VDC (+11 to +18 VDC)
Current Draw:	150 mA at 48 VDC (300 mA at 24 VDC)
GMT Fuse:	3/4 amp recommended

Sensor Power Output

Voltage Output Options:	+12 VDC +24 VDC
Output Current:	500 mA at +12, or 250mA at +24 VDC
Input Current Draw:	May increase by 150 mA at 48 VDC
GMT Fuse:	3/4 amp recommended
Visual Interface:	LCD display 19 RGB LEDs
Audible Notification:	Alarm speaker (with volume control)
Operating Temperature:	32° to 140° F (0° to 60° C)
Storage Temperature:	-22° to 176° F (-30° to 80° C)
Industrial Temperature Option:	-22° to 158° F (-30° to 70° C)
Operating Humidity:	0%–95% non-condensing
MTBF:	60 years
Windows Compatibility:	Windows 95, 98, NT, ME, XP, 2000, Vista, 7 32/64 bit, 8, 10, 11

***RoHS 5 Approved**

Note: 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.

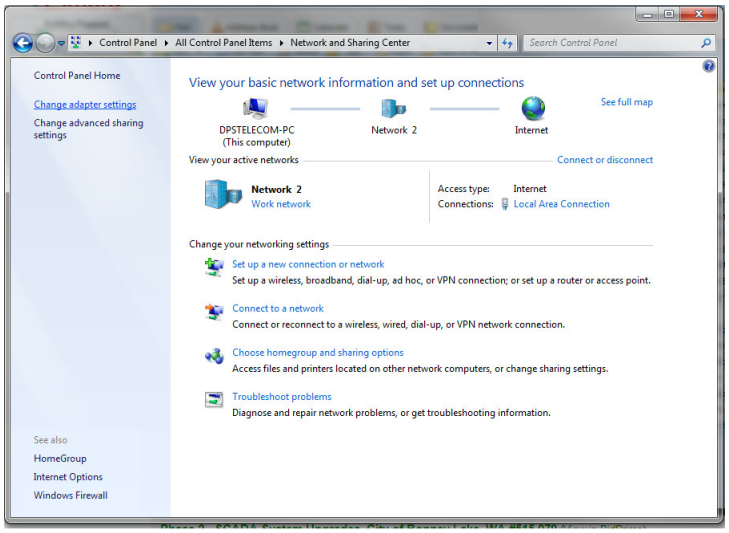
3 Connect to Network

This section provides step-by-step instructions on how to connect your NetGuardian 832A G6 Controller to your network.

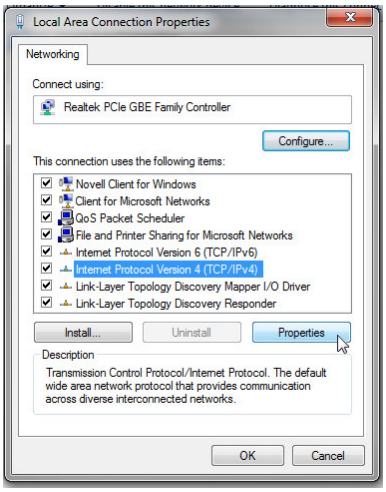
The following pictures and instructions depict either Windows 7 or Windows 10. Other operating systems will likely be similar.

3.1 Change Your PCs IP

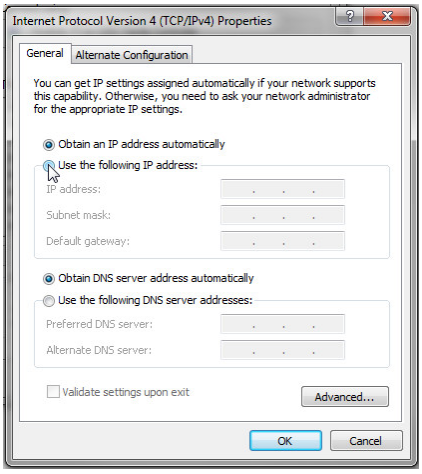
1. Plug LAN cable into PC.
2. Click **START**.
3. Select **CONTROL PANEL**.
4. Select **NETWORK AND INTERNET**.
5. Select **NETWORK AND SHARING CENTER**.
6. Click **CHANGE ADAPTER SETTINGS** in the left menu.



7. Find the appropriate adapter (most likely, this will not be a wireless connection).
8. Right-click the adapter.
9. Select **PROPERTIES** from the drop-down menu.
10. Click **INTERNET PROTOCOL VERSION 4** from the menu.



11. Click the **PROPERTIES** button.
12. Click the radio button for the option that states "Use the following IP address:"
    - If this button is already selected, record information before changing it so that you can set it back later.
    - If "Obtain an IP address automatically" is an option, you don't have to record the IP address information.

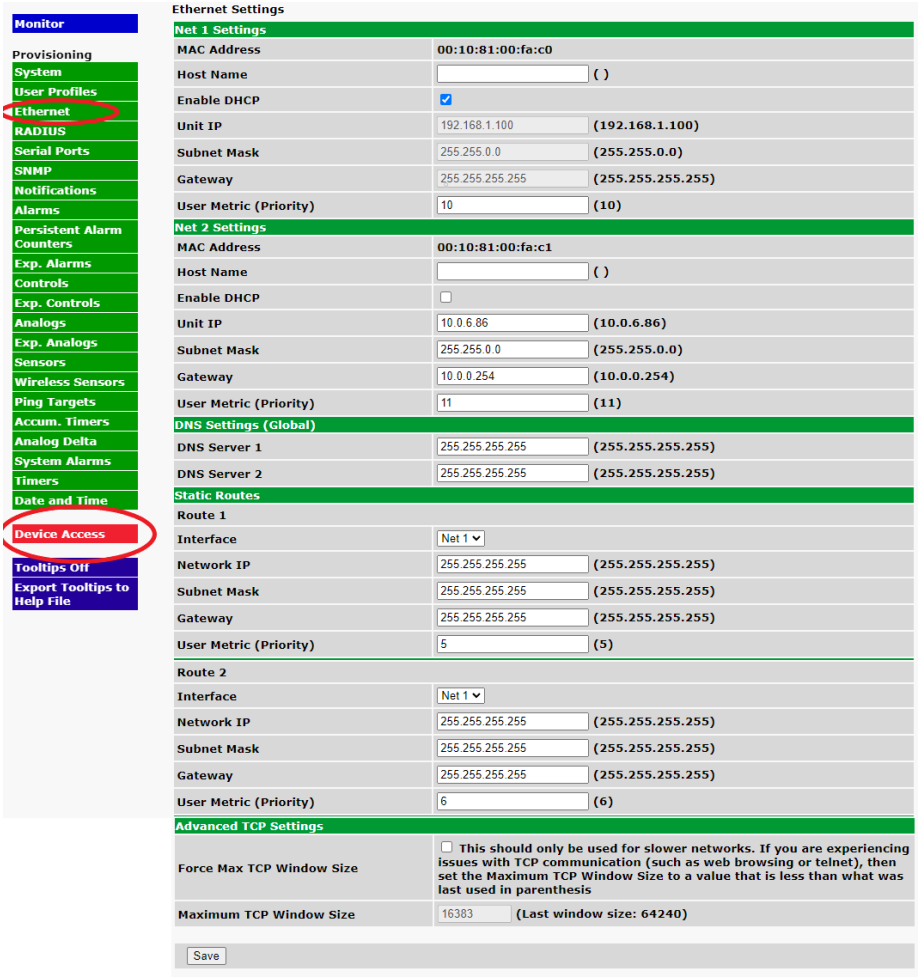


13. Enter in an IP address that is within your G6's Subnet (see defaults below). When installing a new G6 that has factory default settings, your PC's new IP should be 192.168.1.XXX (replace the XXX with any number from 1-255, excluding the IP used by the unit (see defaults below).
    - **Default G6 Controller IP (Net 1): 192.168.1.100**
    - **Default G6 Controller IP (Net 2): 192.168.1.101**
    - **Default G6 Controller Subnet Mask: 255.255.255.0**
14. Click *OK and close the window*.

3.2 Browse the Web Interface

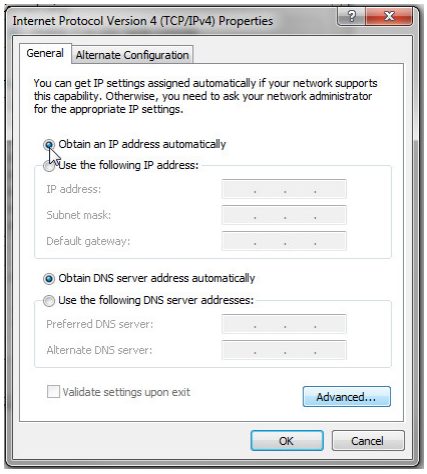
1. Using the web browser of your choice, browse to the G6's unit's IP address.
2. The login form should appear. Enter the admin login information provided below and click *Login*.
   - Username: admin
   - Password: dpstelecom

3. Expand the Provisioning menu.
4. Click **Ethernet**.
5. Change the G6's default IP address, subnet mask, and default gateway to be compatible with your network.
6. Click **Save** at the bottom of the page to cache your changes. To commit changes to the unit, click **Device Access** in red **o**n the bottom left, then **Write** *and* **Reboot**.



3.3 Restore and Connect

1. Return to the Internet Protocol Version 4 page on your PC.
2. Reset the IP address by typing in the numbers you recorded previously or by clicking the "Obtain an IP address automatically" button.



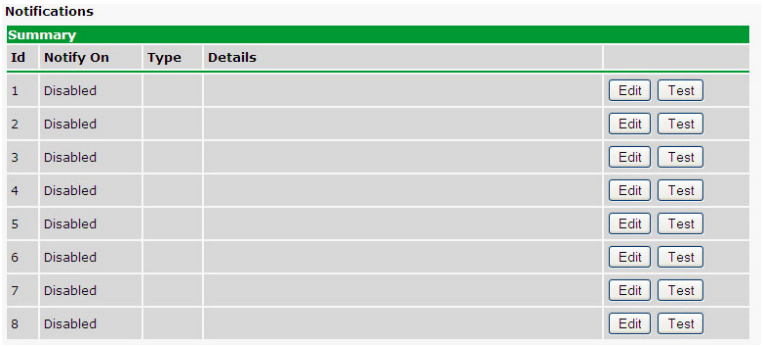
3. Click **OK**.
4. Log back onto the unit as described previously.
5. Click **Provisioning**.
6. On the System Settings screen, change your default user and password.
7. Save your changes.

4 Quick Turn Up

The next sections of this manual will walk you through some of the most common tasks for using the G6. 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.

4.1 How To Send Email Notifications

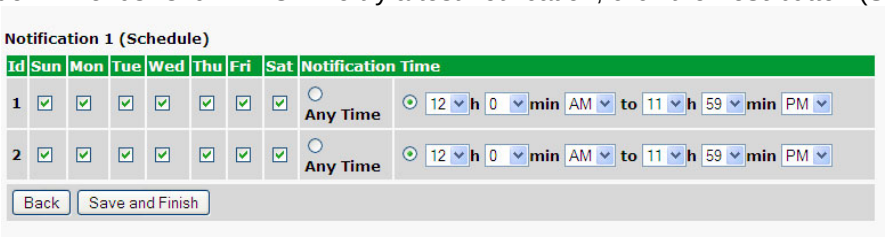
1. Click on the **Notifications** button in the **Provisioning** menu. You can setup as many as 8 different notifications. Begin the setup "wizard" by clicking **Edit** for a notification number. In this example, we'll setup Notification 1 to send emails.



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** 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. **NOTE:** if using Host Name, make sure that DNS Servers settings are configured. 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 two 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.)

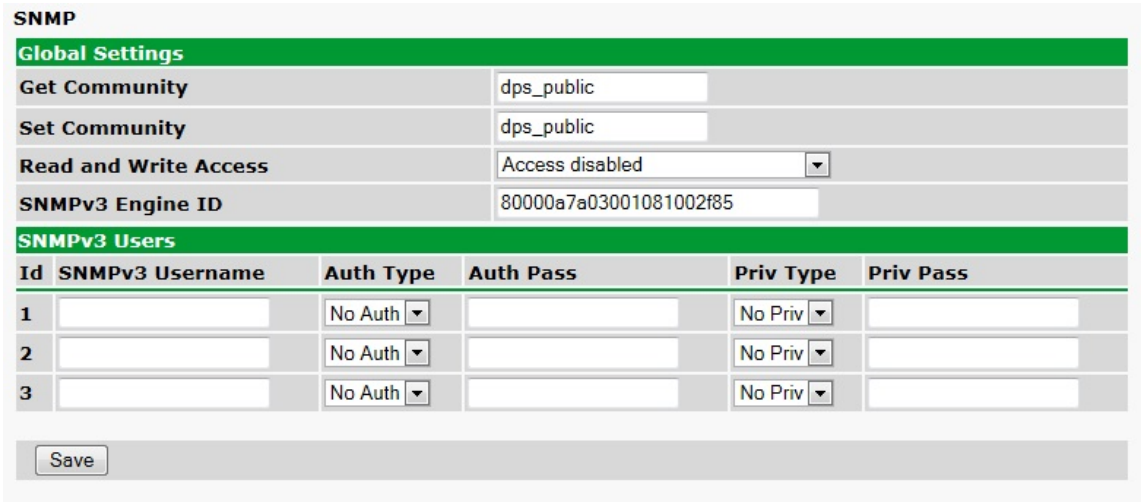


5. If you chose to test the email notification you've just setup, you will prompted with a pop up . Click **OK** to send a test email alarm notification. Confirm all your settings by checking your email to see if you've received it. **NOTE:** This test only means that your notification settings are correct,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

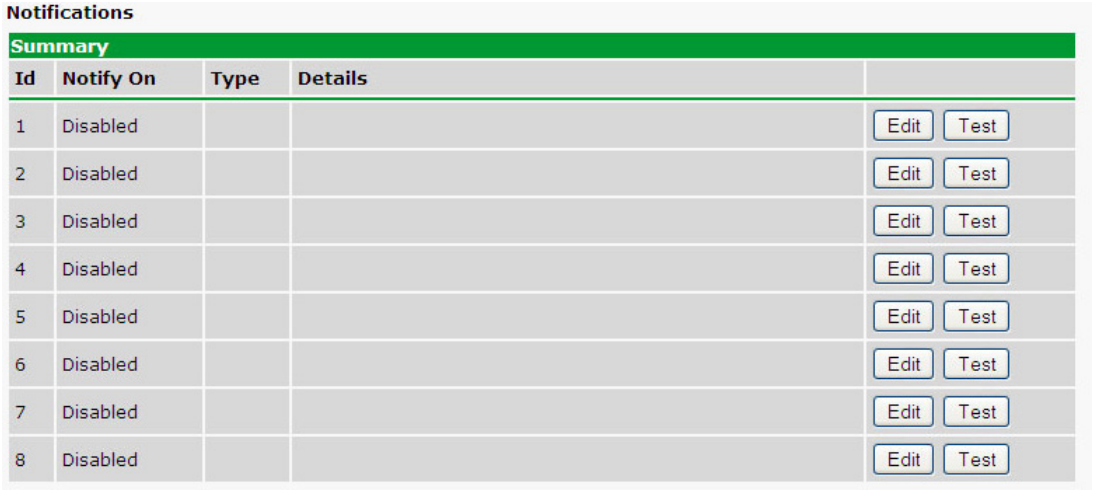
6. Now you will associate this notification to an alarm (system, base, analog, etc.) You have 8 notification devices available to use. Remember that Notification #1 in the Notifications menu corresponds to the first "Notifications" column of check boxes "N1". (Notification #2 "N2" is the second column, and so on until Notification #8 "N8")

4.2 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 **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**.

4. 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.)

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 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.

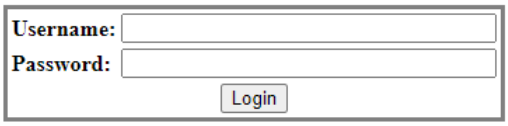
5 Logging on to the NetGuardian

For Web Interface functionality, the unit must first be configured with some basic network information. If this step has not been done, refer to the NetGuardian User Manual for initial software configuration setup.

1. To connect to the NetGuardian from your Web browser, you must know its IP address or domain name if it has been registered with your internal DNS. Enter it in the address bar of your Web browser. It may be helpful to bookmark the logon page to simplify access.

2. After connecting to the NetGuardian's IP address, enter your Username password and click the Login button, see image below.
   NOTE: The factory default username/password is **admin/dpstelecom.**

3. In the left frame there is **Monitoring** menu button, a **Provisioning** menu button and a **Device Access** menu button**.** Most of the software configuration will occur in the **Provisioning** menu. The following sections provide detailed information regarding these functions.



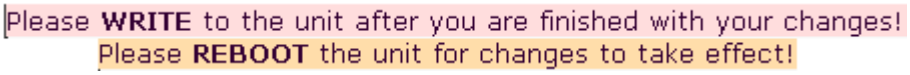
Enter your username/password to enter the NetGuardian Web Browser Interface.

6 Provisioning Menu Field Descriptions

G6 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 G6:
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.

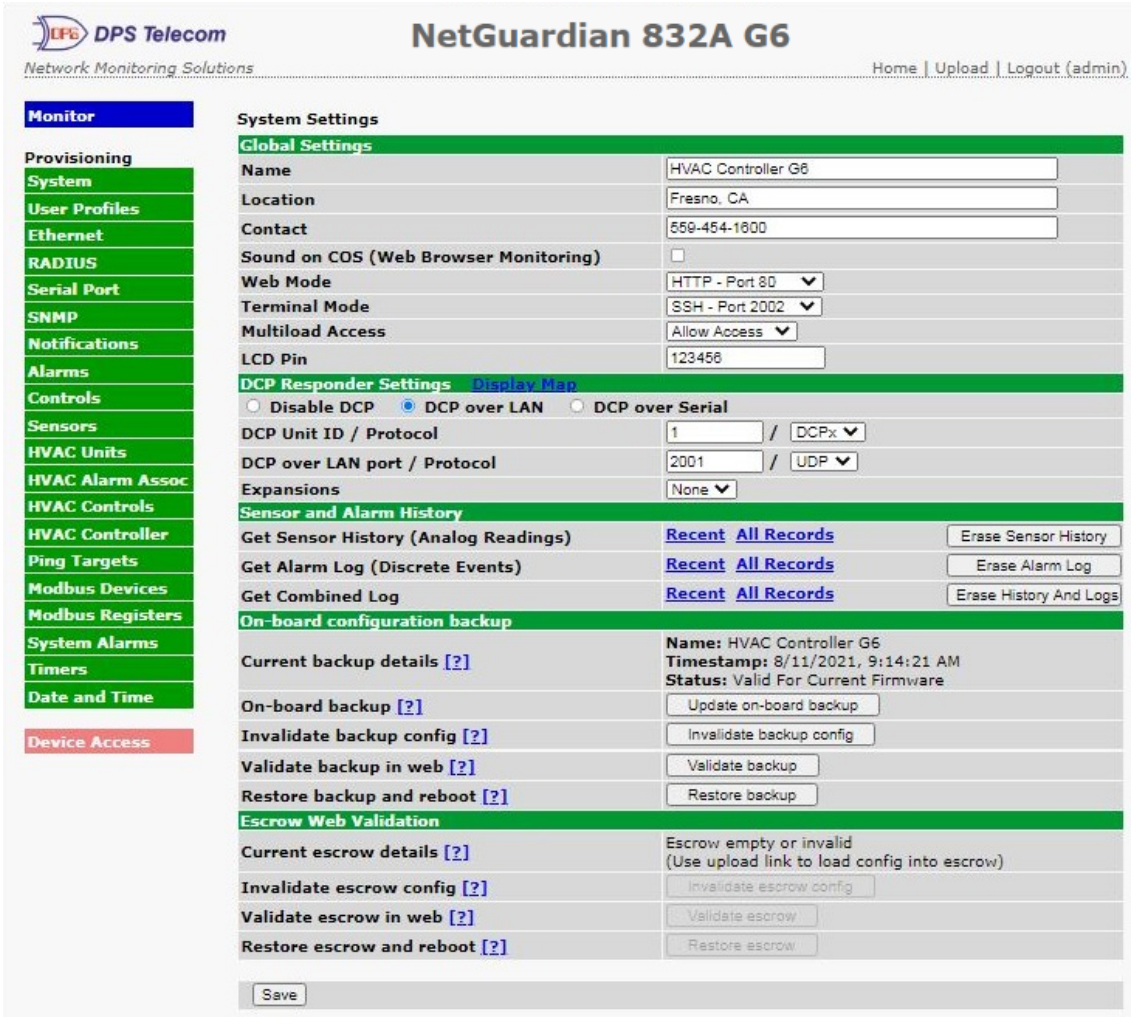


Status messages on the G6 Device Access menu, inform you how to implement your changes

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

6.1 System

From the **Provisioning** > **System** menu, you will configure and edit various global settings that apply widely. You can also save/erase logs and backup/restore device configurations.



The Provisioning > System menu

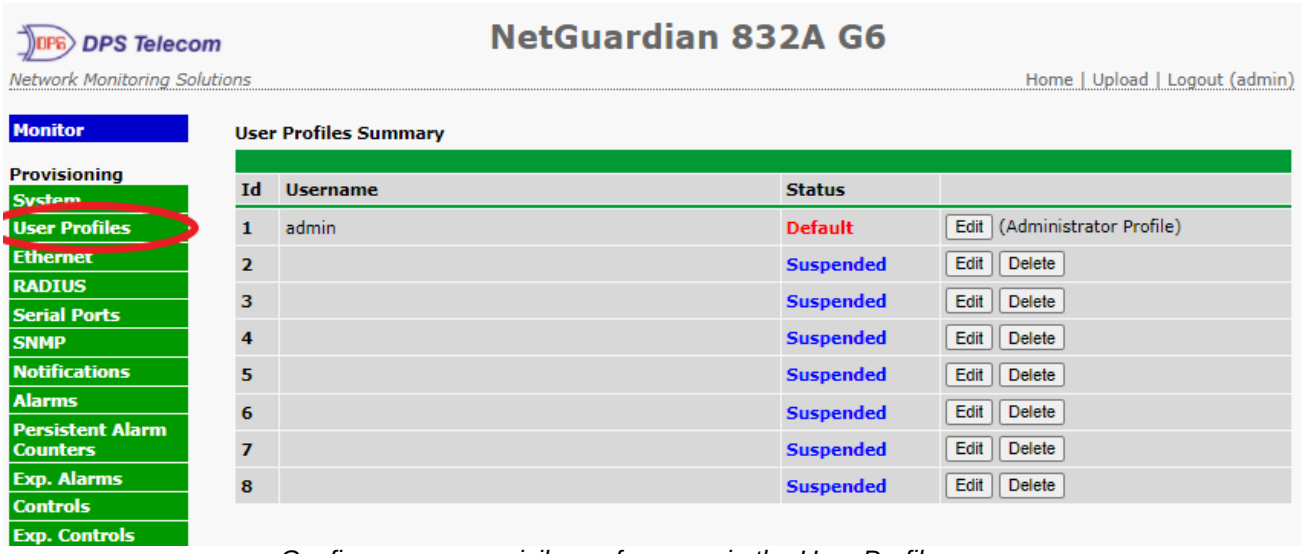
Global System Settings	
Name	A name for this unit. (Optional, useful for coordination & notifications)
Location	The location of this unit. (Optional, useful for coordination & notifications)
Contact	Contact telephone number for the person responsible for this unit. {Optional field)
Sound on COS	Checking this box enables Sound on COS when viewing the Alarms, Sensors, Ping Targets, or System Alarms page under the Monitor menu.
Web Mode	HTTP on port 80 or HTTPS on port 443. Changes will only go active after reboot. (Default HTTPS - Port 443)
Redirect HTTP to HTTPS	Only available when web mode is HTTPS - Port 443. When enabled, opens port 80 for sole purpose of redirecting to landing page of HTTPS server. When disabled, leaves port 80 closed and browsing to http://<ip address of unit> will yield a connection refused message. (Default = Enabled)
Terminal Mode	Telnet on port 2002 or SSH on port 2002. (Default - Telnet on port 2002).
Multiload Access	"Allow Access" or "Require Login". When set to "Allow Access", unit will allow direct navigation to the Upload page (for updating firmware, web image, or config) without needing to authorize for user access. This can help with recovery of unit, but may not be desired in secure deployments.
LCD PIN	Passcode used to unlock Device Setup on the Touchscreen (Default: 123456)

DCP Responder Settings *(For use with T/Mon)*	
Disable DCP, DCP over LAN / Serial	Select one of these 3 options to send DCP protocol over LAN, serial, or disable DCP completely.
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.
Expansions	Select the number of expansion units connected to the unit.
Sensor and Alarm History	
Get Sensor History	Download a log of all configured analog and sensor values. Also, "Erase" button to clear the history.
Get Alarm Log	Download a log of the device's recent alarm history. Also, "Erase" button to clear the log.
On-board Configuration Backup	
Current backup details	If backup has been created, displays the Name, Timestamp, and Status of the on-board backup. • Name: System Name of the stored backup configuration. • Timestamp: Unit time when backup configuration was created. Note that this time may be before the time when the on-board backup was last updated, particularly in cases where the configuration had been live for some time before later updating the on-board backup. • Status: Indicates whether backup configuration is valid for current firmware, or gives additional instruction when the backup is not valid for current firmware. Usual causes of an invalid backup result from a firmware version change without subsequently updating the on-board backup.
On-board backup	Creates a backup of the current written and active configuration.
Invalidate backup config	Erases the saved backup configuration from the unit.
Validate backup in web	Exercises a "Device Access > Read" operation, except that the unit will read in the values from the backup configuration rather than the active configuration. The values read into the web interface can be validated in the edit interface and written back to the unit as an active configuration. When doing this, the current local user profiles will be applied to the backup configuration instead of restoring the backup configuration's local user profiles.
Restore backup and reboot	Reboots the unit and restores the onboard backup configuration - rather than the active configuration. This will restore the local user profiles from the backup configuration.

Escrow Web Validation	
Current escrow details	On power up, will show escrow empty or invalid. By using the multiload interface, a backup configuration (previously downloaded from "Device Access > Backup Config") can be uploaded to the escrow location for web validation before going active. When a config has been uploaded to escrow, this will show the Name, Timestamp, and Status, similar to the on-board configuration above.
Invalidate escrow config	Explicitly erases the escrow configuration from the unit. **NOTE:** Uploading a new configuration will overwrite the previous escrow configuration. **NOTE:** Rebooting the unit without restoring a configuration from escrow will erase the escrow configuration.
Validate escrow in web	Exercises a "Device Access > Read" operation, except will read in the values from the escrow configuration rather than the active configuration. Works similarly to on-board configuration backup validation.
Restore escrow and reboot	Reboots the unit with a message to the bootloader that it should attempt to boot using the escrow configuration rather than the active configuration. This will restore the local user profiles from the escrow configuration.

6.2 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's web interface.



Configure access privileges for users in the User Profile screen

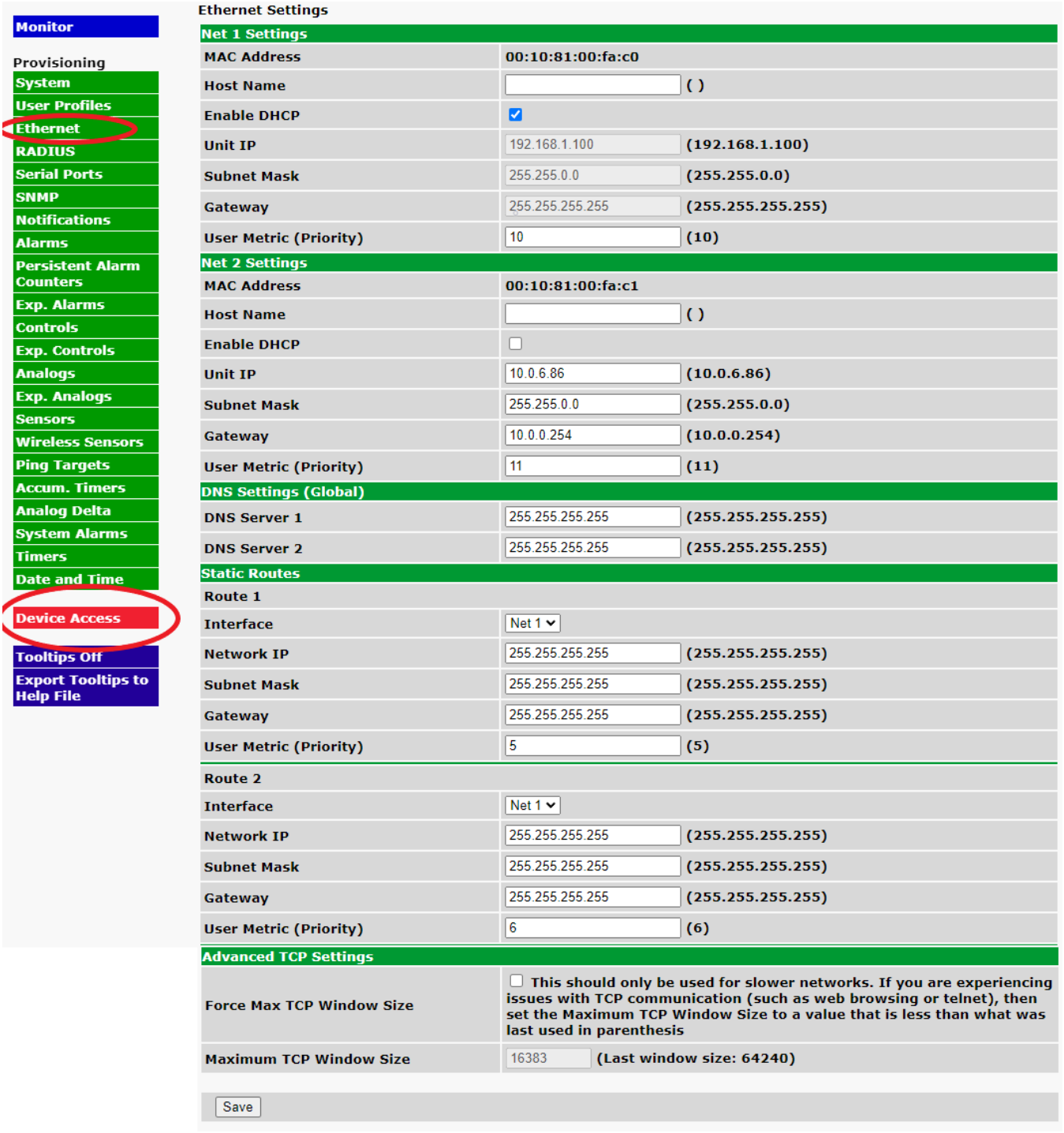
To create or edit any of the 8 user profiles (including the Admin), click the **Edit** button. From there, you can change all configurable settings for a user profile.

	User Profile
Suspend this Profile	If this box is checked, the profile will not be able to access the unit.
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 unit 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

6.3 Ethernet

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



The Provisioning > Ethernet menu

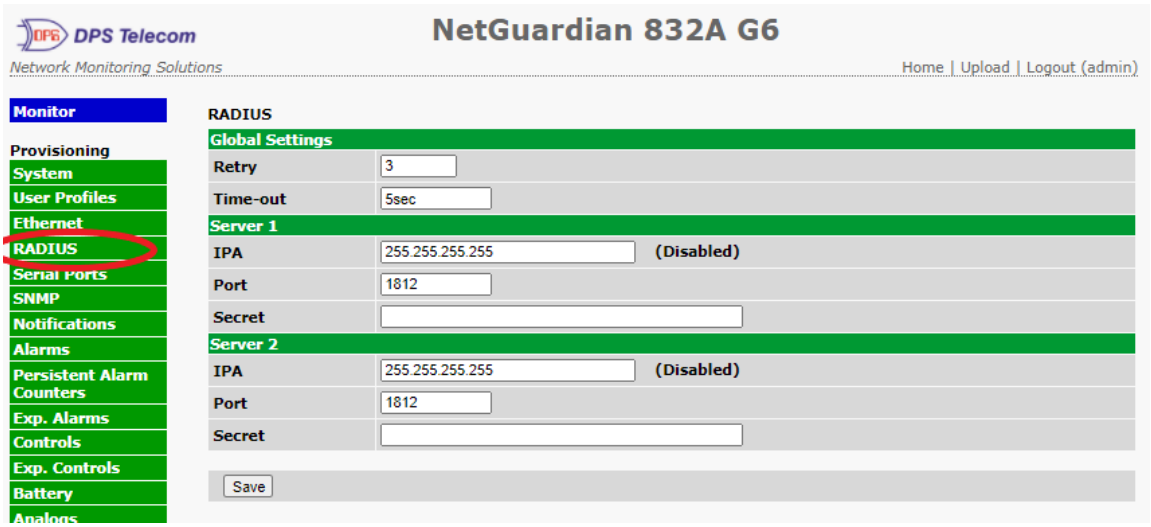
Ethernet Settings (Many are separate for Net 1 & Net 2)	
MAC Address	Hardware address of the NetGuardian. (Not editable - For reference only.)
Host Name	Used only for web browsing. Example: If you don't want to remember this NetGuardian's IP address, you can type in a name is this field, such as "MyNetGuardian". Once you save and reboot the unit, you can now browse to it locally by simply typing in "MyNetGuardian" in the address bar. (no "http://" needed).
Enable DHCP	Used to turn on Dynamic Host Connection Protocol. NOT recommended, because the unit is assigned an IP address from your DHCP server. The IP you've already assigned to the unit becomes inactive. Using DHCP means the unit will NOT operate in a T/Mon environment.
Unit IP	IP address of the NetGuardian.
Subnet Mask	A road sign to the NetGuardian, 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 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.
User Metric (Priority)	Used to prioritize one network over another (Net 1 vs. Net 2) when making an outbound connection. The network gateway with the lower metric is the default gateway; the network gateway with the higher metric is a fallback gateway.
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.
[Static Routes]	Options for creating a static route to a designated subnet through a specified gateway. The "User Metric (Priority)" is used for prioritization similar to network behavior; any matching static routes with a lower metric will be attempted before those with higher metrics.

Advanced TCP Settings	
Force Max TCP Window Size	The defined TCP window size is used. (For low-bandwidth networks)
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.

6.4 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 G6 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. You can access the RADIUS page by clicking on **Provisioning** menu > **RADIUS** link. See image below.



Provisioning > RADIUS

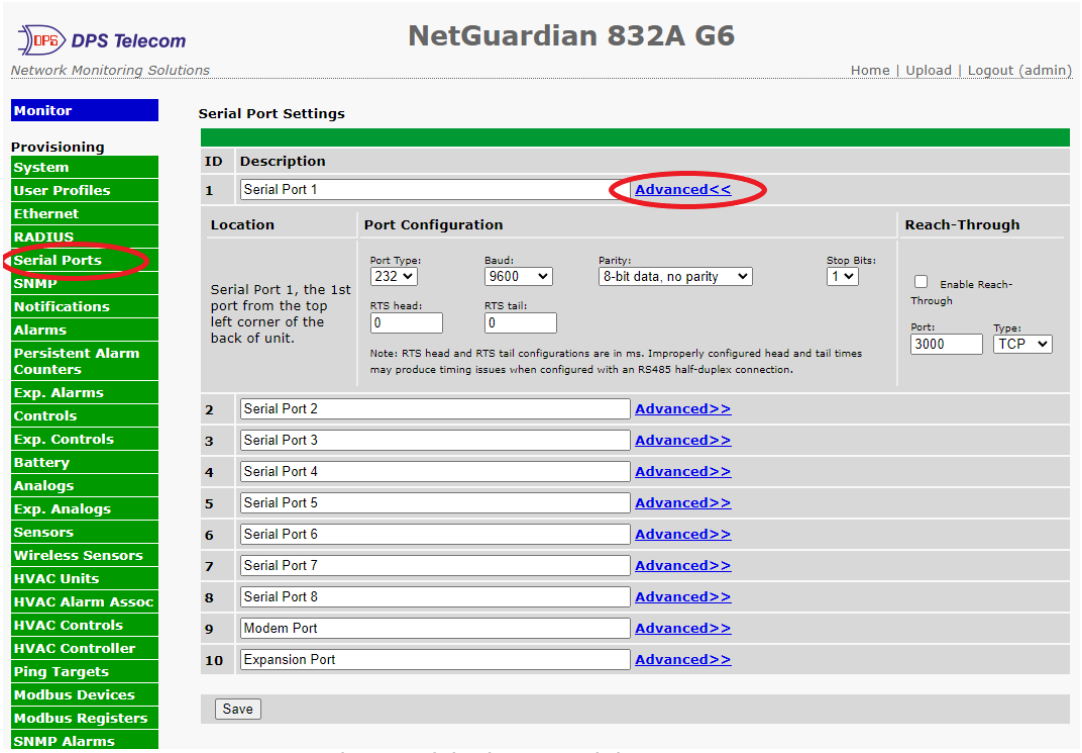
Global Settings	
Retry	Enter the number of times the RADIUS server should retry a logon attempt
Time-out	Enter in the number of seconds before a logon request is timed out
Server 1 & Server 2	
IPA	Enter the IP address of the RADIUS server
Port	Port 1812 is an industry-standard port for using RADIUS
Secret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

After successfully entering the settings for the RADIUS server, the G6 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 G6, the local authentication will not be valid.

6.5 Serial Ports

The **Provisioning > Serial Port** menu allows you to change settings depending on the port type of your G6. From this menu, you can select a mode of operation and enable reach-through serial port functionality.

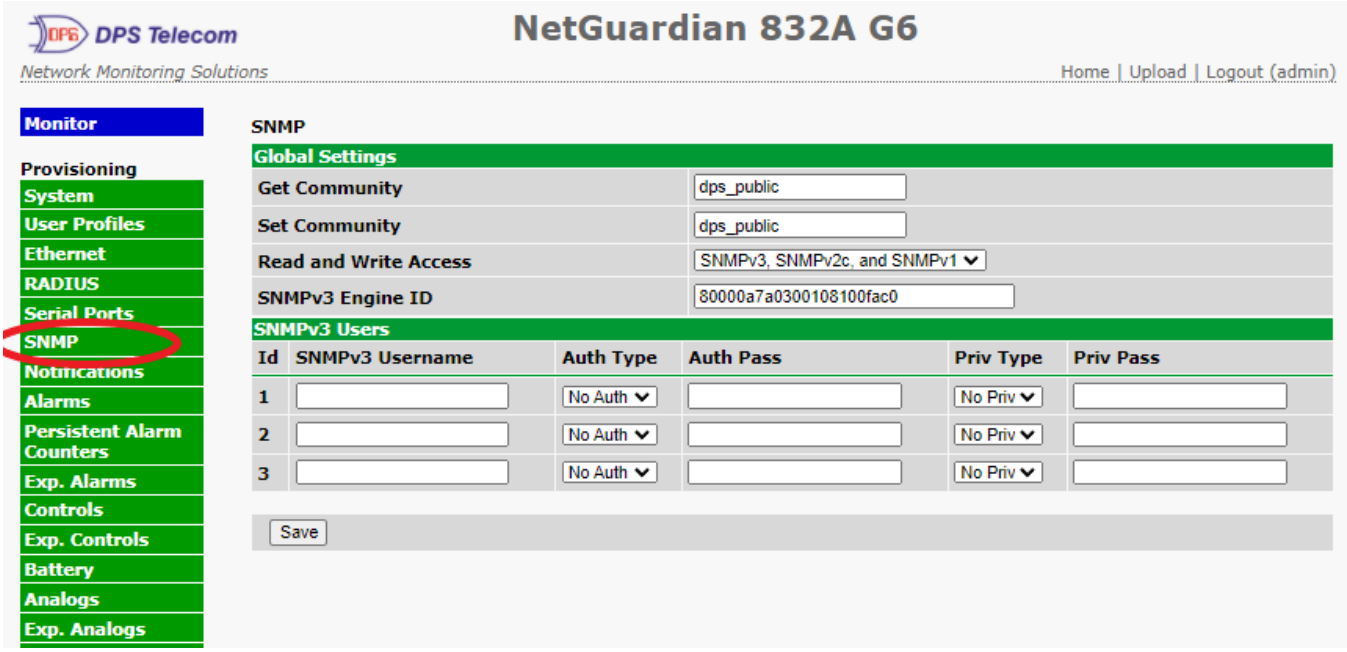


The Provisioning > Serial Ports menu

Location	
Reminder that the primary serial port is located on the back of the unit chassis.	
Port Configuration	
Port Type	Select the serial port for your build of the unit. Choose from 232, 485...
Baud, Parity, and Stop Bits	Select the appropriate settings from the drop-down menu.
RTS Head	Useful for RS485 serial connections, and especially necessary when configuring 485 half-duplex.
RTS Tail	Useful for RS485 serial connections, and especially necessary when configuring 485 half-duplex.
Reach-Through	
Enable Reach-through	Checking this box enables the port to be used as a terminal server. Most commonly used to Telnet through the port over LAN to a hub, switch, or router. From a command prompt, type the following *(note the spaces between each entry)*: telnet [IP address] [port] **Example**: telnet 192.168.1.100 3000
Port	Port number used for reach-through to a serial device.
Type	Select TCP or UDP traffic to be passed through to a serial device. Can also be set to "proxy" for establishing proxy reach-through from a TTY interface.

6.6 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 G6 may be accessed via SNMP. This can be set to the following: • Access Disabled- Restricts all access to unit via SNMP • SNMPv2c only- Allows SNMPv2c access only • SNMPv2c and SNMPv1-Only- Allows SNMPv1 and SNMPv2c access • SNMPv3, SNMPv2c and SNMPv1- Allows SNMPv3, SNMPv2c and SNMPv1 access

Fields in the Provisioning > SNMP settings

6.7 Notifications

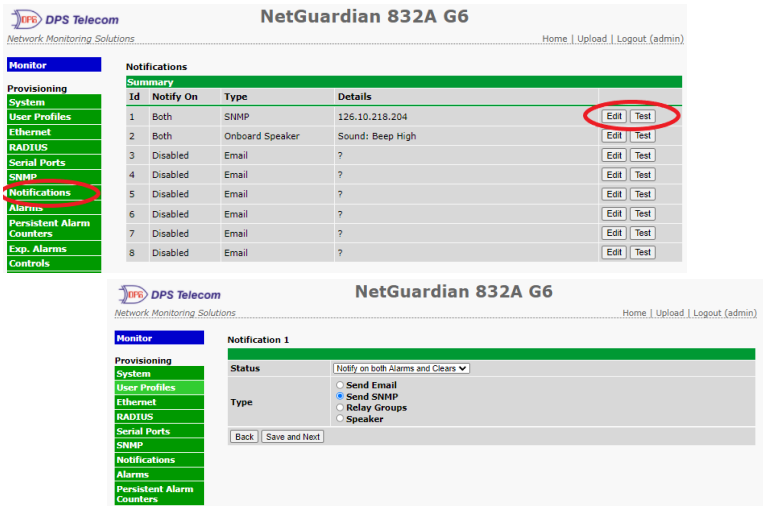
From the initial **Provisioning** > **Notifications** menu, you will see which of the notifications are enabled, their type, and details. Click on the **Edit** link for one of the notifications to begin configuration. Once you have entered the **Edit** menu you will be given the option to set the status type of alarms which will trigger a notification. Entering the status drop down box offers you the following options:

1. Notification disabled.
2. Notify on both alarms and clears.
3. Notify on alarms only.
4. Notify on clears only.

The NetGuardian 832A G6 offers 4 types of notifications. Select one of these options under the type section:

1. Send Email.
2. Send SNMP.
3. Relay Groups.
4. Speaker.

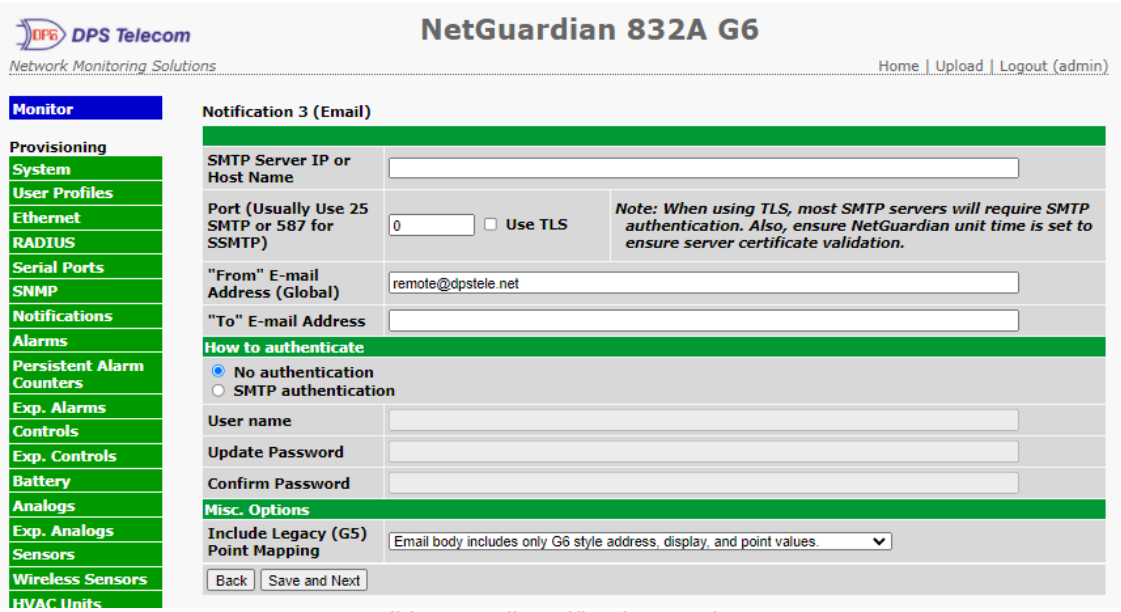
Once your options have been selected you must click the **Save and Next** button to proceed for further configuration. Clicking the back button will take you to the previous Notification page. Click the **TEST** link to initiate a test of the notification to ensure your configuration settings are valid.



Clicking the **Save and Next** button does not save your settings. You will be required to **Write** your settings to the device in order for you configurations to be saved. The NetGuardian 832A G6 will provide a prompt reminding you of this requirement. You will access the Write option via the **Device Access** > **Write** menu.

6.7.1 Notification Settings

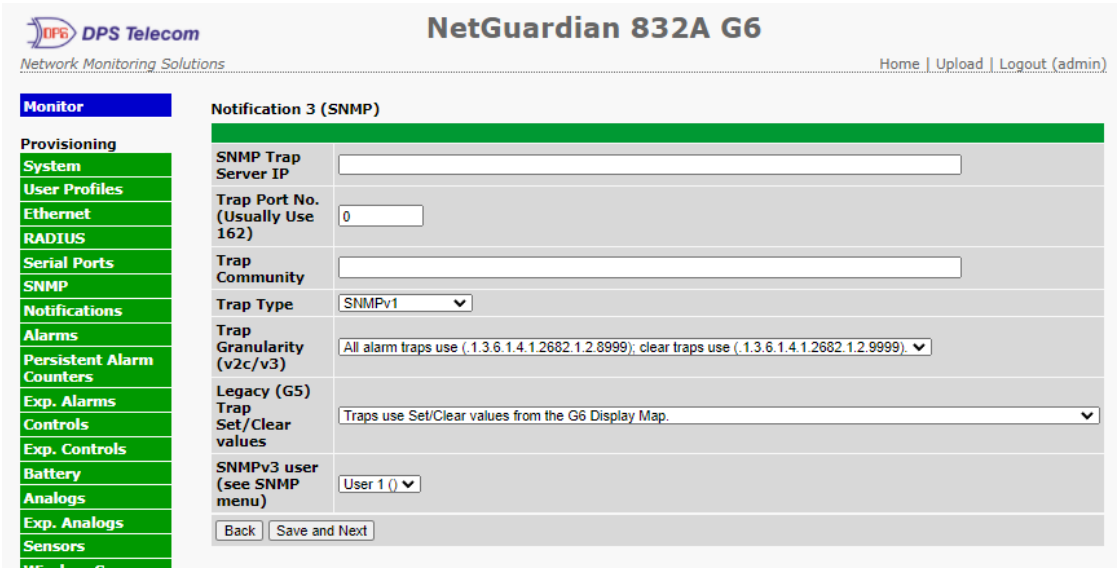
Email Notification Fields



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 TLS	Check this box to use TLS encryption. Currently, this feature has been tested with common email providers, like Gmail, Yahoo!, and others. As an example, to send via 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 587. • 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 will send emails from. Not editable from this screen. For interoperability with SMTP servers, this defaults to the authentication username.
"To" E-mail Address	The email address of the person responsible for this NetGuardian, who will receive email alarm notifications.
How to Authenticate	
User Name	Full email address for the account (such as Gmail) being used.
Password	Password will be updated if the "Update Password" and "Confirm Password" fields contain an identical new password. If these are blank, the password will not change. If the two fields do not contain the same new password, an alert message will appear when you attempt to save.

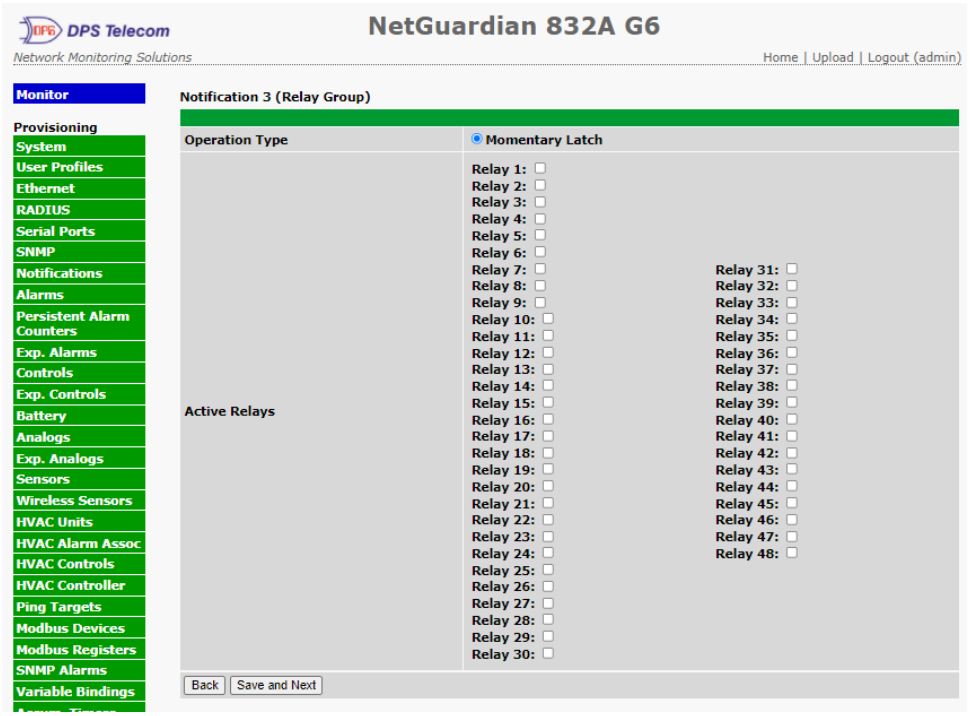
SNMP Notification Fields



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, v2c inform, or v3 traps.
Trap Granularity (v2c/v3)	Set whether traps generated by this notification type are sent with generic (*.8999 for sets, *.9999 for clears) OIDs, of if they are generated using granular OIDs designated in the G6 display mapping.
Legacy (G5) Trap Set/Clear Values	Set whether traps generated by this notification type are sent using G6 granular OIDs, or if they are sent using G5 granular OIDs. Note that the trap granularity setting takes priority over this field. Note also that generic trap OIDs (*.8999 for sets, *.9999 for clears) will be used in G5 mode when a trap cannot be uniquely mapped to a G5 granular OID.
SNMPv3 user (see SNMP menu)	When Trap Type v3 is selected, this determines the username, authentication, and privacy settings to be applied to the trap. These must be configured on the SNMP provisioning page.

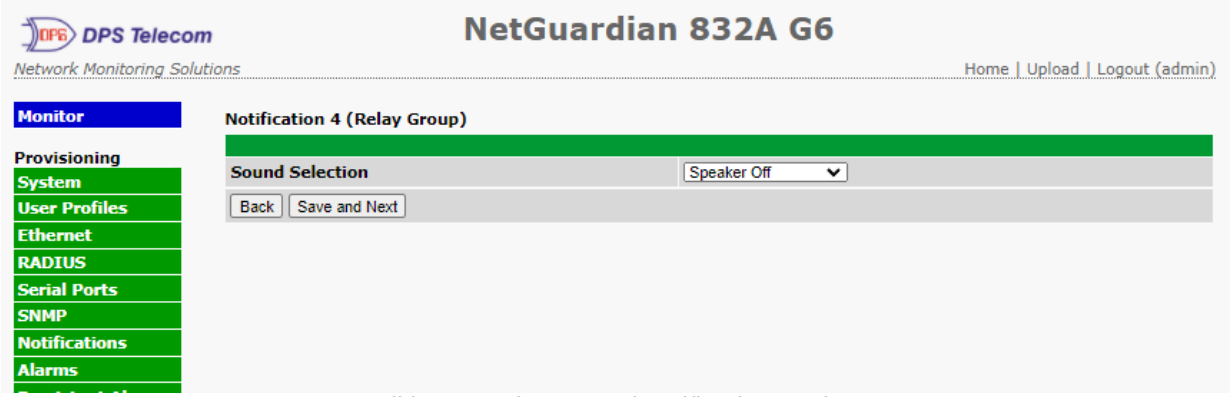
Relay Group Notification Fields



Editing Relay Group notification settings

SNMP Notification	
Operation Type	When a notification event occurs, selected active relays will momentarily latch for the momentary time configured on the controls provisioning page.
Active Relays	Momentary latch configured inside the control. Briefly latch and release a rely contact

Speaker Notification Fields



Editing Speaker Sound notification settings

SNMP Notification	
Sound Selection	Enter the drop box to select the type of sound alarm from the speaker. Select from the following: • Speaker Off • Speaker Tone • Speaker Siren • Speaker Beep Low • Speaker Beep High

6.7.2 Notification Schedule

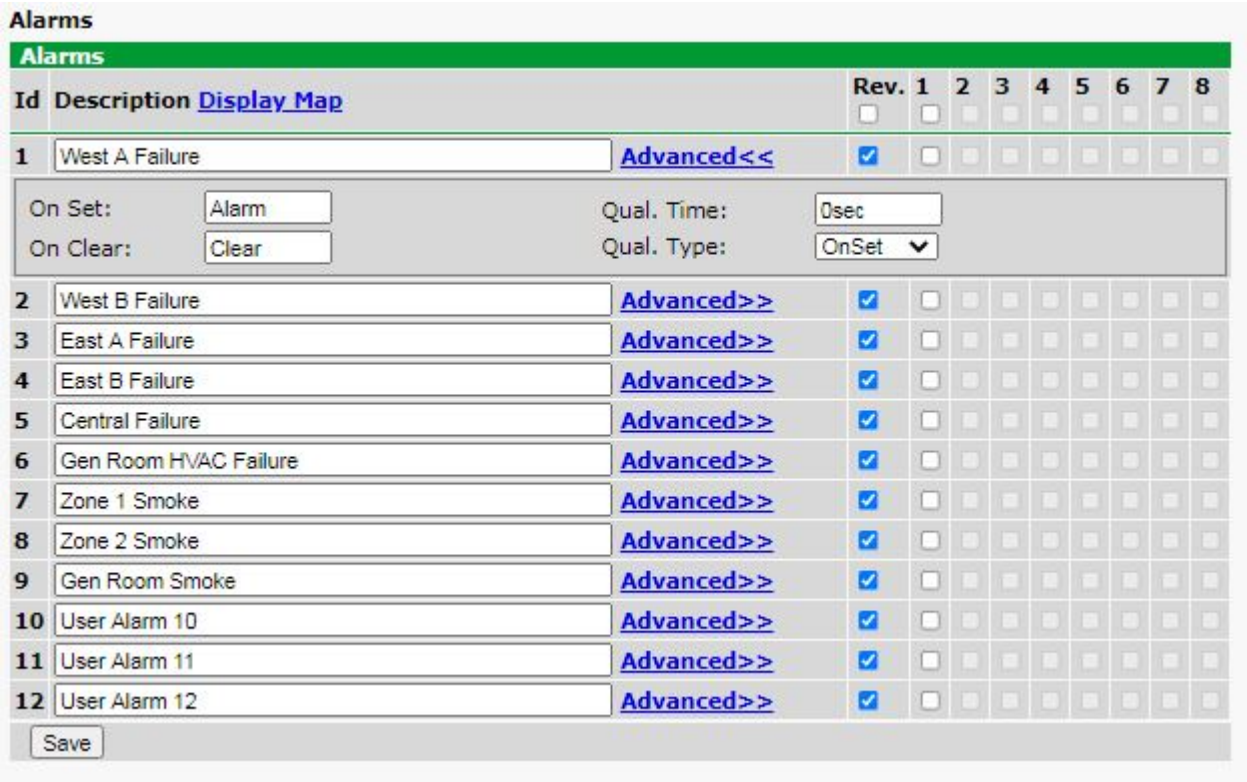
The notifications scheduling menu is where you will tell the G6 exactly which days and times you want to receive alarm notifications. You set 2 different schedules for each.

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.

6.8 Alarms

Discrete alarms are configured from the **Provisioning** > **Alarms** and **Provisioning > Exp. Alarms** menus.

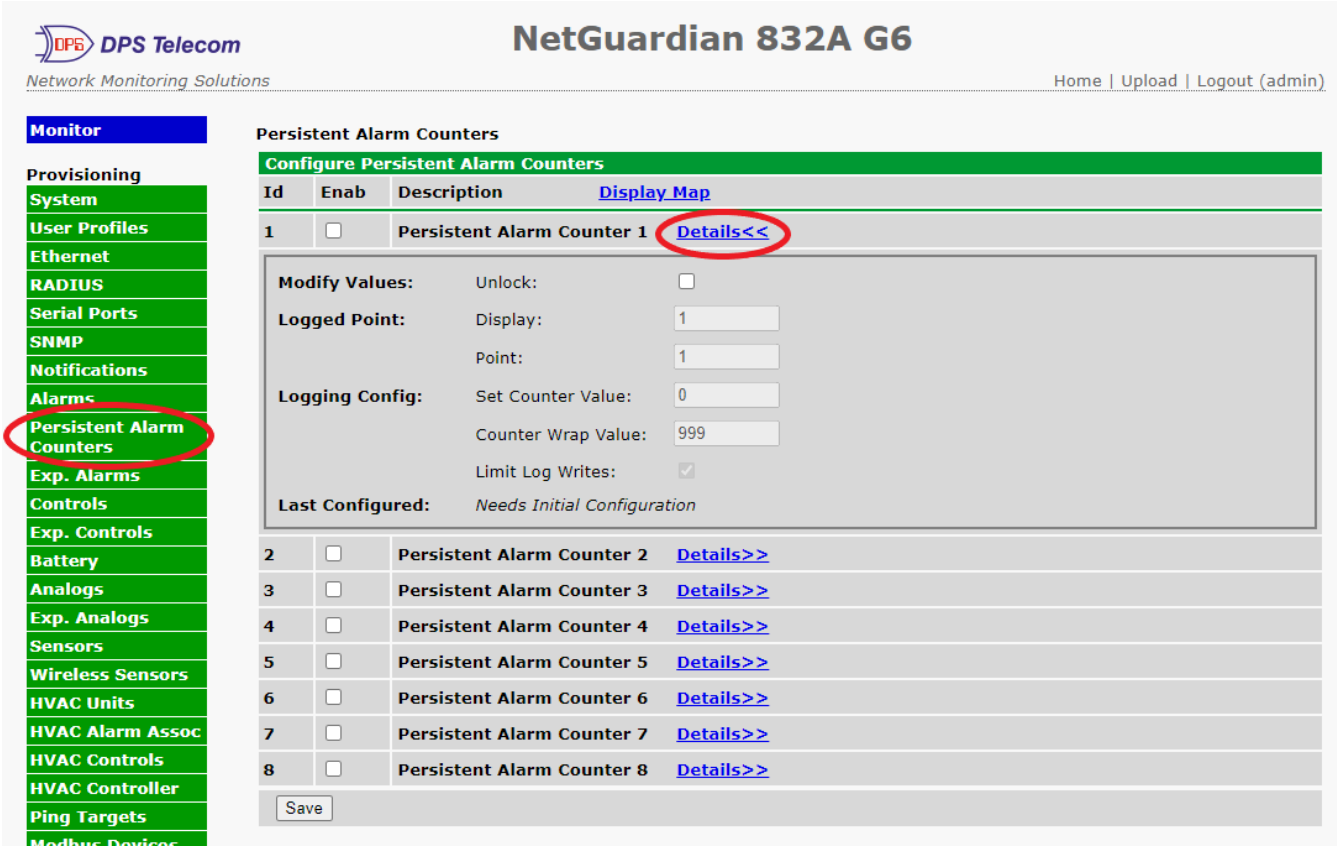


The Provisioning > Alarms menu

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. Unchecked (Normally Open): Alarm is clear when contact is open and set when contact is closed. Checked (Normally Closed): Alarm is clear when contact is closed and set when contact is open.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for that alarm point.
Advanced Alarm Configuration (Advanced>>)	
On Set	User-definable description (condition) that will appear for the discrete alarm input on Set. Example: "Alarm".
On Clear	User-definable description (condition) that will appear for the discrete alarm input on Clear: "Example: "Alarm Cleared".
Qual. Time (Qualification Time)	The length of time that must pass, without interruption, in order for the condition to be considered an Alarm or a Clear.
Qual. Type (Qualification Type)	Allows you to choose whether you want to apply the Qualification Time to the alarm Set, Clear, or Both.

6.9 Persistent Alarm Counters

Persistent alarm counters are configured from the **Provisioning** > **Persistent Alarm Counters** menus. Configure specific alarm points to track alarm events over time, with event counters that persist across device reboots. To configure the Persistent Alarm, locate the alarm description and click the corresponding **Advanced** link to expand.



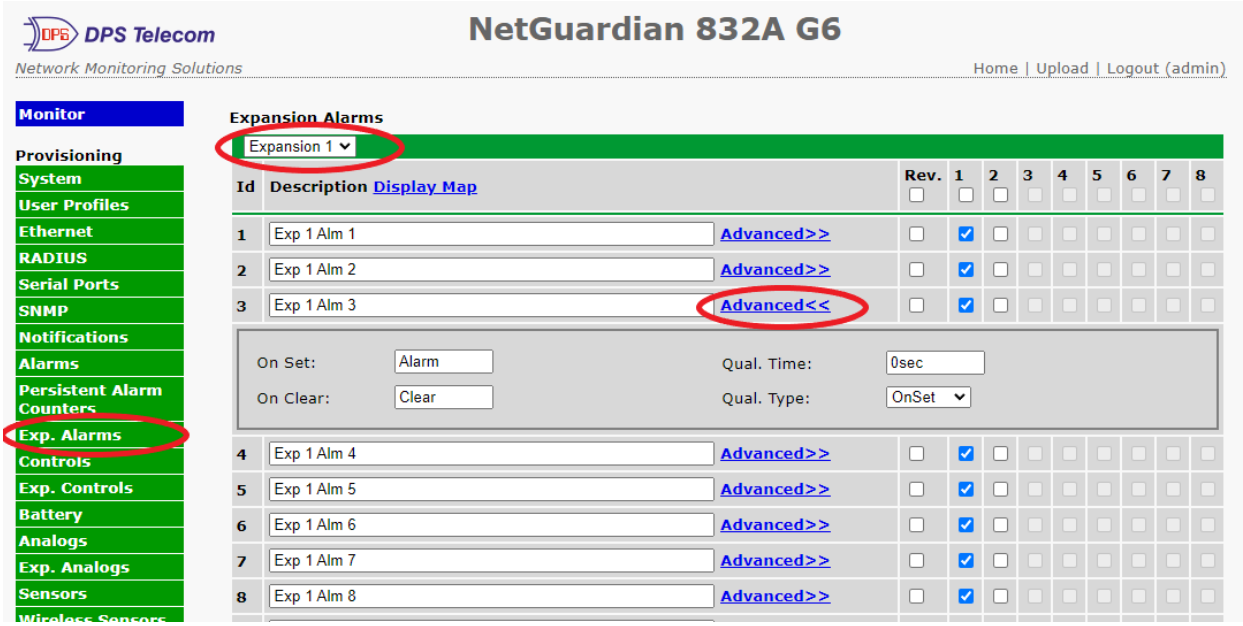
The Provisioning > Persistent Alarm Counters menu

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

6.10 Expansion Alarms

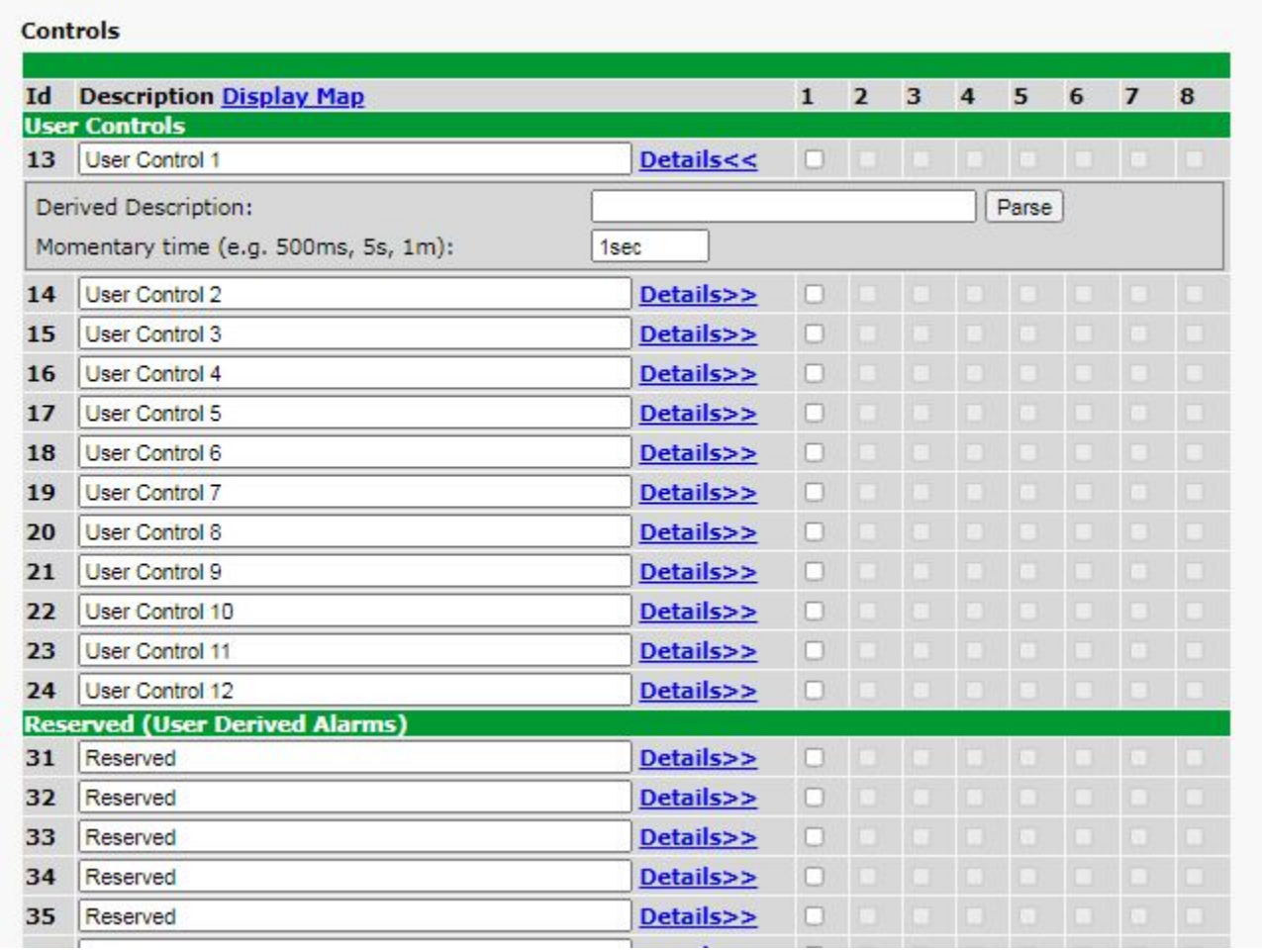
NOTE: *This menu option does not appear unless an expansion unit has been connected to your base G6.*

Expansion Alarms have the same functionality as Alarms. They are added as part of an expansion unit, depending on your expansion configuration you will have the ability to select which expansion alarms to configure via the drop down box. See image below.



6.11 Controls

The G6 control relays can be configured in the **Provisioning** > **Controls** and **Provisioning Exp. Controls** menus. You can enter your own description for these relays and designate them to a notification device(s).

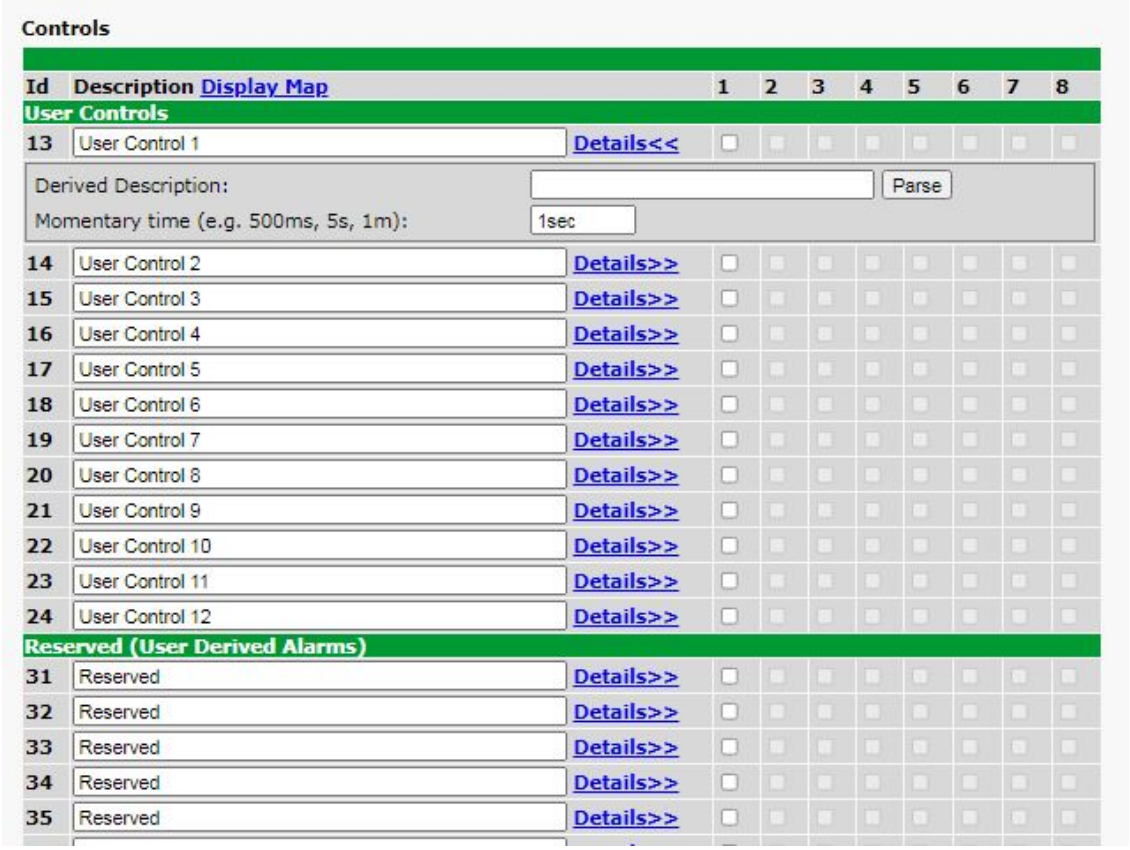


The Provisioning > Controls screen

Basic Controls Configuration	
ID	ID number for the control relay.
Description	User-definable description for the NetGuardian's control relay.
Details: Derived Description	Define simple if-then automation for this relay. Leave blank for pure manual operation. (see "Derived Controls" section for details and syntax)
Details: Momentary Time	Control on time (in milliseconds) when you execute the MOM command. Max limit of 600 seconds.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for the control relay.

6.11.1 Derived Controls

The G6's derived controls can be configured in the **Provisioning > Controls** screen. Each control can be configured for derived control. Click on Detail to show the derived controls setting. Enter in a derived control equation into the Derived Description field. Click on Parse to issue a parse command. The parse command is a test that will attempt to parse the derived control equation. It will return with a "Parse Successful!" or "Parse FAILED!" message. If "Parse FAILED!" is returned, there is an error in the syntax of the equation.



Configure derive Controls in the Provisioning menu > Controls screen > Details > Derived Description

Virtual alarms and control relays can be created from derived formulas using the following operations:

_OR : Set the current operation to OR.
_AN : Set the current operation to AND.
_NO : Set the current operation to NOT
_XR : Set the current operation to XOR.
D : Tag to change the active display number.
C# : Used as a constant where # is either a 1 or a 0.
. : Used like a comma to delimit numbers.
- : Used to specify a range of points.
S : Used like an open parentheses.
F : Used to end or close parentheses (All open parentheses must have a matching close parentheses).

(Spaces included here are for readability purposes only.)

- Precedence of the operations are always left to right unless using **S and F** for parentheses.
- All number references can either be one or two digits.

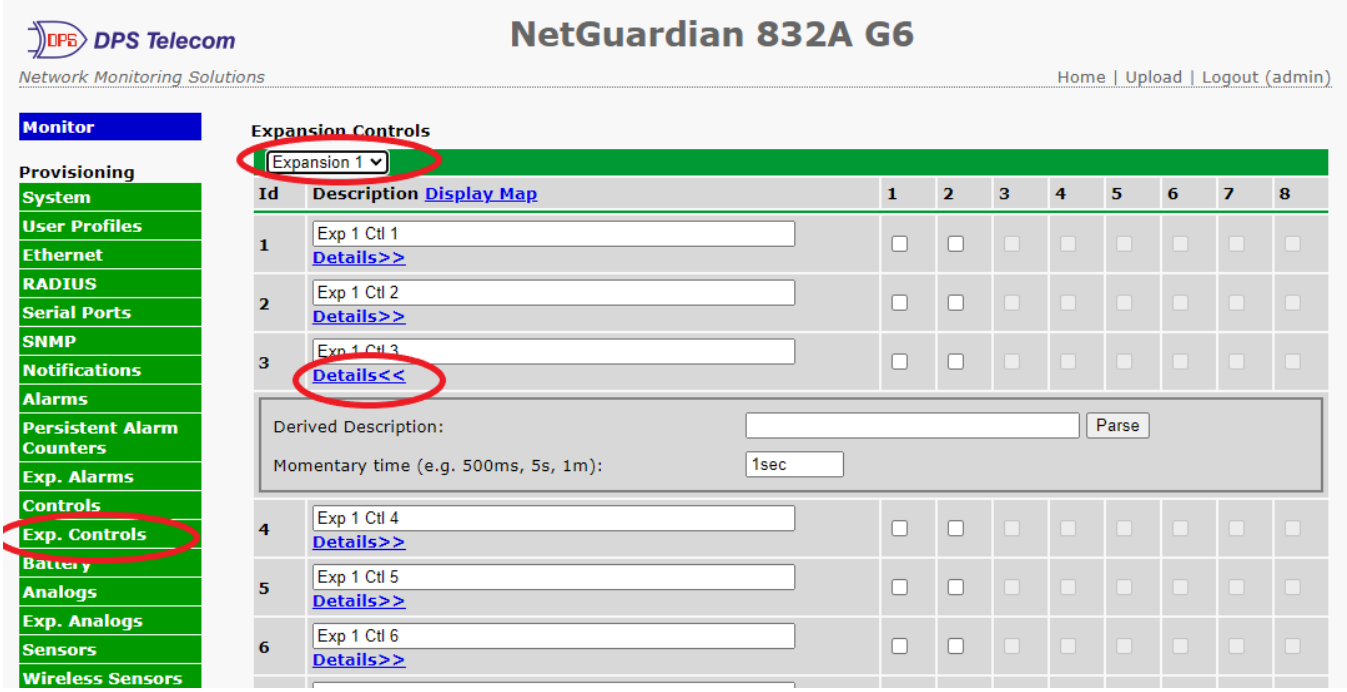
_OR D1.3-5 is logically equivalent to (1.3 || 1.4 || 1.5)
_AN D 1.3-5 D2.6 _OR D3.7 is logically equivalent to ((1.3 && 1.4 && 1.5 && 2.6) || 3.7)

_OR D01.03-05 D02.06 _AN D02.07 D03.10.-12 is logically equivalent to ((1.3 || 1.4 || 1.5 || 2.6) && (2.7 && 3.10 && 3.12))
_AN D1.3-5D2.6_OR.7D3.10.12 is logically equivalent to ((1.3 && 1.4 && 1.5 && 2.6) || 2.7 || 3.10 || 3.12))
_AN D1-2 : Control will parse
_OR S_AND1.1-2FS_AND1.3-4F is logically equivalent to (1.1 && 1.2) || (1.3 && 1.4)
_OR C1 D1.1 is logically equivalent to (1 || 1.1)

6.12 Expansion Controls

NOTE: *This menu option does not appear unless an expansion unit has been connected to your base G6.*

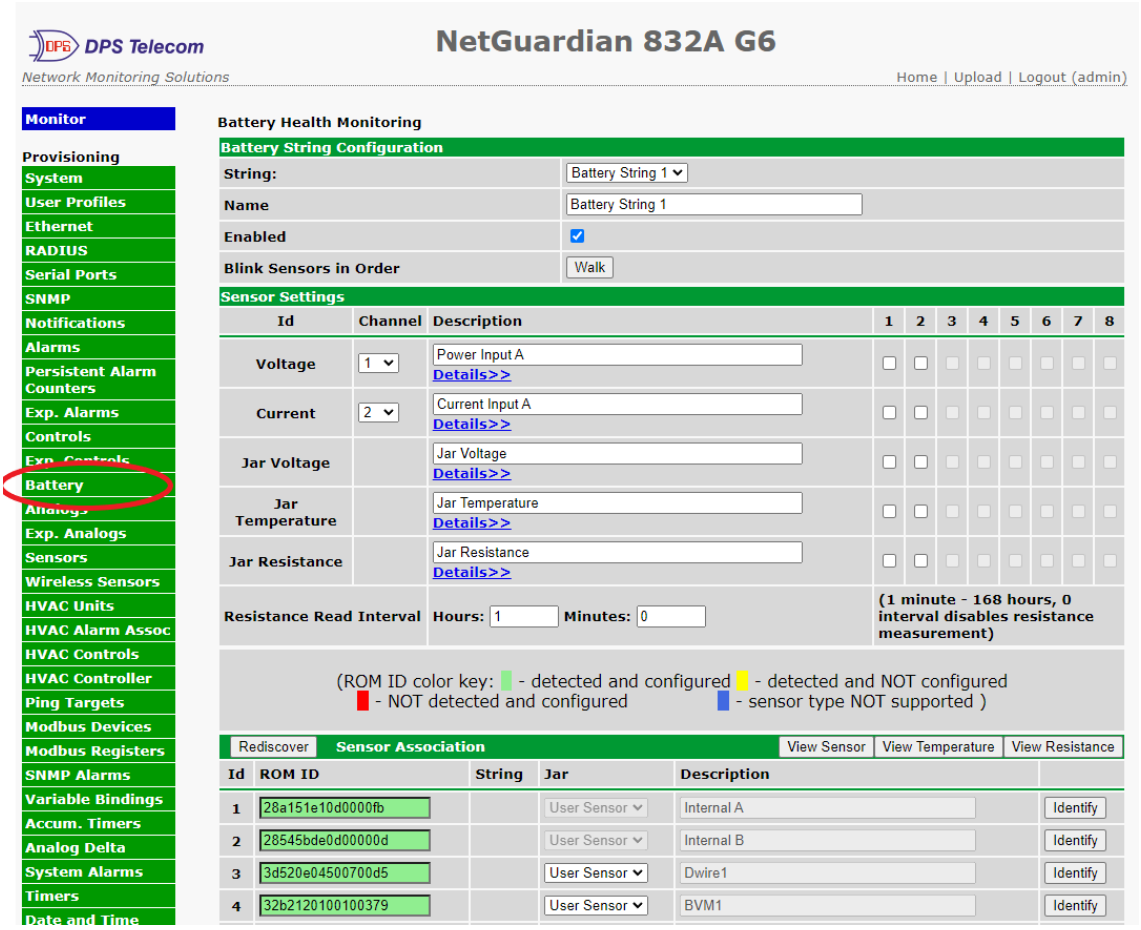
Derived Expansion Controls have the same functionality as Derived Controls. They are added as part of an expansion unit, such as the NetGuardian E16 DX G2, which extends your available quantity of control relays. When available, they will appear on this additional page of control relays. Depending on your expansion configuration you will have the ability to select which expansion controls to configure via the drop down box. See image below.



The Provisioning > Exp. Controls screen

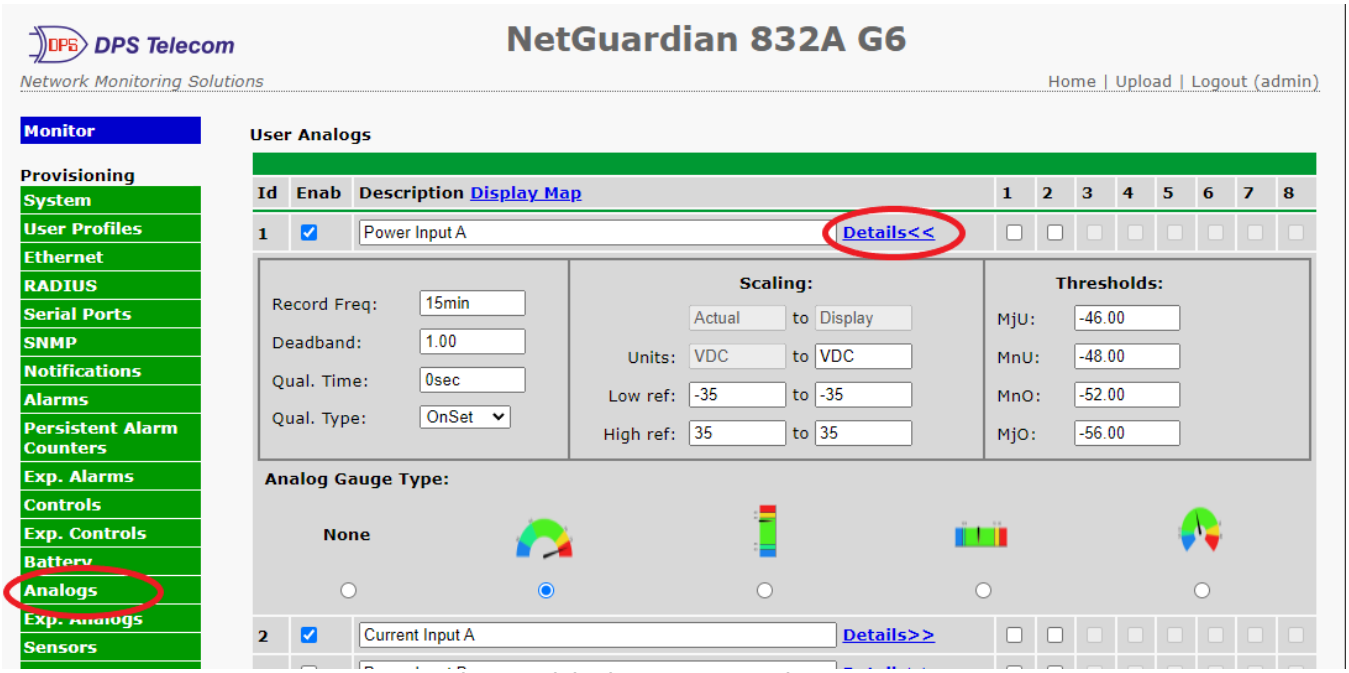
6.13 Battery

1. In the "***Provisioning***" section click the **Battery** link.
2. If you opened this menu after adding a new BVM Sensor to the D-Wire, a new ROM ID will be visible and highlighted in yellow (indicating "detected and NOT configured"). If you add a new BVM Sensor while this menu is open, simply click the 'Rediscover' button.
3. Select a String name and Jar number for this BVM Sensor.
4. Name the Voltage, Temperature, and Resistance sensors as desired (ex. "Jar 1 Voltage")
5. Each time you add your first sensor to a new battery string, configure the string's options at the top portion of this menu (use the dropdown menu to select a string to change its settings). These string settings (including the 4 major & minor, over & under alarm thresholds) are common to all sensors in the string. Some settings, like the Analog Channel for string voltage, are not directly related to your BVM Sensors but instead are related to a separate analog input used to independently measure to total string voltage. 7. Repeat this process for each sensor you add. Consider that, unless your PC is not easily accessible during installation, it is usually easiest to plug in one sensor, configure it, then plug in the next sensor, and so on. This makes it obvious which physical sensor you are configuring in the web interface.



6.14 Analogs

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

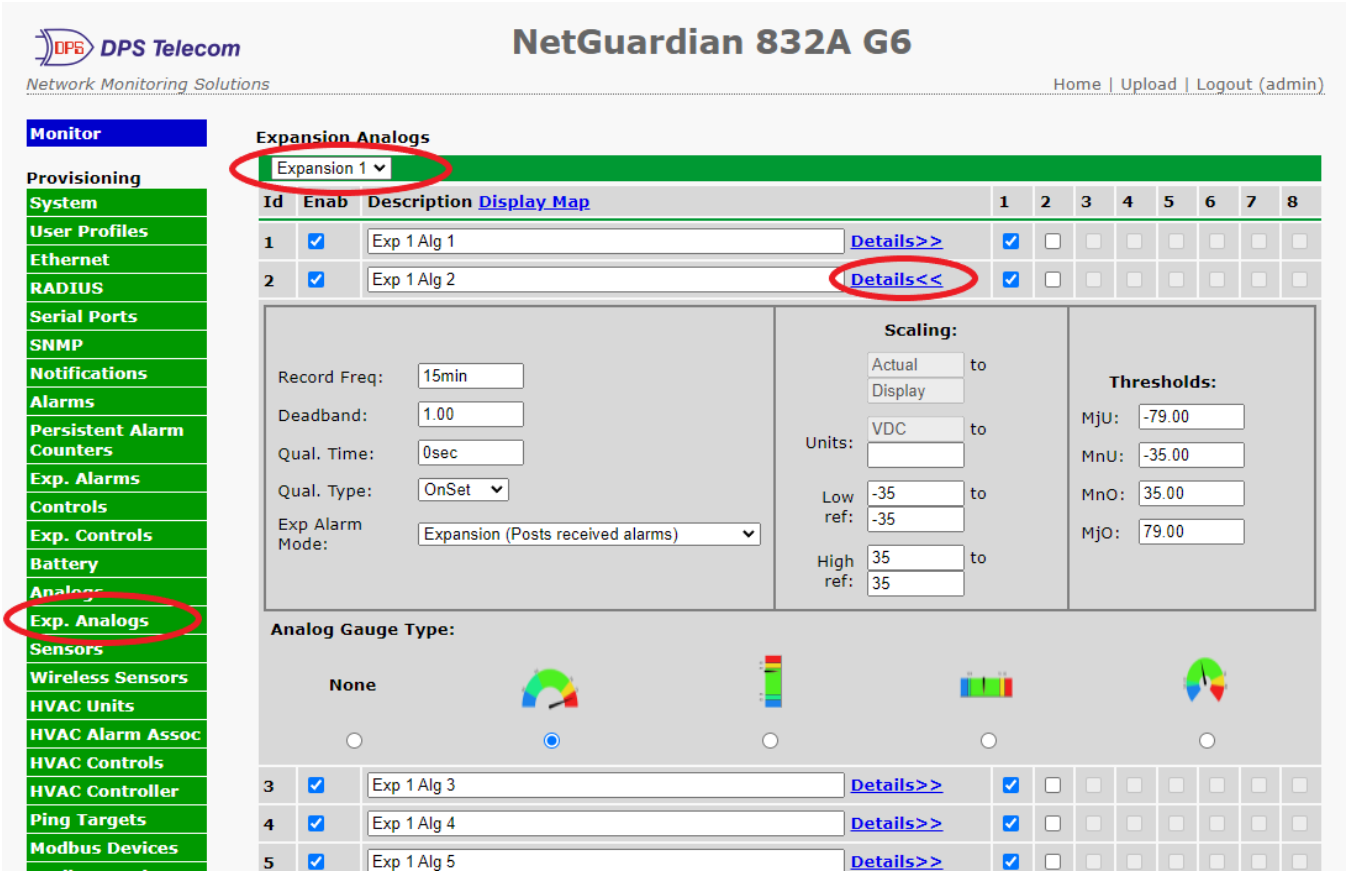
NOTE: Analog channels 7 and 8 are for internal voltage monitoring (On a single power input build, channel 7 is unused.)

User Analogs	
Enab (Enable)	Checking the box in the **Enab** column enables monitoring of the analog channel.
Description	User-definable description for the analog channel
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 TempDefender G2 will record the analog reading
Deadband	The additional qualifying value the TempDefender G2 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 TempDefender G2 to set an alarm. Recorded values less than an under value or greater than an over value will cause alarms.
Discrete Input	Assign the alarm point associated with this analog.
Qual. Time (sec)	Length of time, in seconds, 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

6.15 Expansion Analogs

NOTE: *This menu option does not appear unless an expansion unit has been connected to your base G6.*

Expansion Analogs have the same functionality as User Analogs. They are added as part of an expansion unit. When available, they will appear on this additional page of user analogs. Depending on your expansion configuration you will have the ability to select which expansion controls to configure via the drop down box. See image below.



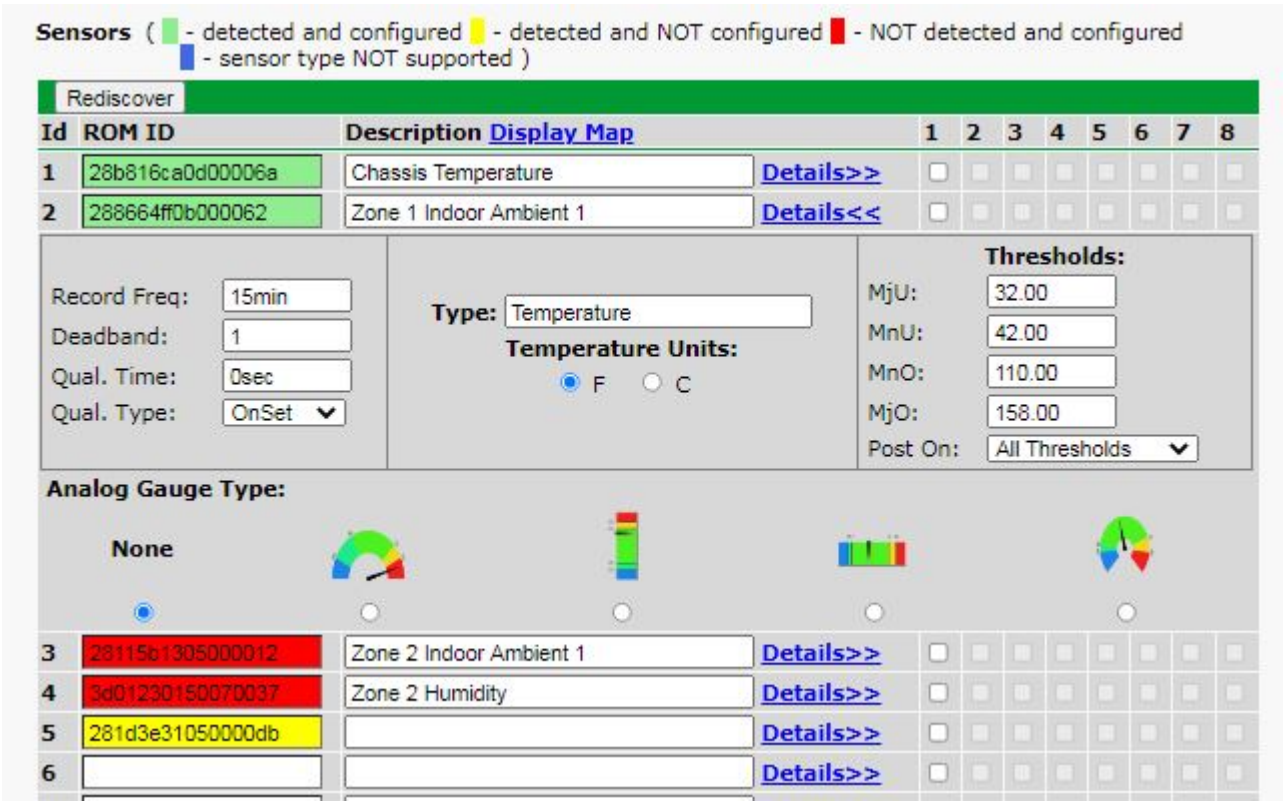
The Provisioning > Exp. Analogs screen

6.16 Sensors

In this section, you can find the settings for your D-Wire Sensors. Most DPS sensors are automatically detected and NOT configured (highlighted yellow in the web browser) when plugged into your DPS remote. Once your sensor is plugged in, you will need to configure it using the ROM ID and sensor description you wrote down earlier when plugging the sensor in (section *Installing Your Sensors*).

D-Wire Sensors

- The HVAC Controller supports up to 32 daisy-chained D-Wire sensors via its D-Wire input. Sensors connected to the HVAC Controller will appear on the web interface. The background color of the ROM field informs the user of the sensor's configuration state.
- One of the HVAC Controller's D-Wire sensor IDs is reserved for 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 HVAC Controller'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.

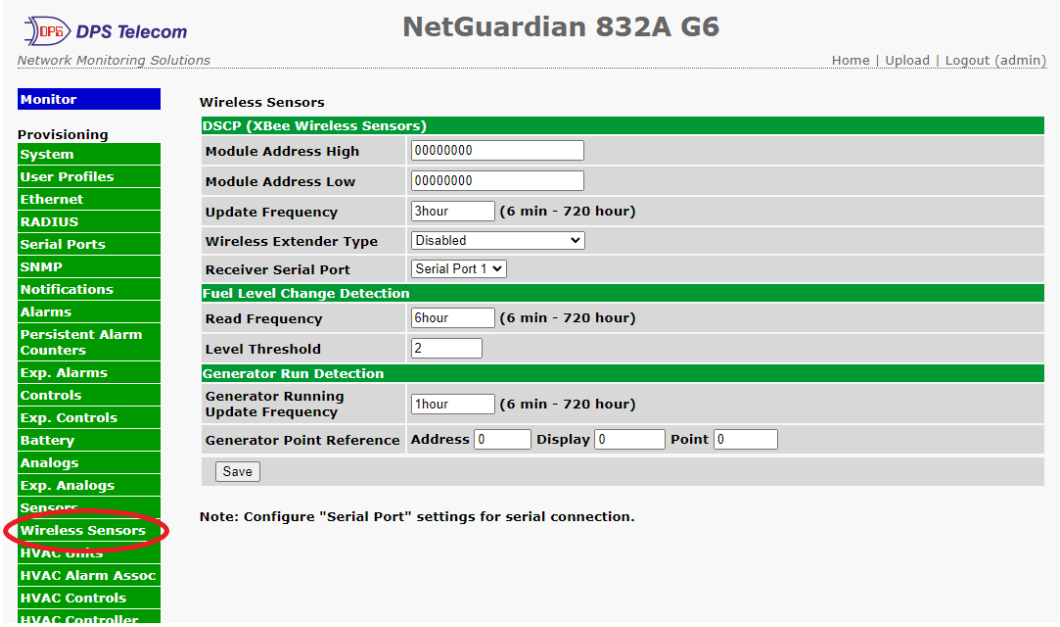


Sensors	
ID	The sensor point number
ROM ID	The ID number found on the sticker of the temperature sensor node. Your HVAC Controller will automatically detect the sensor ID when you plug a sensor into the unit. The color of the sensor ID field will tell you the status of the connected sensor. **Green** - The sensor is connected and properly configured. **Yellow** - The sensor is connected but has not yet been configured (fill in your configuration fields and click **Save** to configure the sensor). **Red** - The sensor is not detected and configured (i.e. a previous configured sensor is no longer connected). **Blue** - The sensor is not supported by the HVAC Controller. To reconfigure or disable the Sensor ID, simply delete any data in this field and click **Save**. The unit will refresh the sensor ID on that channel.
Description	User-definable description for the sensor channel.
Notification Devices	Check which notification, 1 through 8, you want to send alarm notifications for that alarm point.
Details	
Record Frequency	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.
Qualification Time	The length of time that must pass, without interruption, in order for the condition to be considered an Alarm or a Clear.
Qualification Type	Allows you to choose whether you want to apply the Qualification Time to the alarm Set, Clear, or Both.
Thresholds	These settings are set to indicate the severity of the alarm depending on which threshold values have been passed. Enter values for Major Under (MjU), Minor Under (MnU), Minor Over (MnO), and Major Over (MjO).
Post On	Select the threshold alarms to post: All thresholds, Major Only, Minor Only, Major Over Only, Major Under Only.

6.17 Wireless Sensors

Provisioning > Wireless Sensors

Configure a connected wireless receiver unit to gather analog values from a paired wireless extender unit



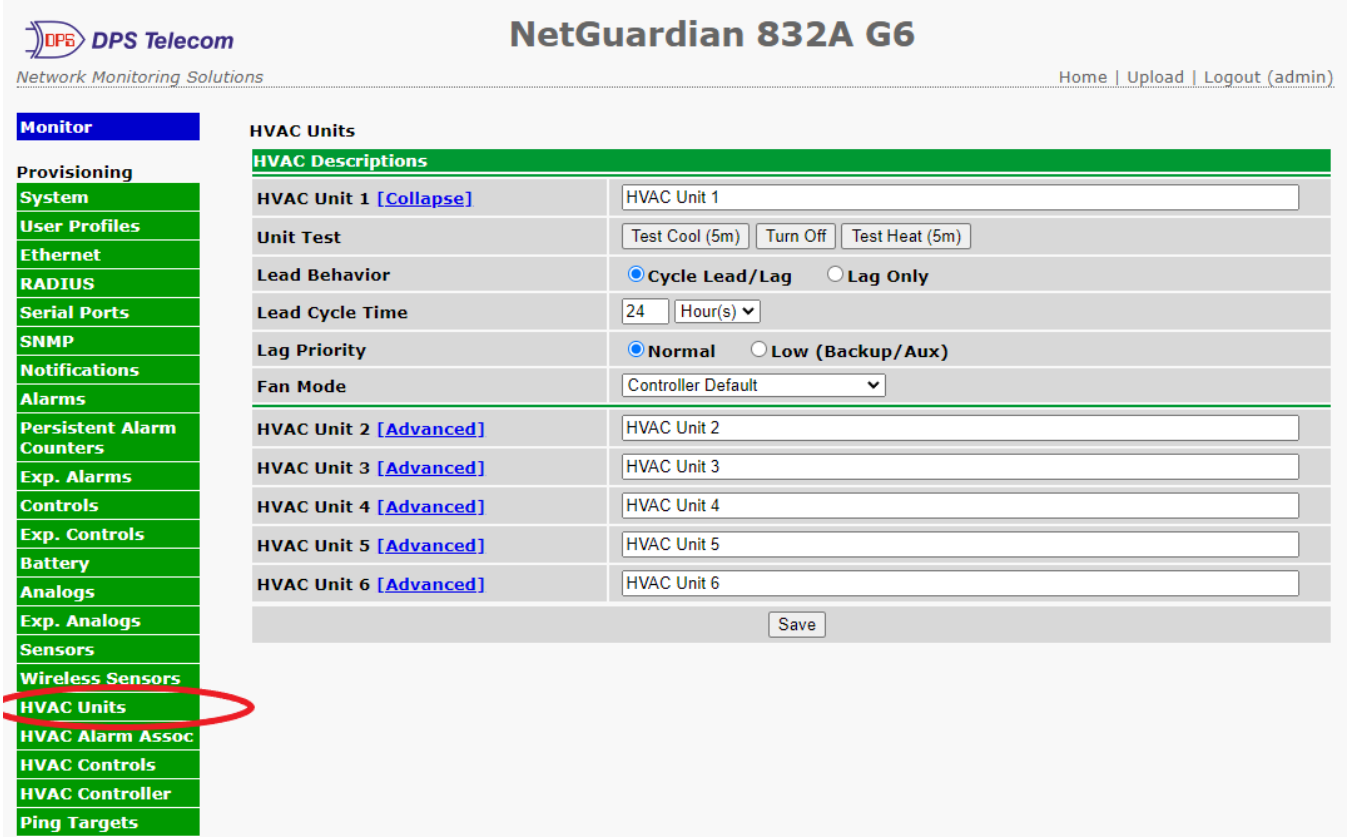
The Provisioning > Wireless Sensor menu

DSCP (XBee Wireless Sensors)	
Module Address High	4-byte identification address that is automatically acquired when the DSCP device is sync'd with the NetGuardian.
Module Address Low	4-byte identification address that is automatically acquired when the DSCP device is sync'd with the NetGuardian.
Update Frequency	The rate that the DSCP device will collect information from the sensor.
Wireless Extender Type	The specific type of DSCP device (Propane Monitor, Track Monitor, etc...).
Receiver Serial Port	Specify which the serial port (1-8)
Fuel Level Change Detection	
Read Frequency	The DSCP device will read the propane level at this frequency and will remember the last read value. Input '0' to disable this feature.
Level Threshold	If the propane level reading differs by the Level Threshold value from the previous reading, then the most recently read value will immediately be sent to the NetGuardian once.
Generator Run Detection	
Generator Running Update Frequency	When the specified alarm point (from Generator Point Reference) is set, the timer value for Generator Running Frequency will override the timer value for Update Frequency (under Module Configuration). This takes effect after the next update.
Generator Point Reference	Specify the Address, Display and Point attached to Gen. Running Frequency. Input '0' to disable this feature.

6.18 HVAC Units

Provisioning > HVAC Units

The G6 can configure 6 different HVAC units into 4 HVAC zones where they can be assigned. Each unit can be assigned in multiple zones. When configuring the HVAC units, it is recommended to use central units that occupy multiple zones as "Lag Only" and assign HVAC units that only occupy a single Zone as Cycle Lead. At all times, it is best to maintain at least one Lead HVAC unit in each Zone.



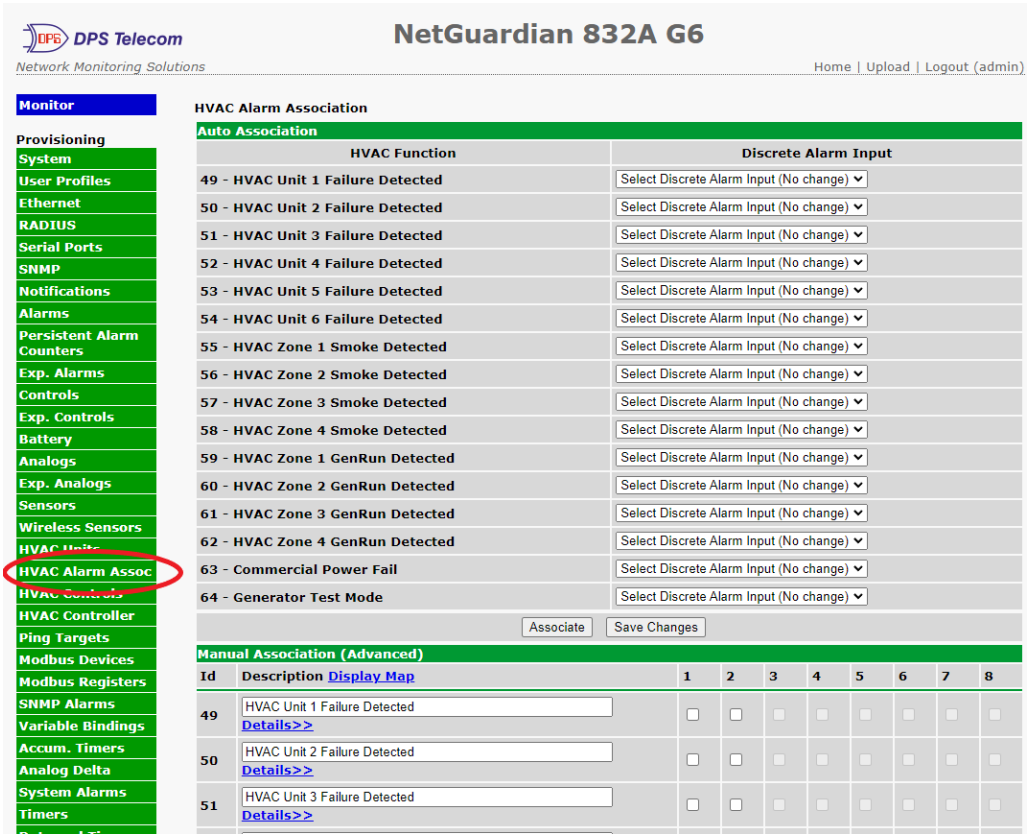
HVAC Units	
HVAC Unit #	User defined name of HVAC unit.
Unit Test	5 minute tests of Cool/Heat will override the zone behavior and any "warm-up" or "cool-down" periods. "Turn off" is an option to force off a specified unit; this results in the unit having to wait for the configured cool-down time before being allowed to cool or heat again.
Lead Behavior	Cycle Lead/Lag = Can be assigned Lead if available Lag Only = Will never be assigned as Lead
Lead Cycle Time	Amount of time before lead HVAC is tagged out for a new unit
Lag Priority	If Low is selected, then this HVAC will only be activated once all other HVACs of normal priority have been chosen and there is still a need to activate another unit.
Fan Mode	Fan Mode relates to an HVAC units blower behavior: "Controller default" means that the blower will be on only if cooling or heating. "Always on while lead" will keep blower on if the unit is a lead unit, even when cooling or heating is not enabled. "Always on" will turn the blower on permanently, unless some other error condition forces the blower off (e.g. presence of smoke, HVAC unit reports a fault).

6.19 HVAC Alarm Association

The alarm impulses from the HVAC Zones are abstracted from physical inputs, through virtual controls 49-64 ("Controller Special Function Inputs"). This allows us to create combinations of different alarm points through the derived control interface, allowing more complex alarm input behavior if needed.

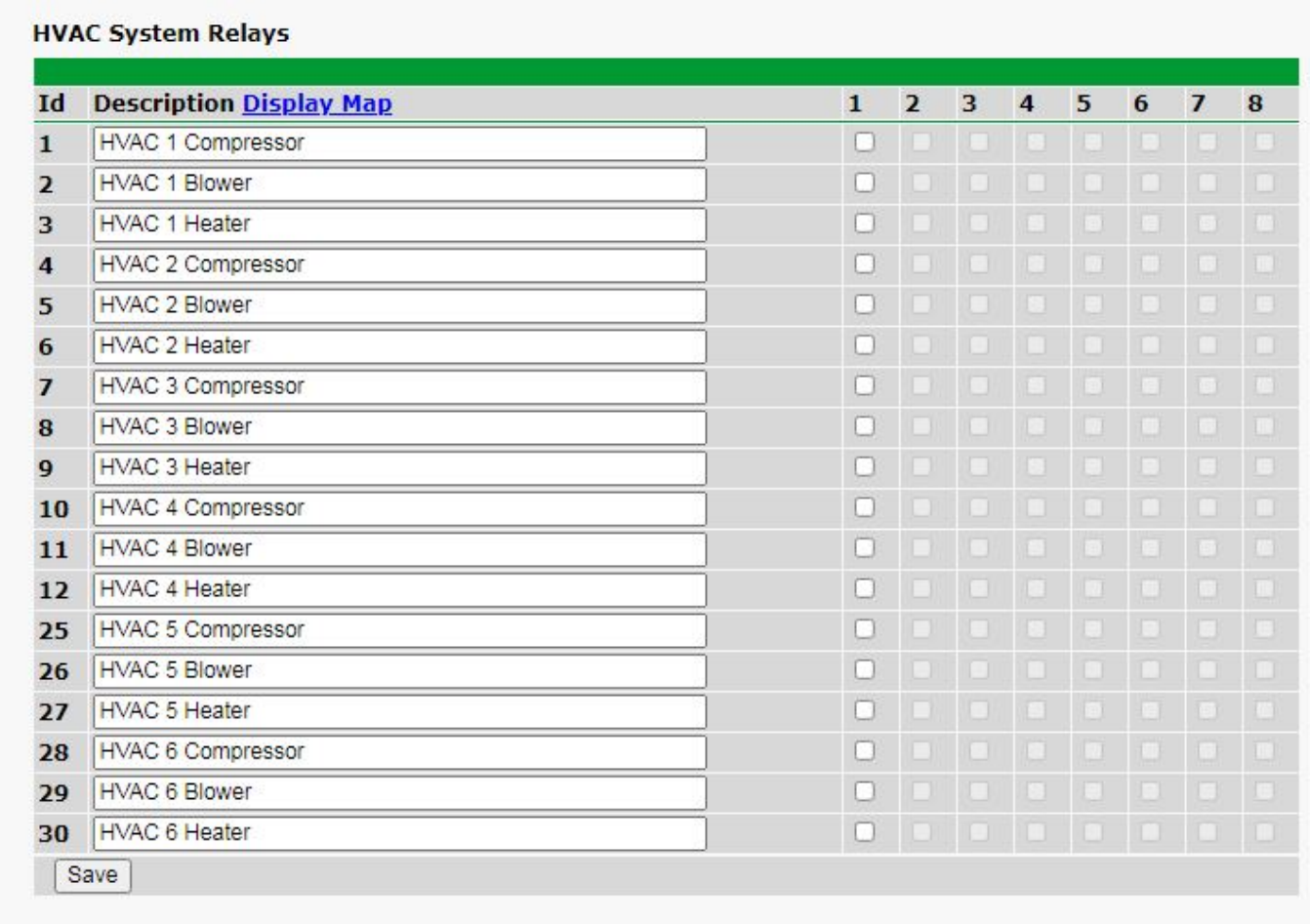
Auto Association will automatically populate a simple derived control based on a discrete alarm input. Select the desired discrete alarm input(s) for the HVAC function(s) and click 'Associate' to generate the appropriate derived control to link a discrete alarm to the G6.

Manual Association allows you to manually parse a derived control for the indicated HVAC function, and allows you to notify on these virtual points as well.



6.20 HVAC Controls

This section contains the set of control relays that are dedicated to HVAC unit control relays. This are separate from the general-purpose controls.

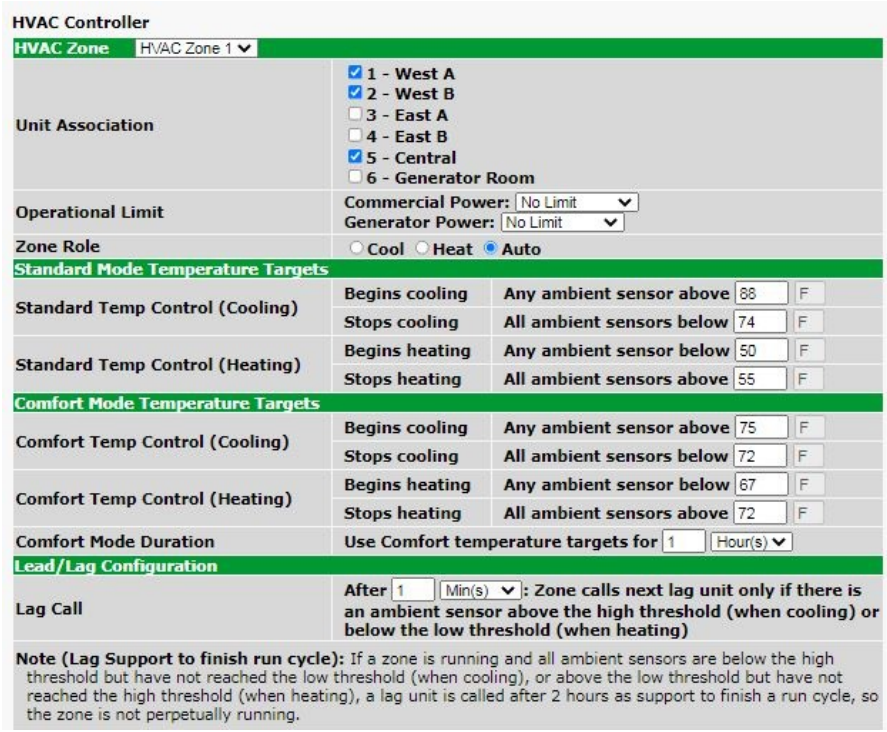


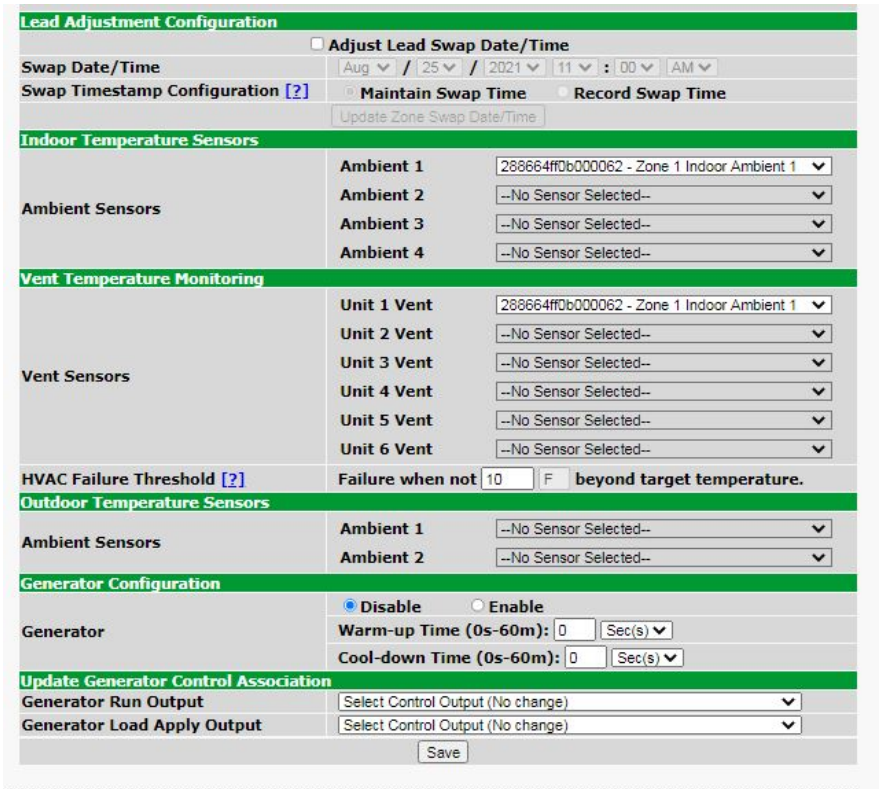
Provisioning > HVAC Controls

HVAC/Base Controls	
Num	ID number for the control relay.
Description	Description for the HVAC Controller's control relay.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for the control relay.

6.21 HVAC Controller

See the Lead/Lag Behavior section for information on the HVAC's cooling and heating logic.





HVAC Zone	
HVAC Zone	Select which zone to configure.
Unit Association	Assign HVAC units to the selected zone. Units can be assigned to multiple zones. A zone with no assigned units will appear as "Not Configured" or "Suspended" in monitor interfaces.
Operational Limit	Restricts the number of HVACs that can be active under commercial or generator power.
Standard Mode Temperature Targets	
Standard Temp Controller (Cooling)	Set the temperature thresholds at which HVACs will begin and end cooling
Standard Temp Controller (Heating)	Set the temperature thresholds at which HVACs will begin and end heating
Comfort Mode	
Comfort Mode	Similar to Standard cooling, comfort mode is designed to hold ranges more comfortable for people when they are within the HVAC Zone.
Comfort Mode Duration	Time Comfort Mode will be active before switching to Standard Mode.
Lead Adjustment Configuration	
Adjust Lead Swap Date/Time	Select this to change the timestamp of last swap. Useful for testing purposes: by setting timestamp to 24 hours before the current timestamp, you can trigger the lead swap.
Swap Date/Time	Timestamp of the last HVAC lead swap.
Maintain Unit Swap Time	When updating lead unit, swap time will be updated by adding the previous lead unit's cycle time. This mode is better for scheduling lead cycles at a fixed time; this mode prevents an expected forward drift in swap date/time that accumulates when lead swap is delayed due to HVAC zone activity at time of swap.
Record Unit Swap Time	When updating lead unit, swap time is set to the current unit time.
Indoor Temperature Sensors	
Ambient Sensors	Sensors used to monitor temperature within the HVAC Zone.
Vent Temperature Monitoring	
Vent Sensors	Sensors used to monitor how effective the HVAC is at reaching target temperatures.
HVAC Failure Threshold	Triggers a failure alarm when the vent sensors are not within the threshold.
Outdoor Temperature	
External Sensors	Optional sensors to monitor temperatures outside of the HVAC Zone.
Generator Configuration	
Generator	Enable if your HVAC environment will rely on generator power, otherwise disable.
Warm-up Time	The length of buffer time between when the generator starts running and when the the generator is ready to handle the power load.
Cool-down Time	The length of buffer time between when the generator load apply is switched off and when the generator stops running.
Update Generator Control Association	
Generator Run Output	Assign the control you want to use to turn on and off the generator.
Generator Load Apply Output	Assign the control you want to use to turn on and off generator load apply.

6.22 Ping Targets

Each of the 32 ping targets can be provisioned with a description and an IP address. The G6 will issue a call to the notification device configured in the Notifications section in the event a ping alarm occurs.*

Use the following steps to configure the ping targets:

1. From the **Provisioning** menu select **Ping Targets.**
2. Check the **Enab** box to designate that an SNMP trap will be sent when an alarm condition exists. Leaving the box blank designates that an SNMP trap will not be sent when an alarm condition exists.
3. In the **Description** field, enter a description of the device to be pinged.
4. In the **Server (IP or Hostname)** field enter the IP address or DNS hostname of the device to be pinged.
5. Under the **Notification Devices, c**heck which notification device(s), 1 through 8, will send alarm notifications in response to this alarm.
6. Click **Save** link to save the configuration settings.

*See Section 'Timers' to set ping response and fail times.

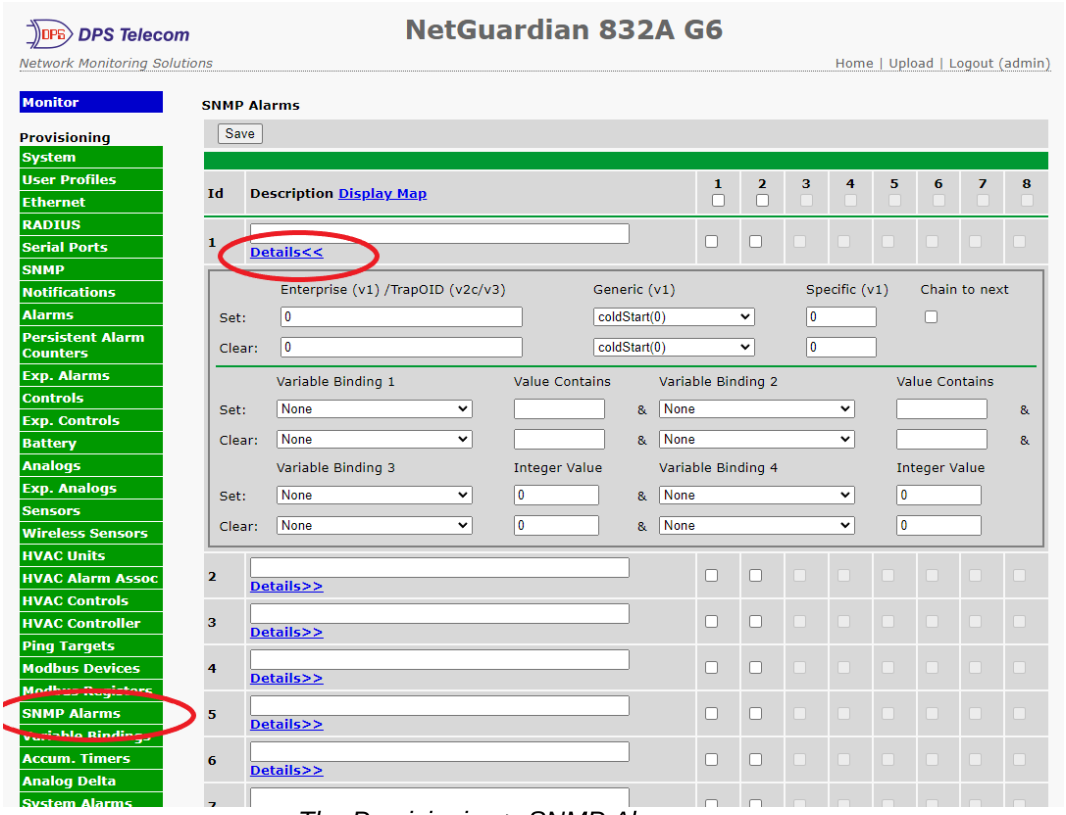
Configure the ping target parameters from the Ping Info page

6.23 Modbus Devices

The Provisioning > MODBUS Devices

Global Settings	
MODBUS Poll Delay	Delay between Modbus polls in milliseconds.
MODBUS Poll Timeout	Time duration before the MODBUS repsonse time fails in seconds.
Send Notification of every register update	This option is used to send a notification whenever a MODBUS register is polled. If the poll delay is too low this may cause some notifications to be lost.
Device Settings	
ID	MODBUS device ID.
Device Type	MODBUS device type.
Connection	TCP or Serial connection.
Host Name or IP	IP used for polling when using TCP Modbus. Unused otherwise.
TCP Port or Serial Port	TCP or physical serial port used when performing Modbus polling.
Modbus Address	Address of MODBUS device.
Device Register Offset	Amount to offset "MODBUS Address" by.
Threshold Mode	This will configure different threshold values based on MODBUS register values. Threshold mode options: 1) "standard thresholds" - default threshold setting. Only one value of thresholds will be used 2) "Idle/Running Thresholds: Status Register" - device idle thresholds will be triggered based on the value of a status register. 3) "Idle/Running Thresholds: Point Reference" - device idle thresholds will be triggered based on the value of a point reference.

6.24 SNMP Alarms

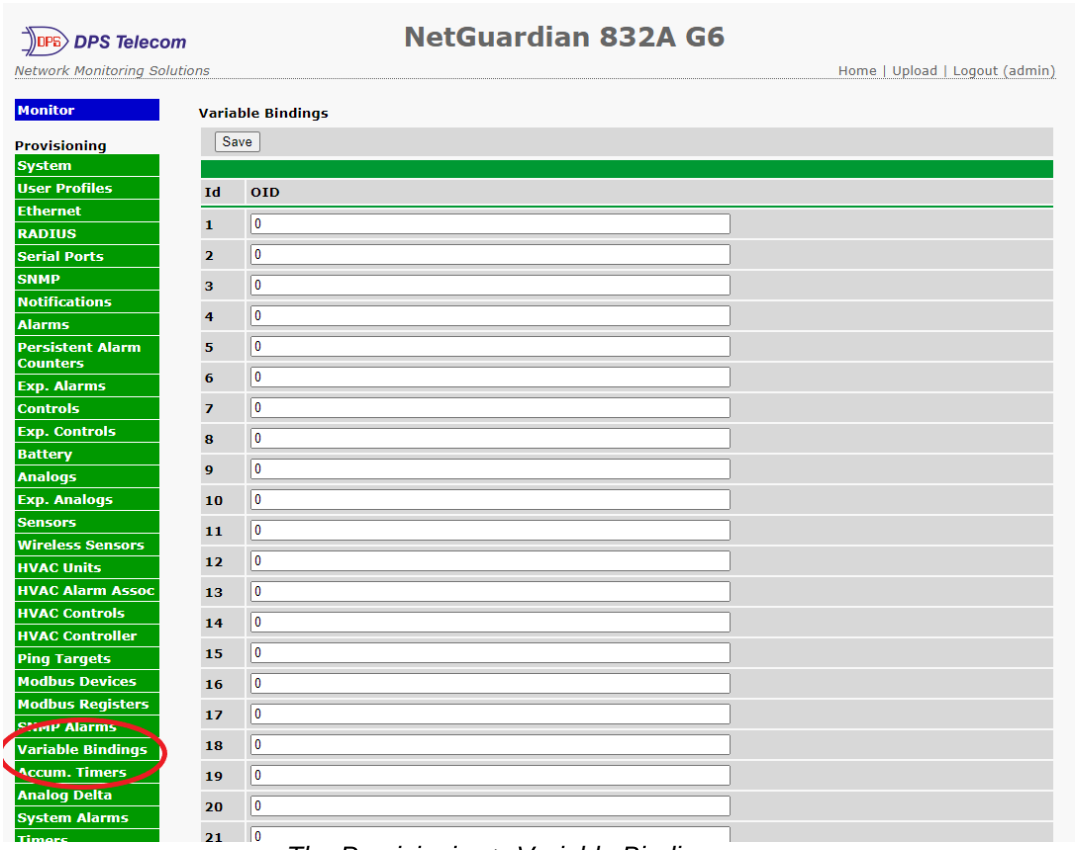


The Provisioning > SNMP Alarms menu
Provisioning > SNMP Alarms > Details

SNMP Alarms Settings	
ID	SNMP Alarm ID number.
Description	User-definable description for the SNMP alarm.
Notification Devices	Check which notification device(s), 1 through 8, will send alarm notifications in response to this SNMP alarm.
Advanced SNMP Alarms Settings (Details>>)	
Enterprise/OID	Enterprise OID for SNMPv1 or Trap OID for SNMPv2c.
Generic	Generic Trap number for **SNMP v1 only.**
Specific	Specific Trap number for **SNMPv1 only.**
Variable Binding OID	If defined, additional OID (from equipment connected to control relay) to uniquely identify the SNMP trap.
Value (Contains)	Value of the variable binding. Must be integer or string (when searching for a specific string, the string must be contained within the received trap variable binding value). **NOTE:** Using a ***** in this field is like a "wild card" - any value is accepted.

6.25 Variable Bindings

Variable bindings for the Trap Relay can be added using the **Provisioning** > **Variable Bindings** menu. Variable bindings are additional OIDs (supplied by the manufacturer of the product connected to the control relay) used to uniquely identify the SNMP trap.



The Provisioning > Variable Bindings menu

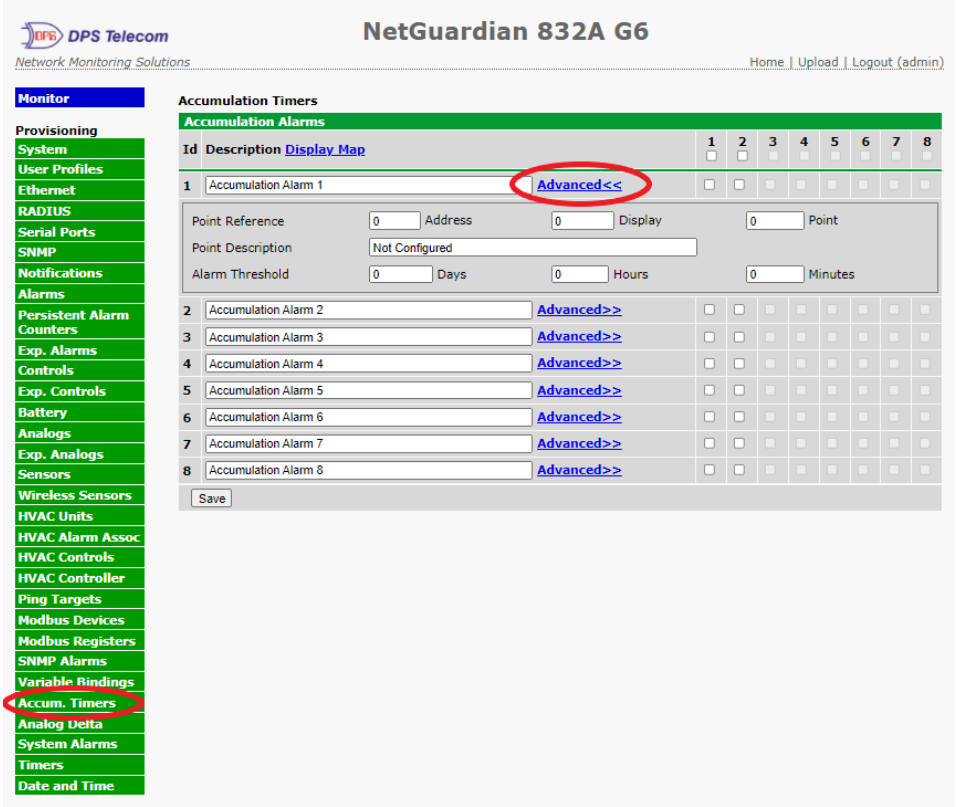
Editing Variable Bindings	
Idx	Index number for the binding.
OID	OID of the variable binding. **NOTE:** Using a ***** in this field is like a "wild card" - any value is accepted.

6.26 Accumulation Timers

The G6's **Accumulation Timer** keeps a running total of the amount of time a point is in an alarm state to send an Accumulation Event system alarm once the total time exceeds a defined threshold. Refer to Table 2.I for field descriptions.

1. Use the following steps to configure the accumulation timer settings:
2. Go to the **Provisioning** menu and select the **Accum. Timers** link, see picture below.
3. Click on the Advanced link of the Accumulation timer you are going to configure.
4. In the **Point Reference** field enter the corresponding alarm point to be monitored.
5. In the **Display Reference** field enter the corresponding display number to be monitored.
6. In the **Event Threshold** row enter the appropriate running total days, hours and minutes a point is in a alarm state in order to send an accumulation event system alarm.
7. Click the **Save** link to save the configuration settings.

The **Point Description, Point Status, Accumulated Time, and Accumulated Since** fields are not configurable. These fields will show the corresponding data of the point you configure for the accumulation timer after you have hit the **Submit Data** button.



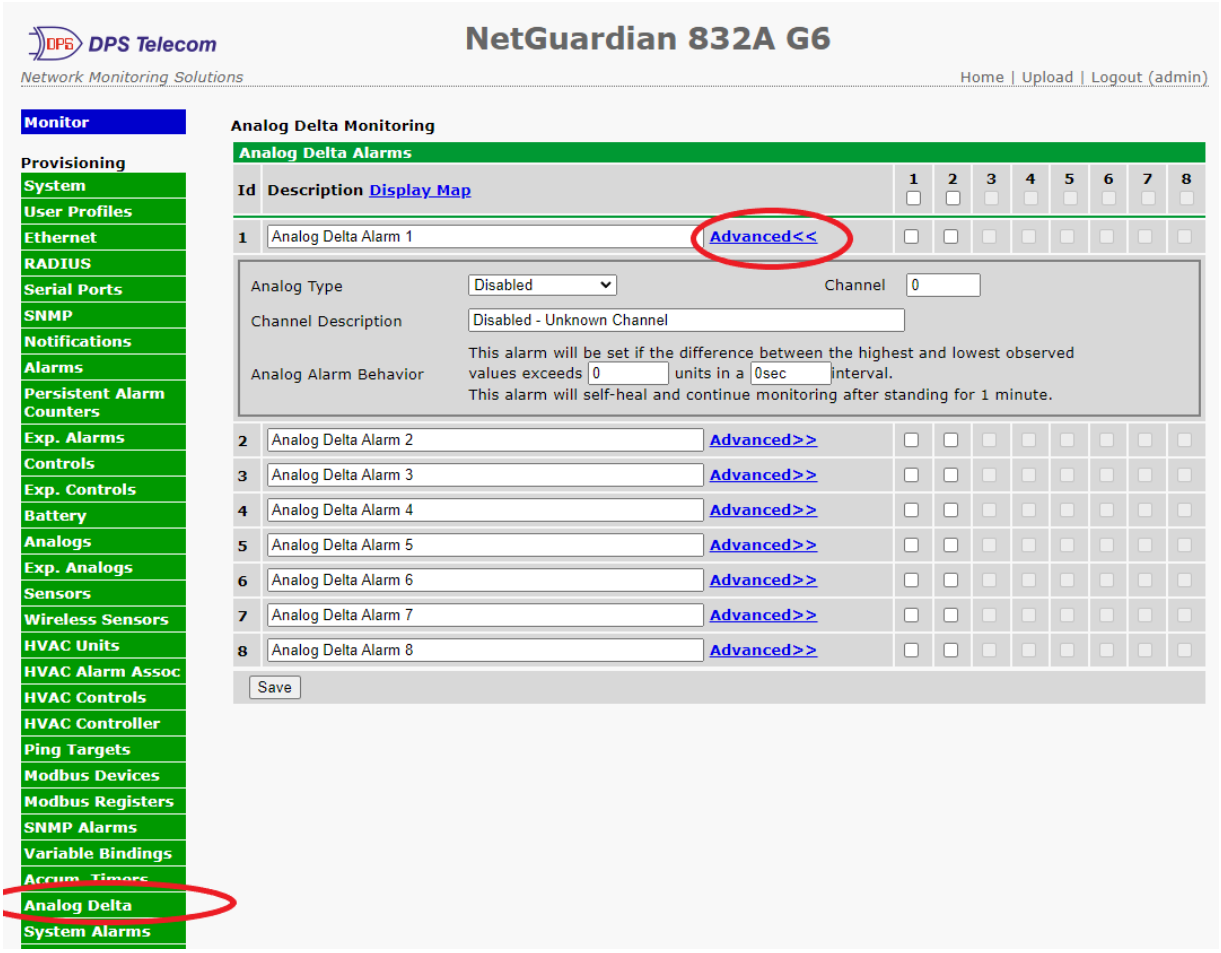
Define the Accumulation Timer settings to send an Accumulation Event alarm.

Field	Description
ID	Accumulation Alarm ID number.
Description	Description for the Accumulation alarm.
Notification Devices	Check which notification device(s), 1 through 8, will send alarm notifications in response to this Accumulation alarm.
Advanced Detail	
Address, Display and Point Reference	Indicates which alarm point is to be monitored
Point Description	The user-defined description of the monitored alarm point.
Alarm Threshold (Days, Hours, Minutes)	The amount of time allowed to accumulate before the "Accumulation Event" system alarm is set. Maximum is 45 days.

Table 2.I. *Fields in the Accumulation Timer screen*

6.27 Analog Delta

Sometimes, simply checking the alarm threshold values of your analog sensors is not enough. The Analog Delta feature allows you to define a discrete alarm to be triggered when your analog value changes too quickly, even if it does not reach an alarm threshold. For example, if temperature or pressure begins rapidly changing, which can cause damage to sensitive equipment.



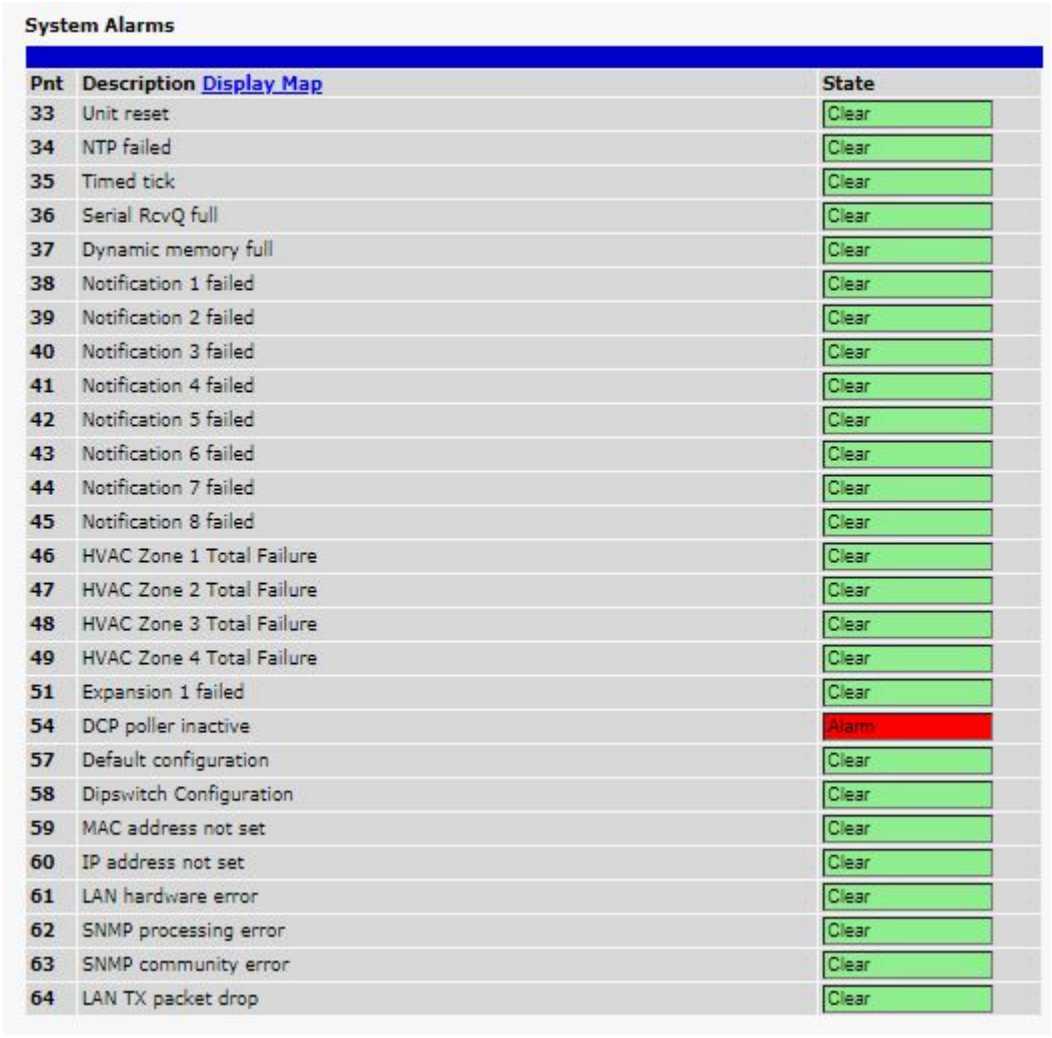
In the **Provisions** > **Analog Delta** menu, you can define a time period and maximum acceptable delta that will let your G6 know how quickly a value is allowed to change, and how often to check for a change.

Field	Description
Analog Type	What kind of analog sensor is being monitored (Base, Expansion, D-wire).
Channel	Which analog channel of the above type is being monitored. **Ex.** "Base Analogs" and "1" would correspond to the first base analog in **Edit** > **Analogs**. "D-Wire Sensors" and "4" would correspond to the fourth D-wire sensor field in **Edit** > **Sensors** (which may not be the fourth node in the daisy chain, if any previous node uses more than one field).
Analog Alarm Behavior	The maximum amount that the analog reading can change within the given time period, in either direction, before the Analog Delta alarm is triggered. **NOTE:** The difference measured is computed from the scaled reading of the analog channel, not the raw voltage difference. See "Analog Sensors" for more info on linear scaling using Reference 1 and Reference 2.

Interval	How often the NetGuardian checks the analog value for a change.

6.28 System Alarms

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



System Alarms

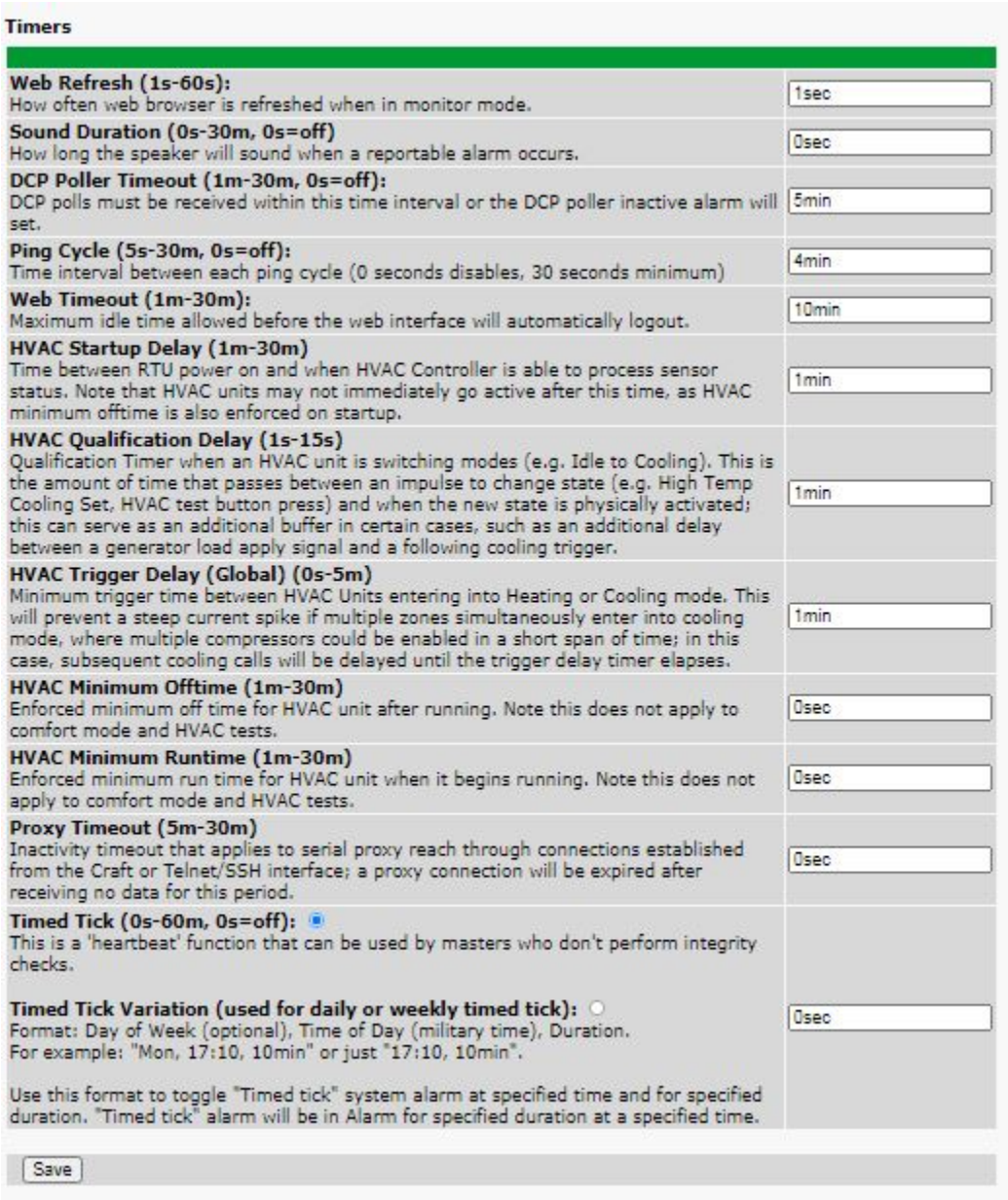
Pnt	Description Display Map	State
33	Unit reset	Clear
34	NTP failed	Clear
35	Timed tick	Clear
36	Serial RcvQ full	Clear
37	Dynamic memory full	Clear
38	Notification 1 failed	Clear
39	Notification 2 failed	Clear
40	Notification 3 failed	Clear
41	Notification 4 failed	Clear
42	Notification 5 failed	Clear
43	Notification 6 failed	Clear
44	Notification 7 failed	Clear
45	Notification 8 failed	Clear
46	HVAC Zone 1 Total Failure	Clear
47	HVAC Zone 2 Total Failure	Clear
48	HVAC Zone 3 Total Failure	Clear
49	HVAC Zone 4 Total Failure	Clear
51	Expansion 1 failed	Clear
54	DCP poller inactive	Alarm
57	Default configuration	Clear
58	Dipswitch Configuration	Clear
59	MAC address not set	Clear
60	IP address not set	Clear
61	LAN hardware error	Clear
62	SNMP processing error	Clear
63	SNMP community error	Clear
64	LAN TX packet drop	Clear

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.

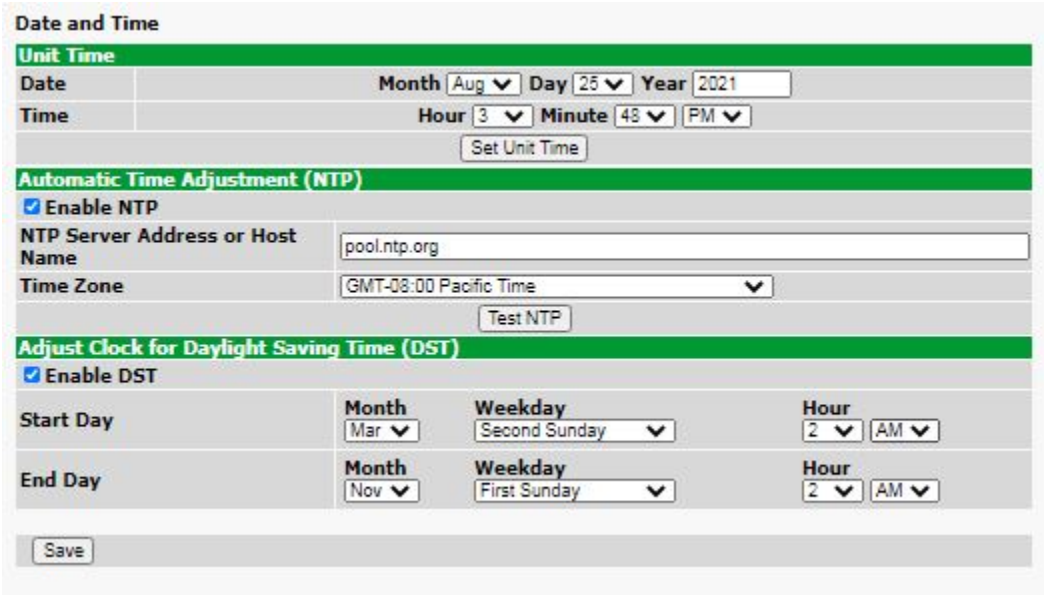
6.29 Timers

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



The Provisioning > Timers menu

6.30 Date and Time

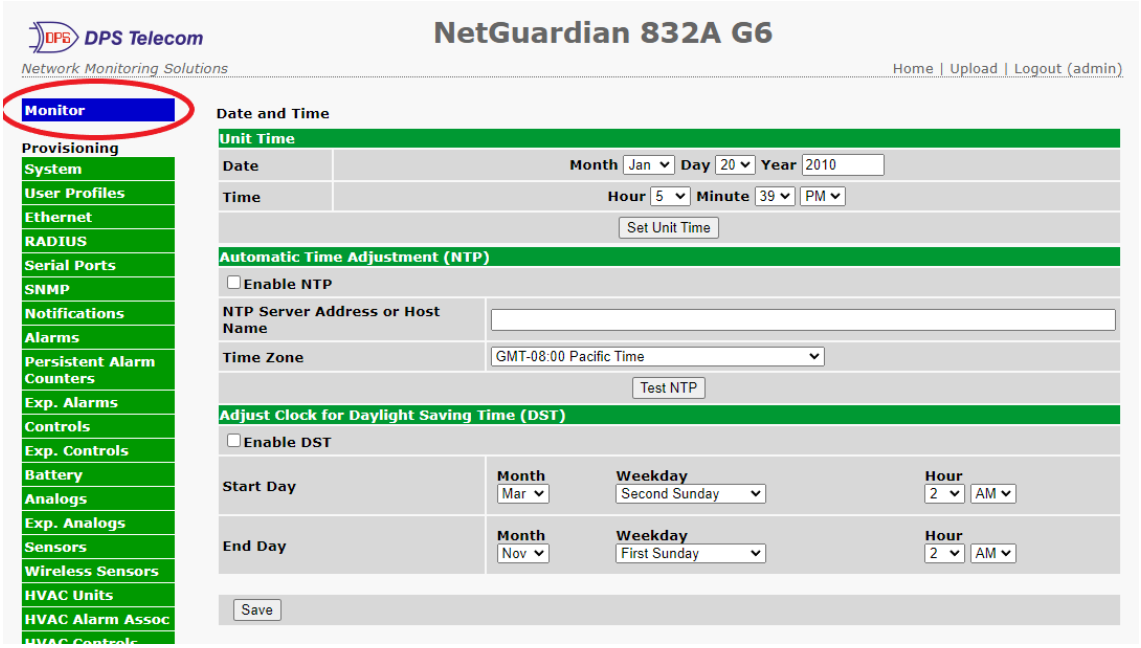


The Provisioning > Date and Time menu

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

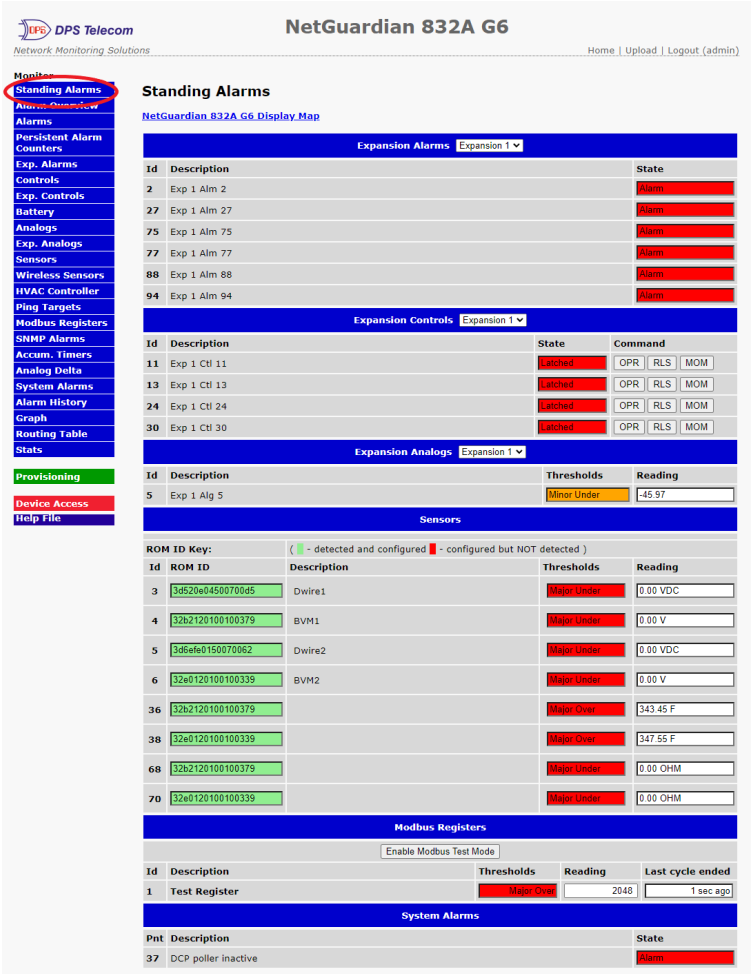
7 Monitoring via the Web Browser

Monitoring mode provides an interactive look at the status of the G6. Click on the blue **Monitor** button on the left to expand the Monitoring list.



7.1 Standing Alarms

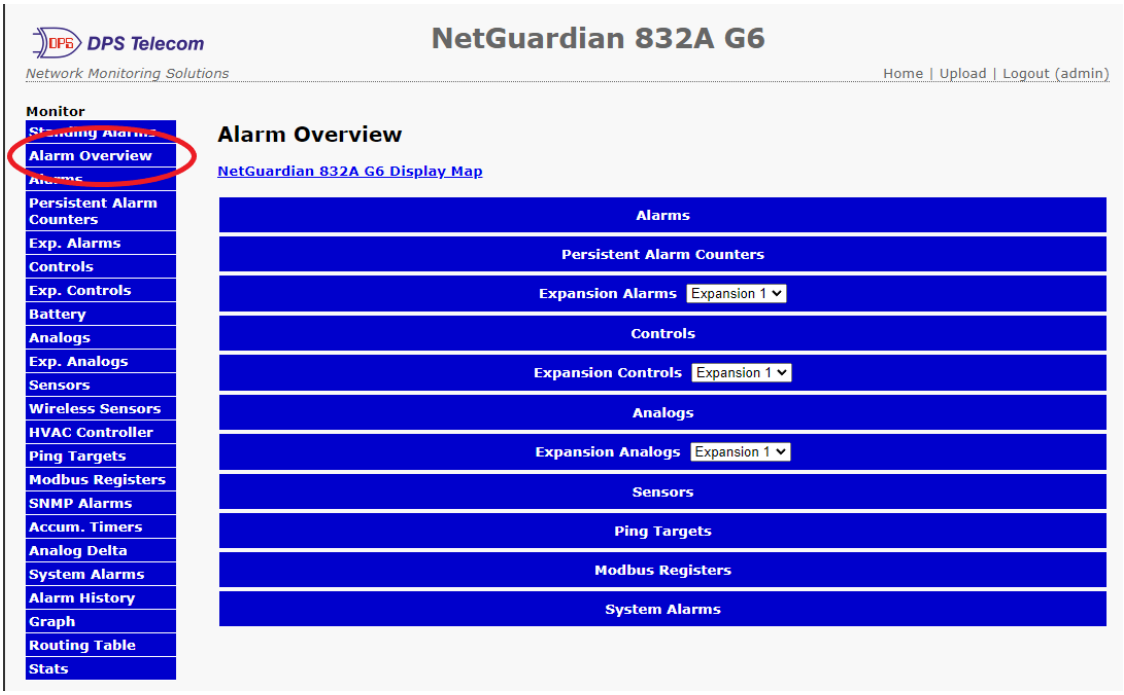
This selection provides an top-level summary of the unit and any detected problems. It's an excellent place to start when accessing the web interface to monitor your systems.



Click "Standing Alarms" to view a summary of active alarms and important analog values.

7.2 Alarm Overview

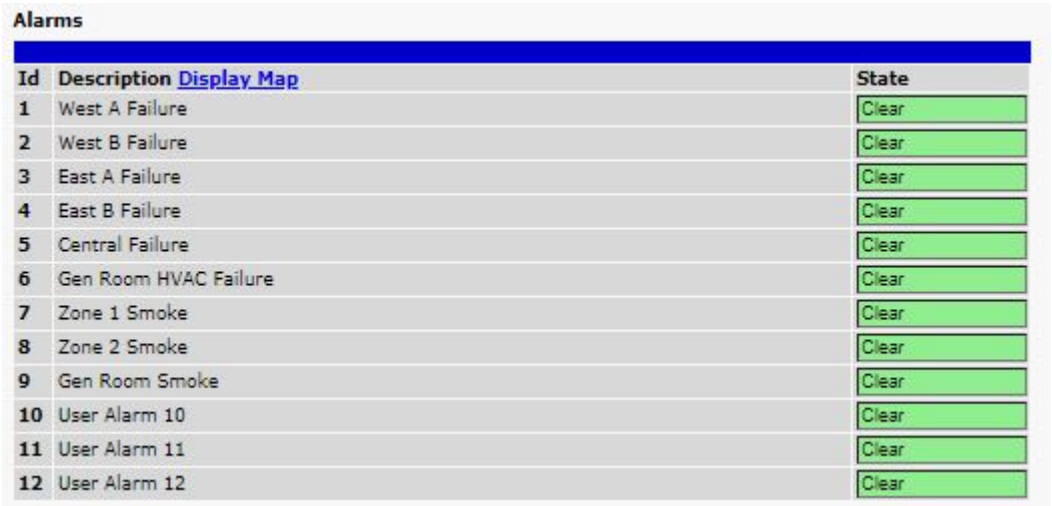
This screen provides an expanding/contracting "accordion-style" view of your alarms, controls, sensors, and more. This is handy when you want to see multiple items at once, such as the immediate effect of alarm states on your automatic Derived Control outputs.



Click "Alarm Overview" to access this list of alarms, controls, and other status information. More information is available here in one glance than in the more detailed sections of the left-pane menu.

7.3 Alarms

This selection provides the status of the base and expansion 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 or Exp. Alarms in the Monitor menu to see if any discrete alarms have been triggered.

Expansion 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; user-defined in Provisioning section)

7.4 Persistent Alarm Counters

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

Persistent Alarm Counters

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

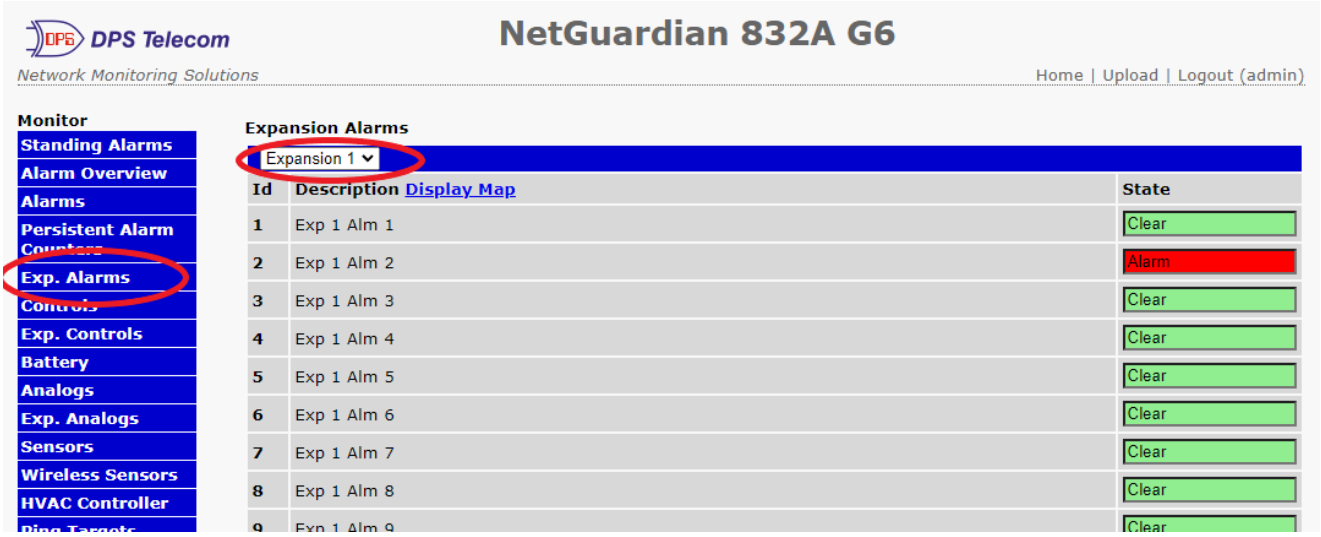
NOTE: A Persistent Alarm Counter will record the number of alarm pulses received on a specified point from the device's display mapping. A pulse is recorded when the point is set from a clear state.

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

7.5 Expansion Alarms

NOTE: *This menu option does not appear unless an expansion unit has been connected to your base G6.*

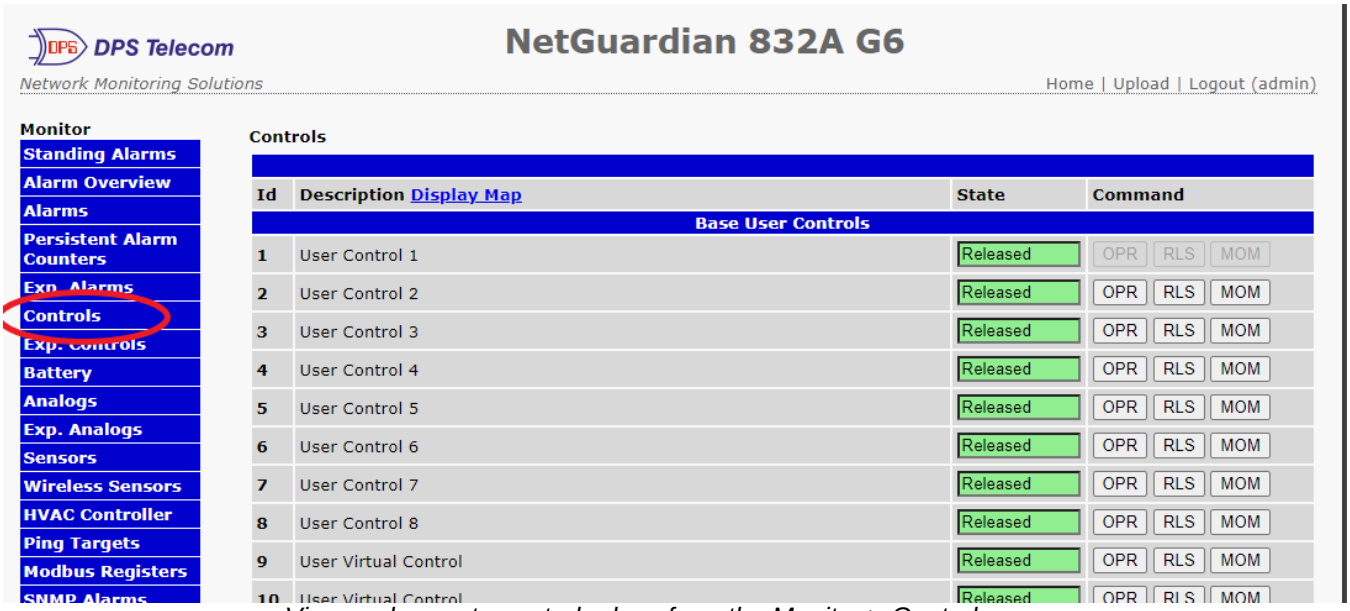
Expansion Alarm Monitoring have the same functionality as Alarms Monitoring. They are added as part of an expansion unit, depending on your expansion configuration you will have the ability to select which expansion alarms to configure via the drop down box. See image below.



7.6 Controls

Use the following rules to operate the G6's control:

1. Select **Controls** (or **Exp. Controls**) from the **Monitor** menu.
2. Under the **State** field, you can see the current condition of the control.
3. To issue the control, click on a command (**OPR** - operate, **RLS** - release, or **MOM** - momentary)



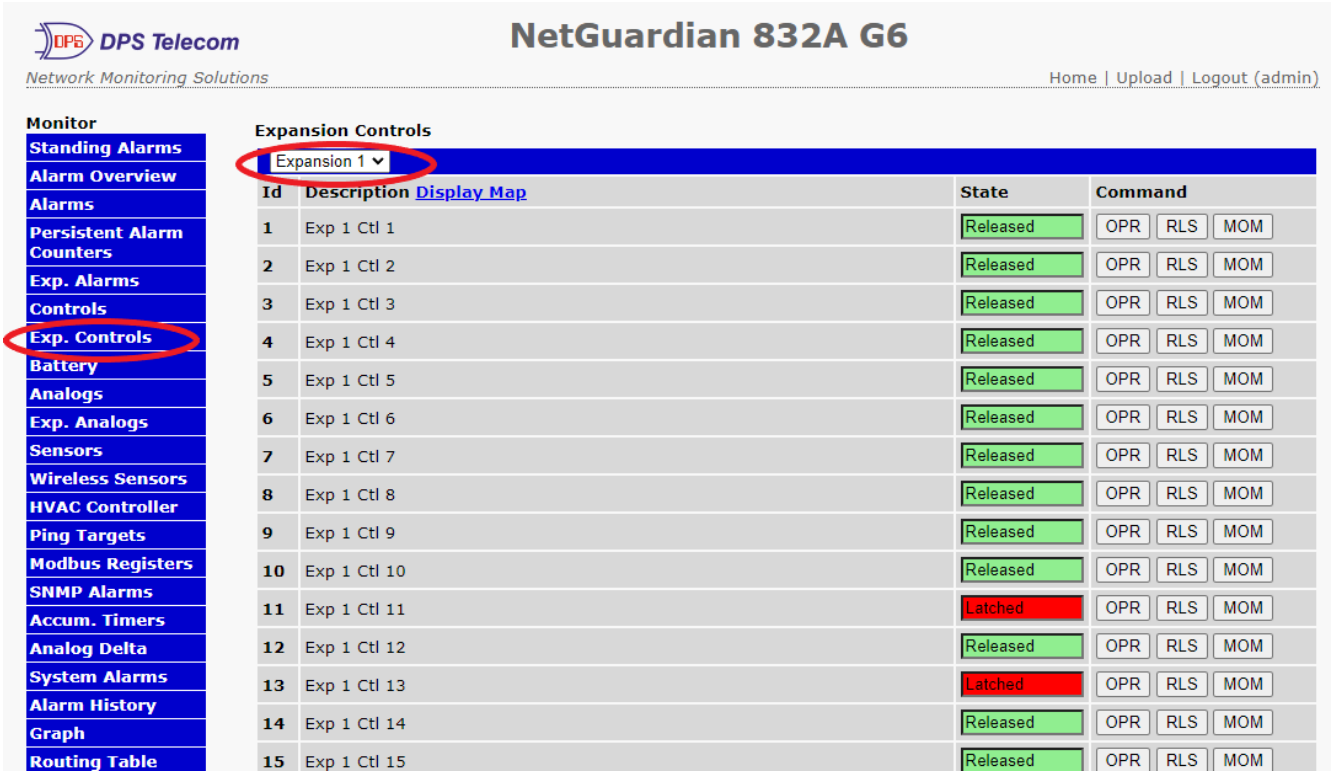
View and operate control relays from the Monitor > Controls menu

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

7.7 Expansion Controls

NOTE: *This menu option does not appear unless an expansion unit has been connected to your base G6.*

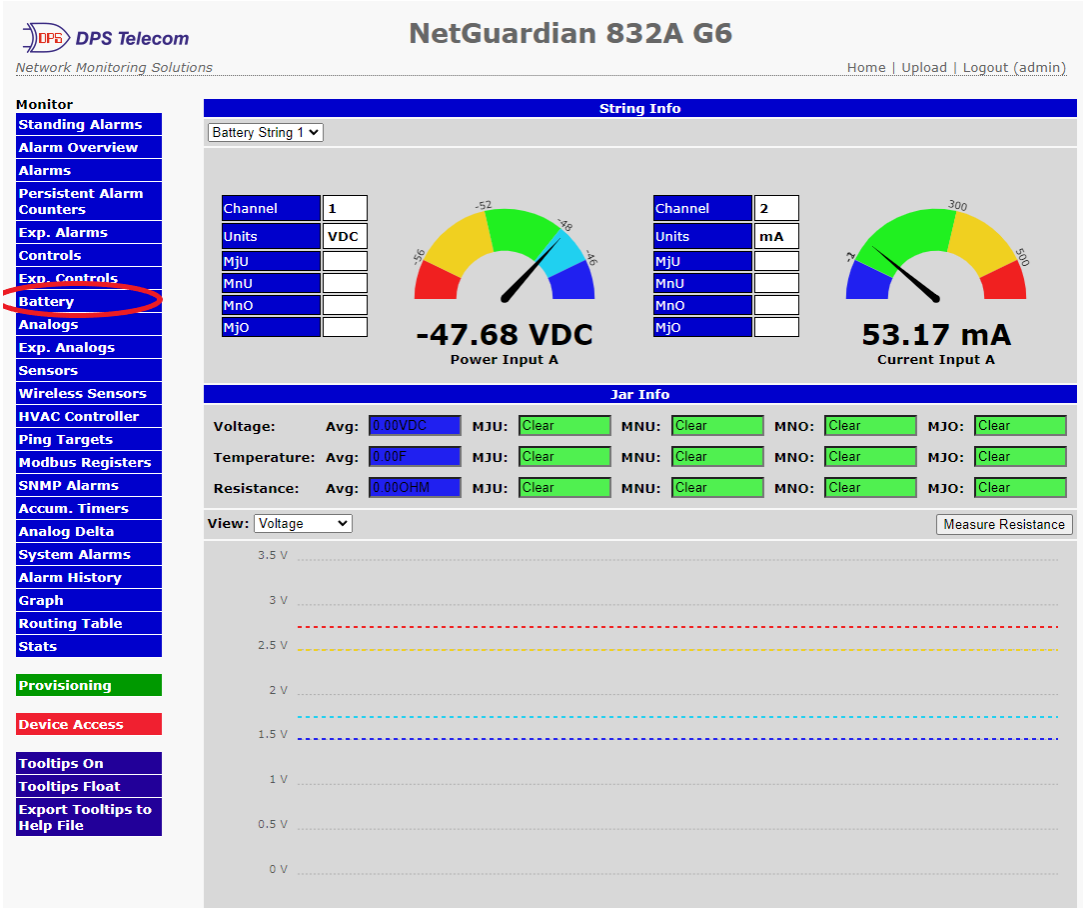
Expansion Controls Monitoring have the same functionality as Controls Monitoring. They are added as part of an expansion unit, such as the NetGuardian E16 DX G2, which extends your available quantity of control relays. Depending on your expansion configuration you will have the ability to select which expansion controls to monitor via the drop down box. See image below.



7.8 Battery

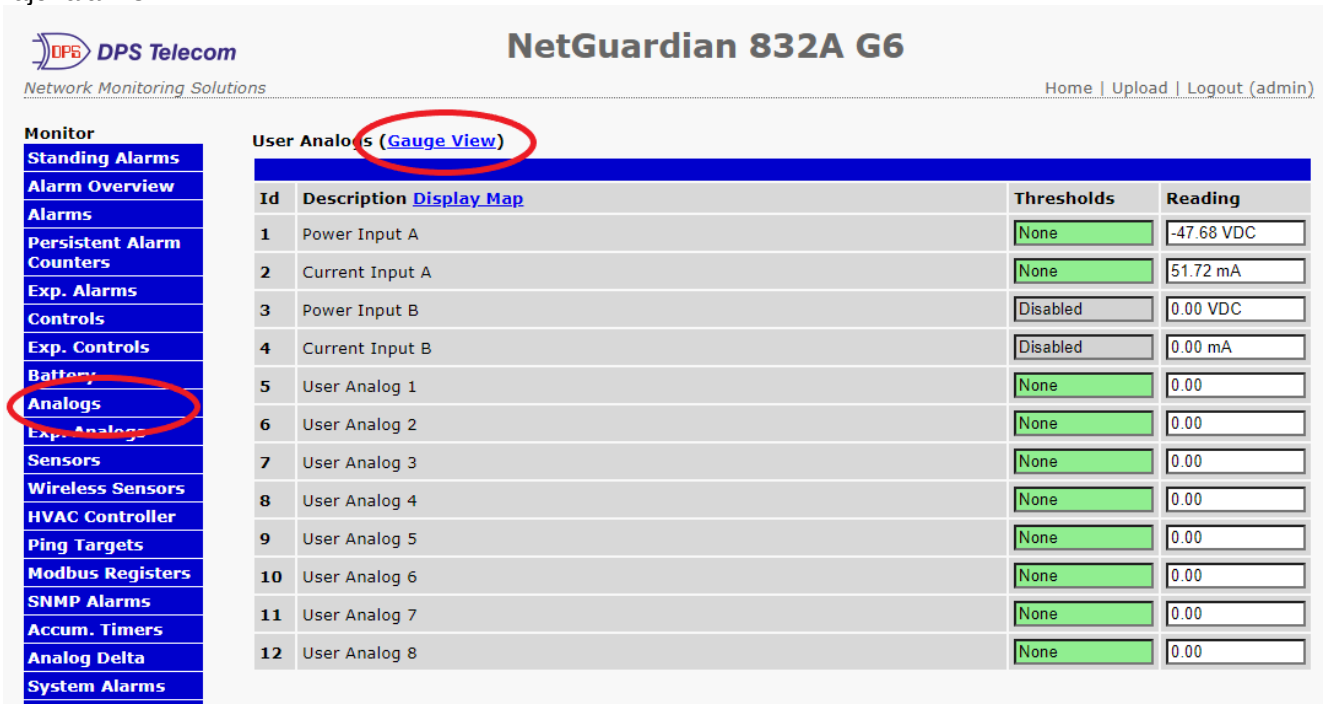
Monitoring Your Batteries from the G6 web interface

1. In the “Monitoring” menus of the G6 web interface (blue), you may view the status of your battery strings at any time.
2. You may choose to view a graph of each jar’s temperature, voltage, internal ohmic resistance, or a combined view of multiple readings simultaneously.
3. If you see a bar in any color other than green (which will be above/below a dotted horizontal threshold line of the same color), that jar is in an alarm state (either major or minor, either over or under the “normal” range you configured in the Provisioning menu earlier).
4. You may click any bar to view a graph of the last 30 days of readings. This can help you distinguish sudden changes from a gradual deterioration.

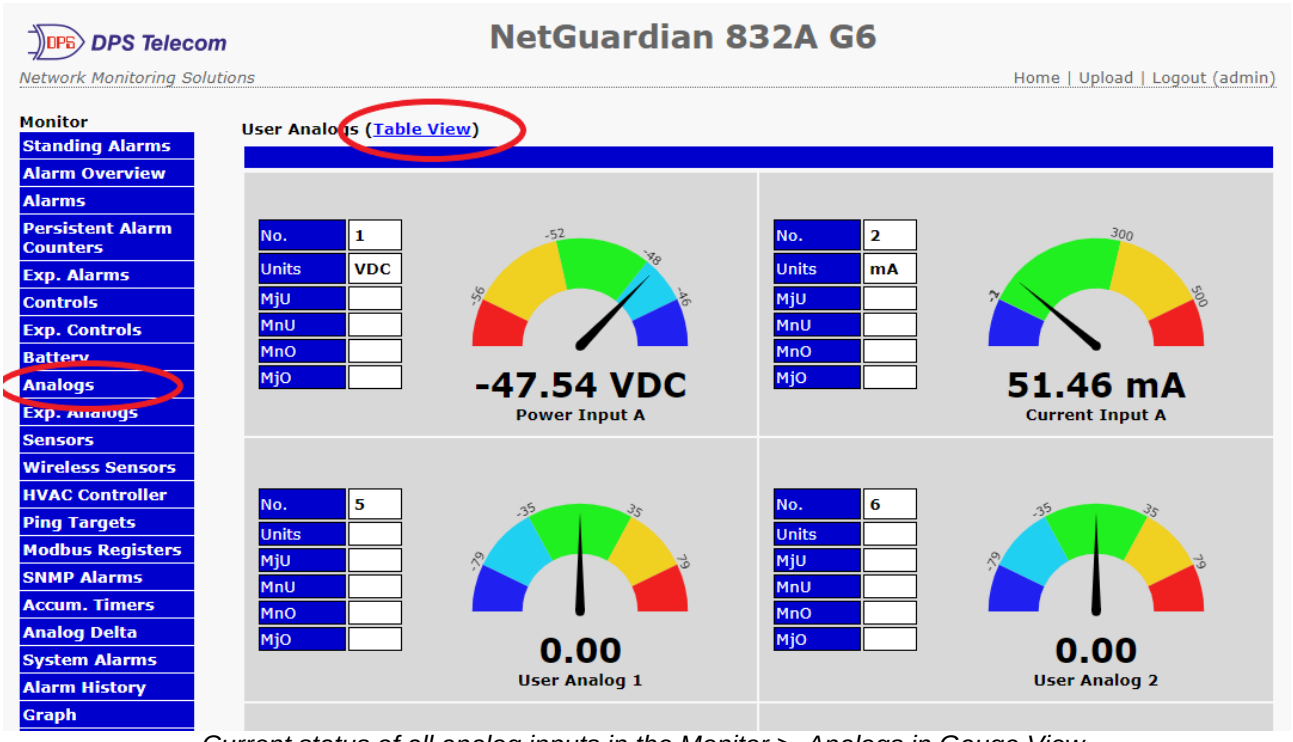


7.9 Analogs

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



Current status of all analog inputs in the Monitor > Analogs in Table View.



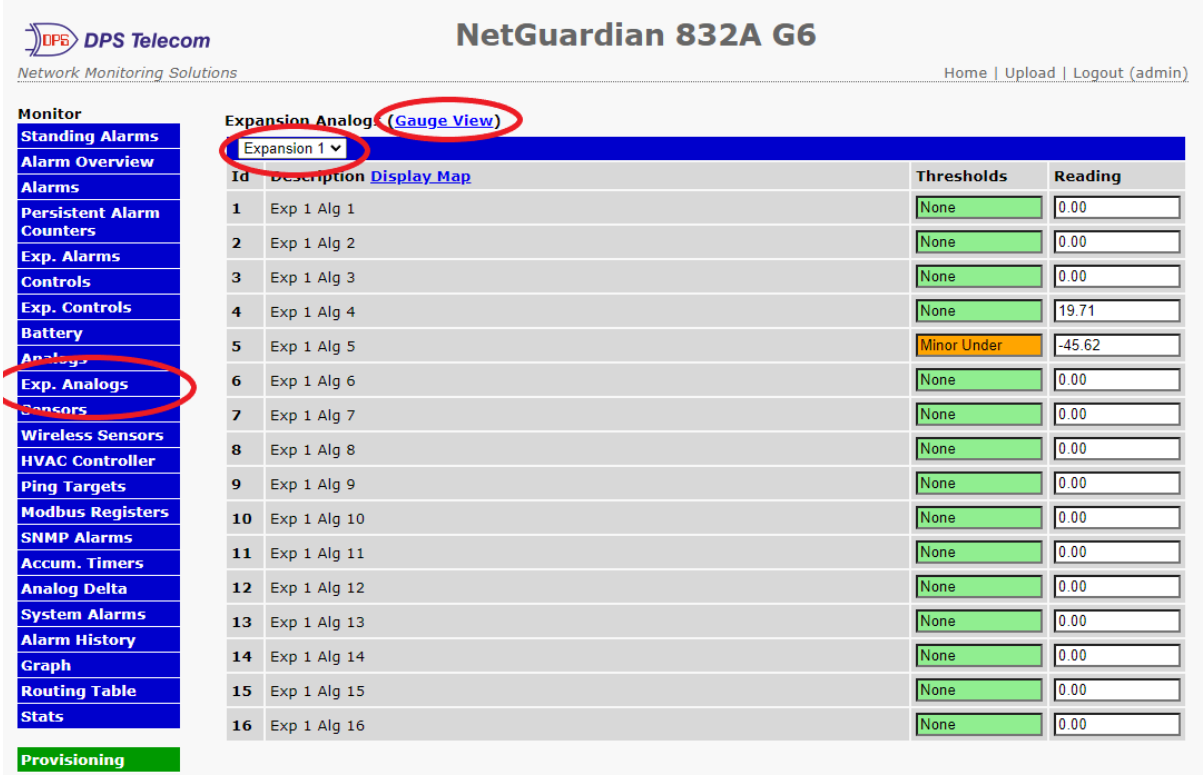
Current status of all analog inputs in the Monitor > Analogs in Gauge View.

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

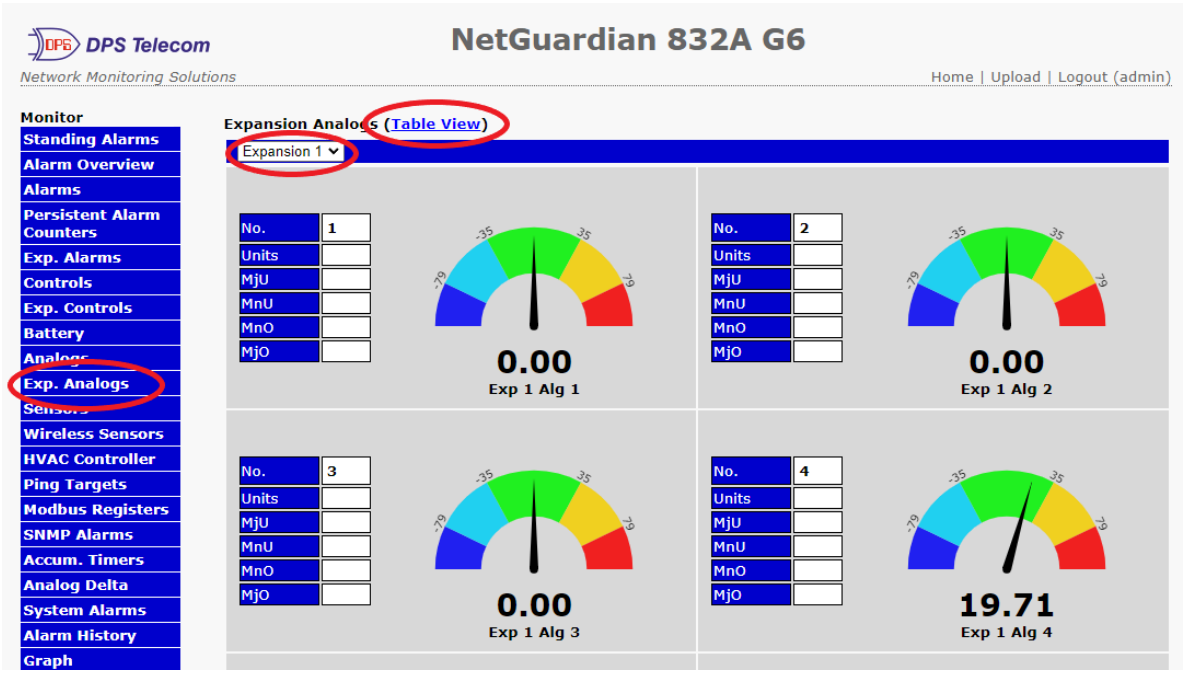
7.10 Expansion Analogs

NOTE: *This menu option does not appear unless an expansion unit has been connected to your base G6.*

Expansion Analogs Monitoring have the same functionality as Analogs Monitoring. They are added as part of an expansion unit. When available, they will appear on this additional page of user analogs. Depending on your expansion configuration you will have the ability to select which expansion controls to configure via the drop down box. See image below.



Current status of all analog inputs in the Monitor > Exp. Analogs in Table View.

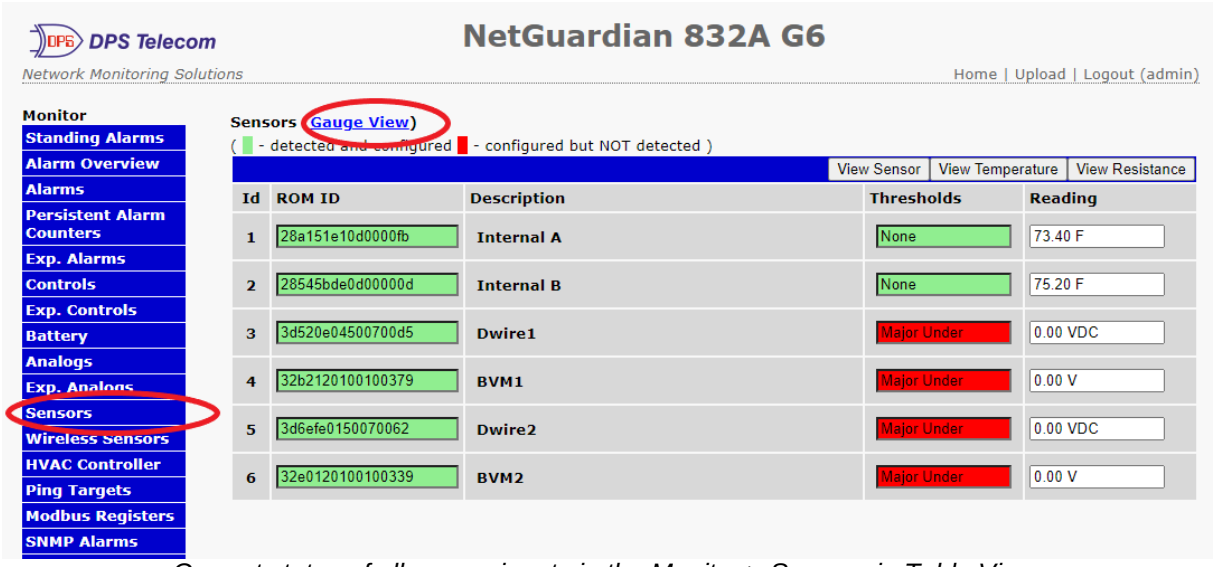


Current status of all analog inputs in the Monitor > Exp. Analogs in Gauge View.

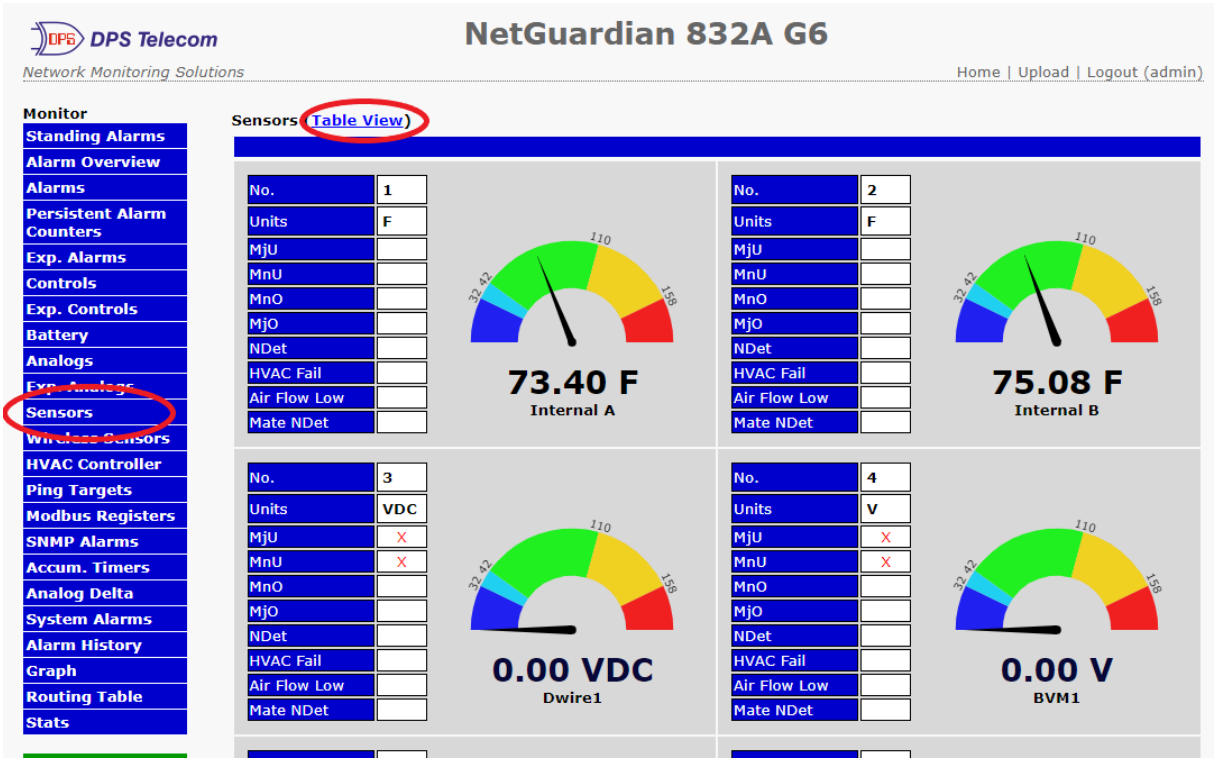
NOTE: The analog gauges do not account for the user definable Deadband. This may result in an alarm threshold to appear crossed in the gauge animation when the point has not set or cleared.

7.11 Sensors

This selection provides the status of the system's sensors by indicating if an alarm has been triggered. The **Monitor** > **Sensors** screen provides a description of each sensor, 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 sensor values will be displayed as a graphical gauge. Selecting **Table View** will display a non-graphical interface of your values.



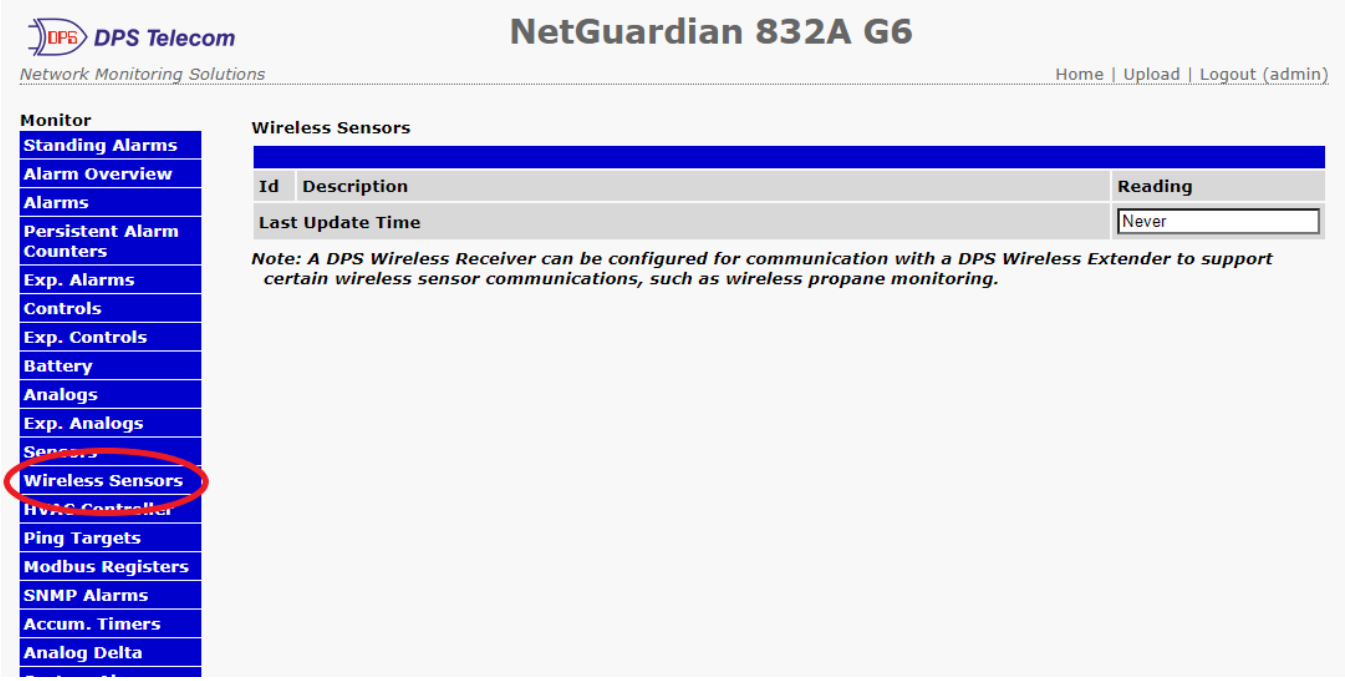
Current status of all sensor inputs in the Monitor > Sensors in Table View.



Current status of all sensor inputs in the Monitor > Sensors in Gauge View.

7.12 Wireless Sensors

Monitor current status of a paired wireless receiver or extender and associated analog inputs.

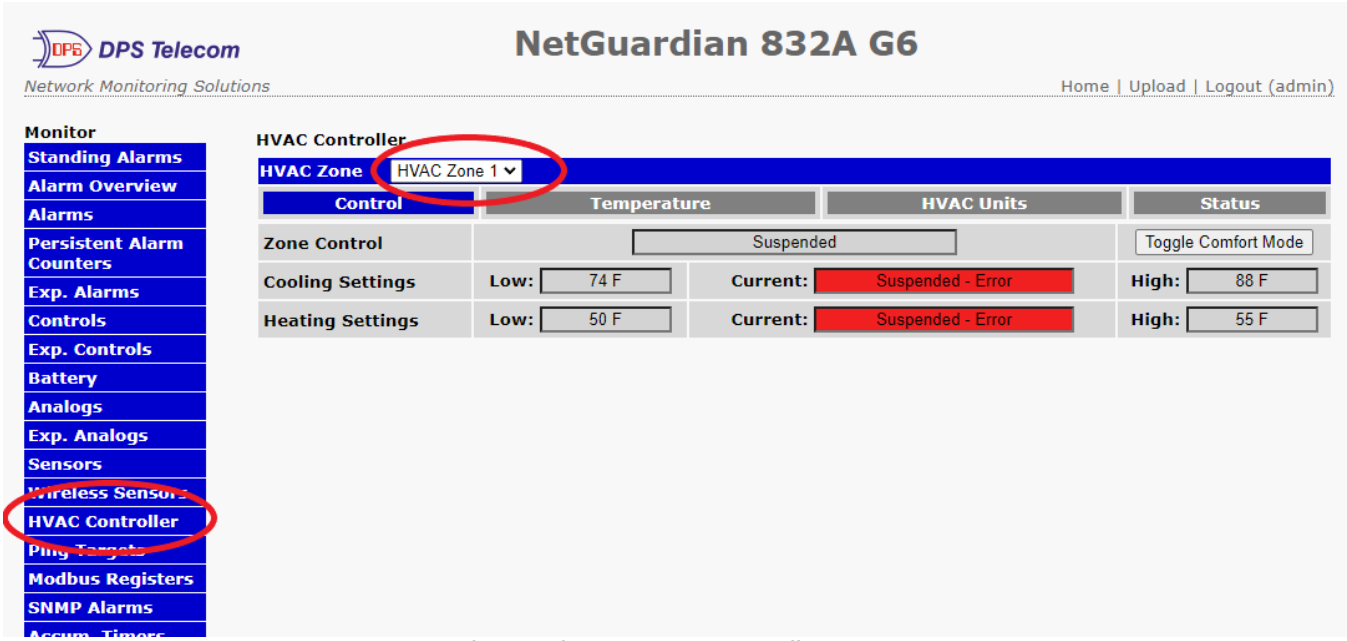


The Monitor > Wireless Sensor menu

7.13 HVAC Controller

The **HVAC Controller** in the Monitoring menu gives you a quick overview of the status of your G6. The Control, Temperature, HVAC Units, and Status views can be toggled between show or hide.

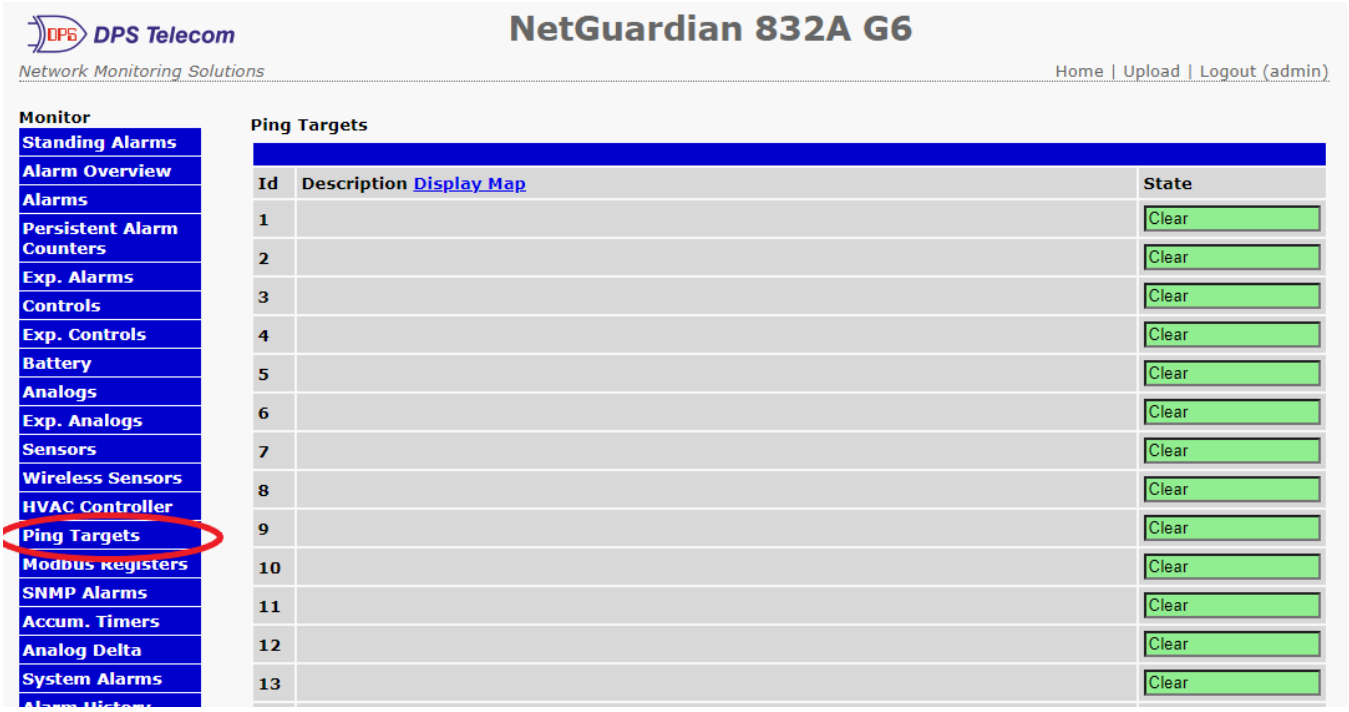
In the event that your G6 is unable to read the temperature sensors, a warning message "Using Internal Temp Sensor as Ambient" will appear.



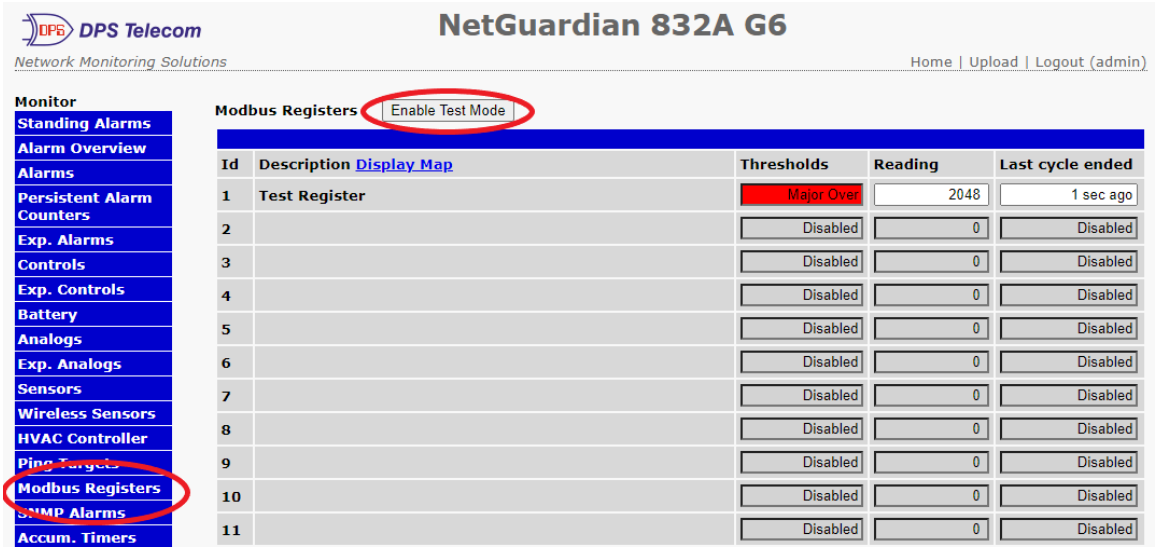
The Monitor > HVAC Controller menu

7.14 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.



7.15 Modbus Registers

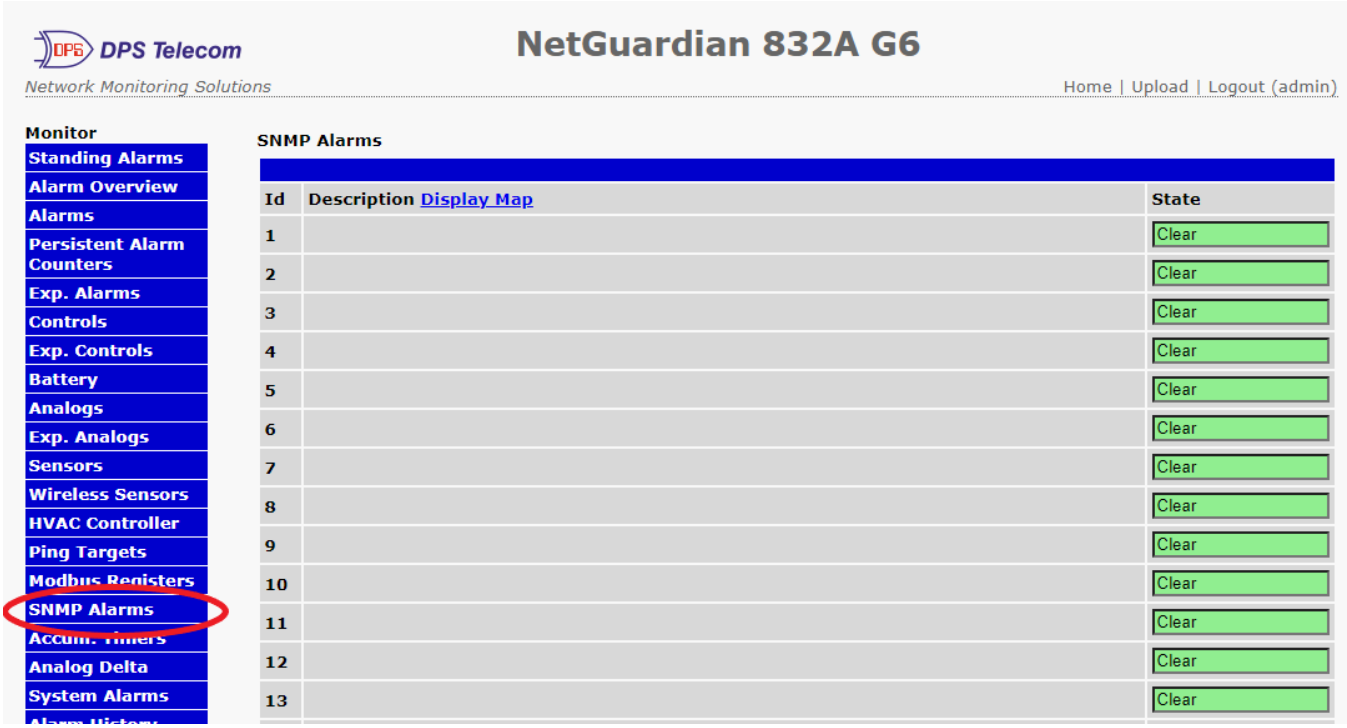


Monitor > MODBUS Registers

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

7.16 SNMP Alarms

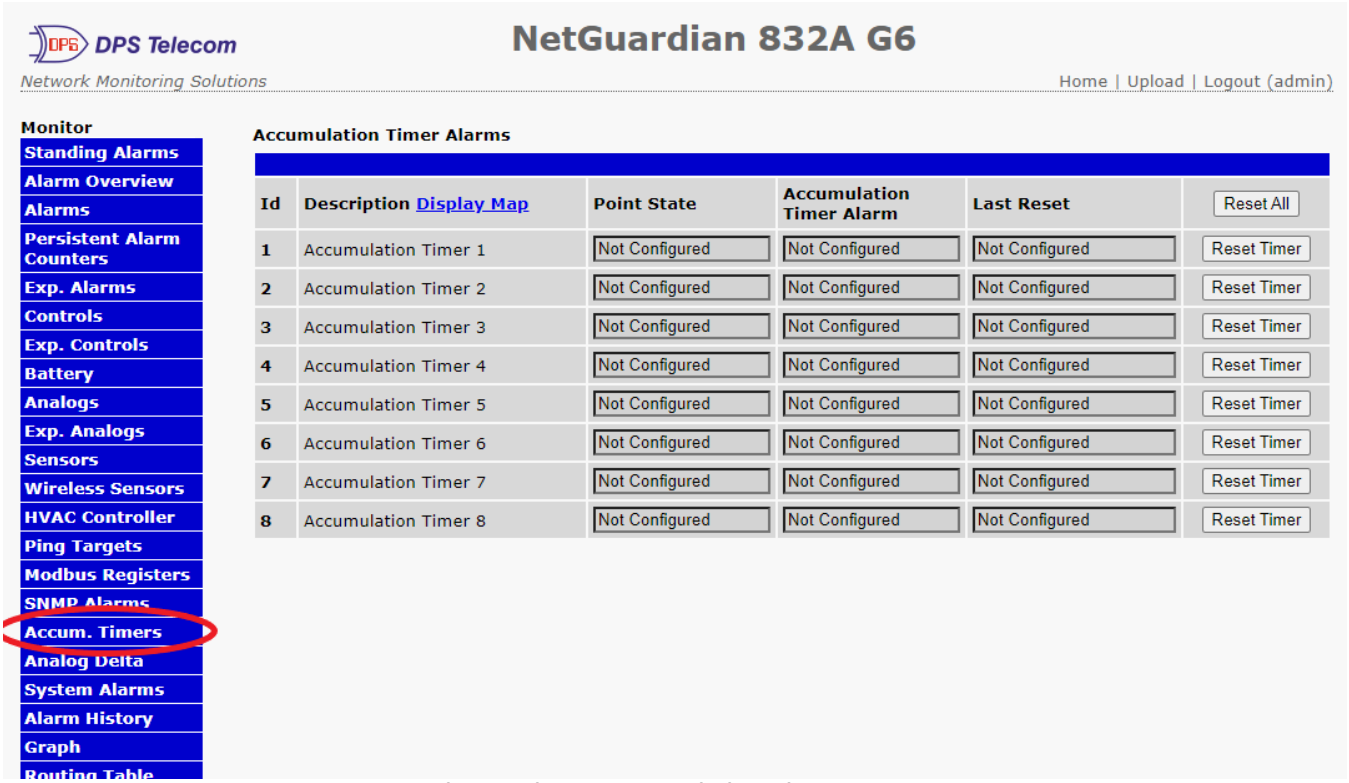
This selection provides the status of the SNMP Alarms by indicating if an alarm has been triggered. Under the **State** column, the status will appear in red if an alarm has been activated. The status will be displayed in green when the alarm condition is not present.



The Monitor > SNMP Alarms menu

7.17 Accumulation Timers

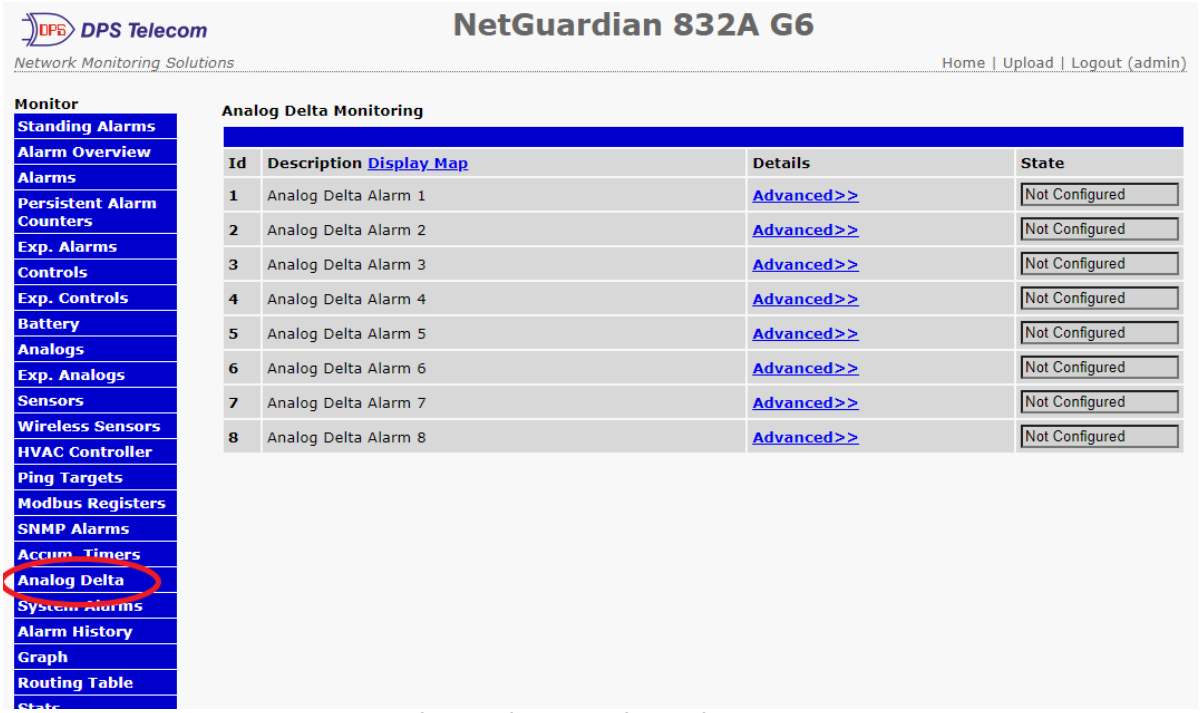
On the **Monitor > Accum. Timers** menu, monitor accumulated time in alarm state for configured alarm points



The Monitor > Accumulation Timers menu

7.18 Analog Delta

On the **Monitor > Analog Delta** menu, monitor configured analog or sensor channels for rapid changes in input value.

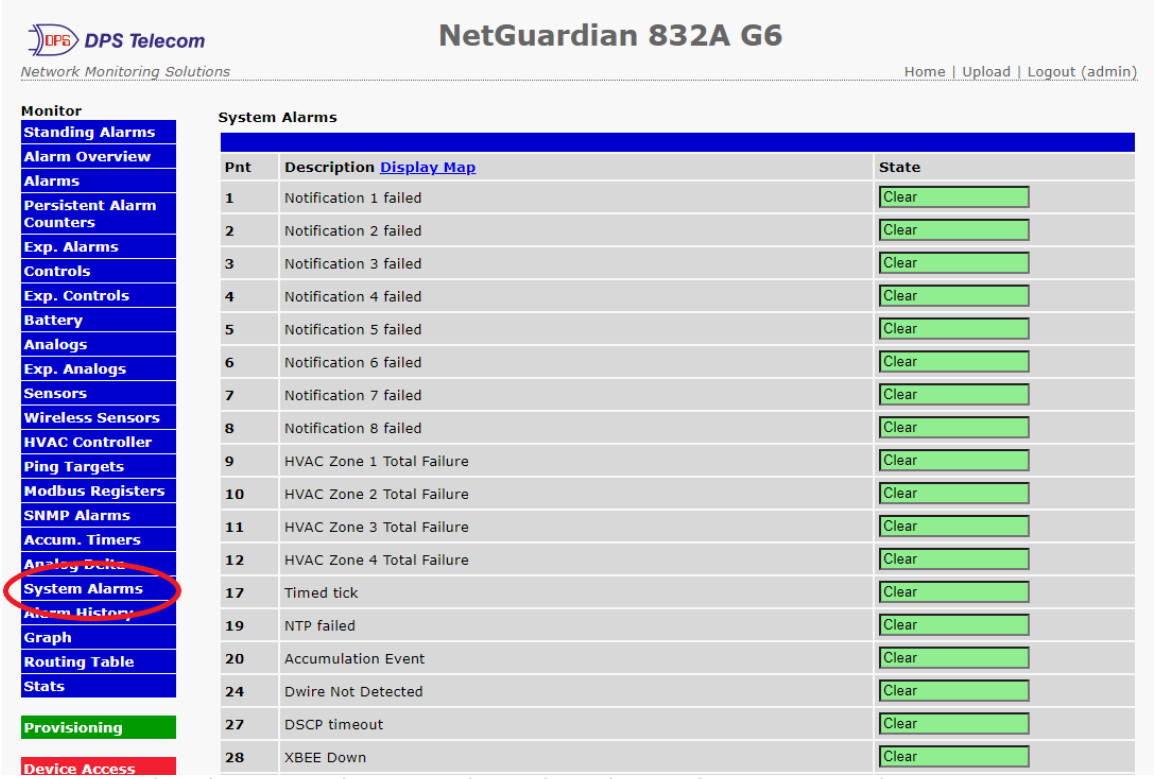


The Monitor > Analog Delta menu

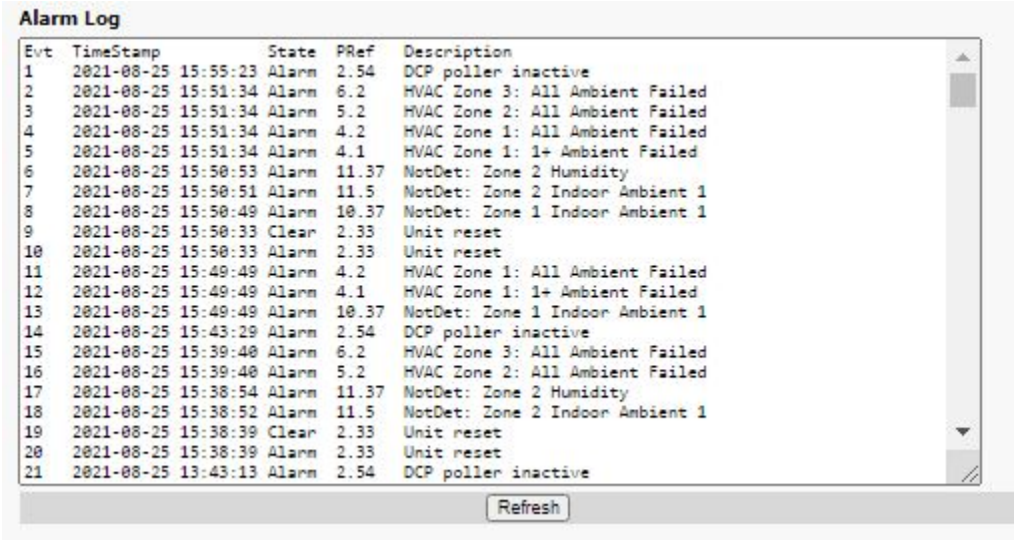
7.19 System Alarms

System alarms are non-editable, housekeeping alarms that are programmed into G6. 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 "Reference" > "System Alarms" in this manual for a complete description of each system alarm.



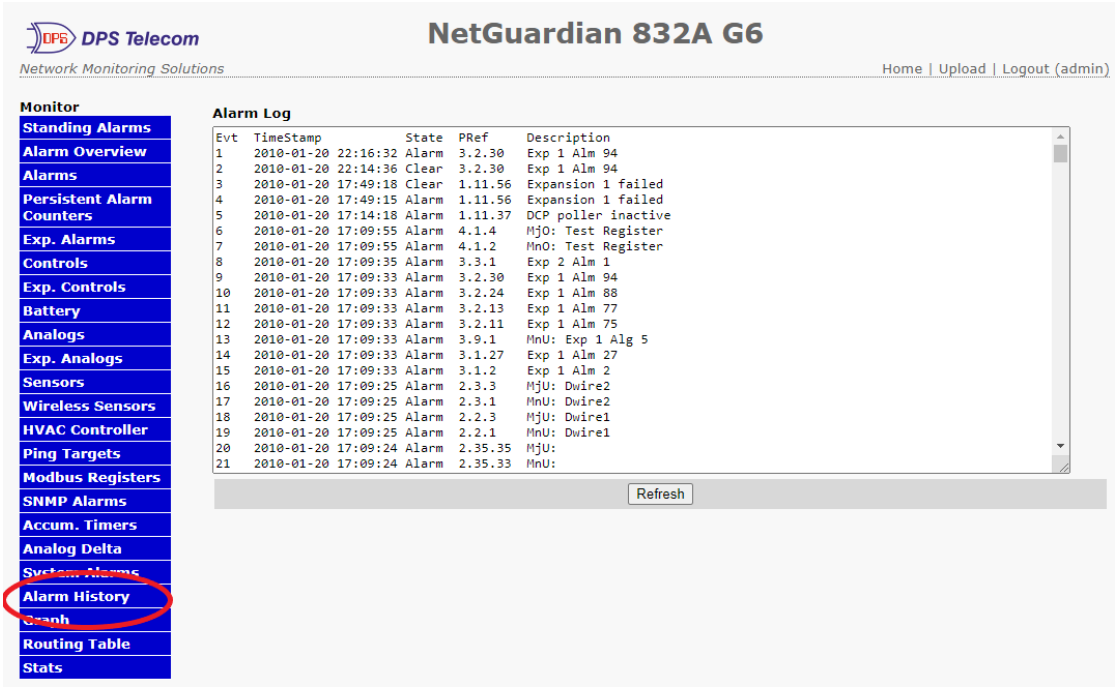
View the status of System Alarms from the Monitor > System Alarms menu.



Monitor > Alarm History menu

7.20 Alarm History

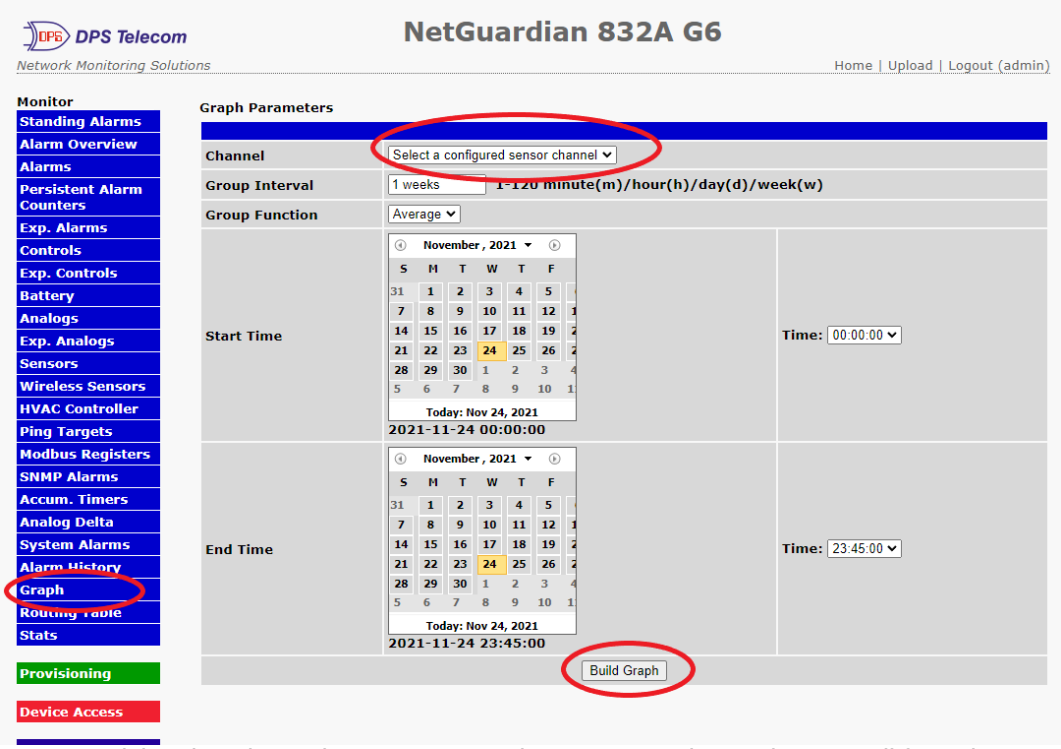
The **Monitor** > **Alarm History** screen provides the historical status of any and all alarms that have been triggered as well as when they are cleared.



Monitor > Alarm History menu

7.21 Graph

The Graph section of the monitor menu lets you build a graph of past sensor measurements, which gives you a visual indication of data over time and points out trending values. To create your Graph, specify the Channel (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."



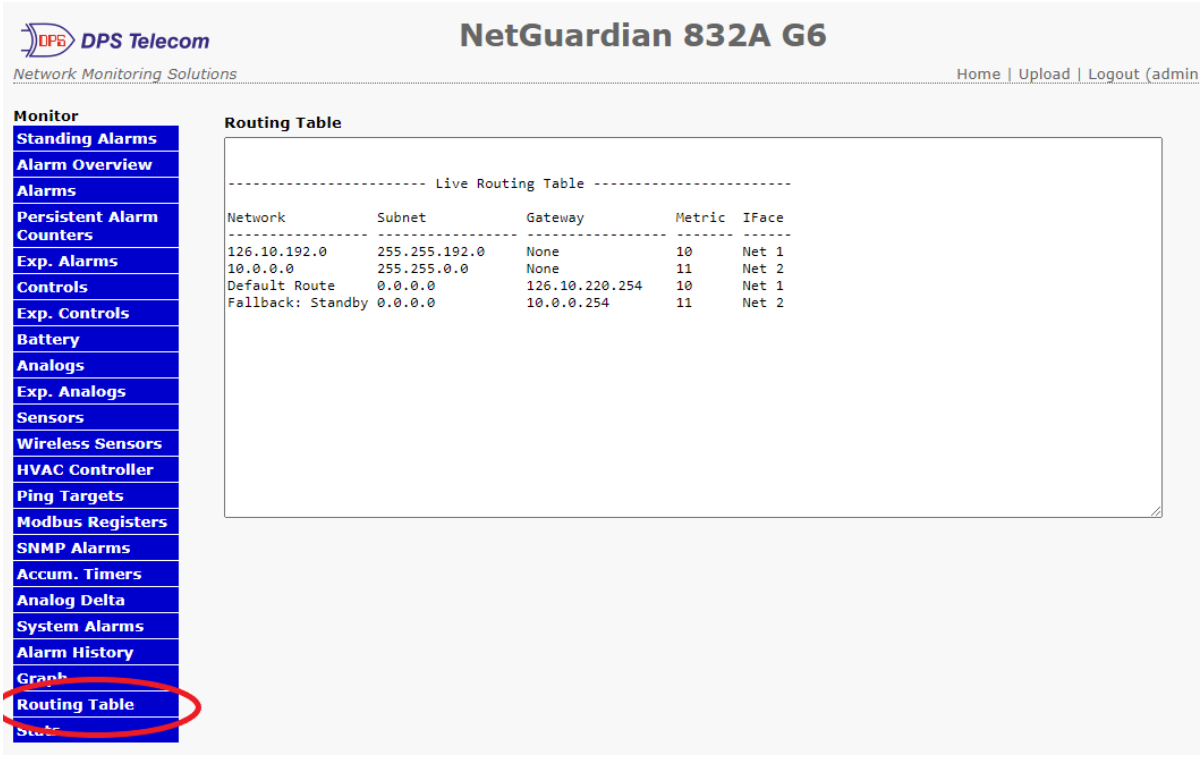
Provision the Channels, Group Interval, Group Function and more - all from the Graph Parameters section of the web browser interface.

Your graph will appear on the next screen. This graph is dynamic 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.

7.22 Routing Table

Monitor > Routing Table

The routing table shows which route the G6 is connected to based on the ethernet settings, static routes, and user metrics assigned within the **Provisioning** > **Ethernet** menu.



View the G6's routing table from the Monitor > Routing Table menu.

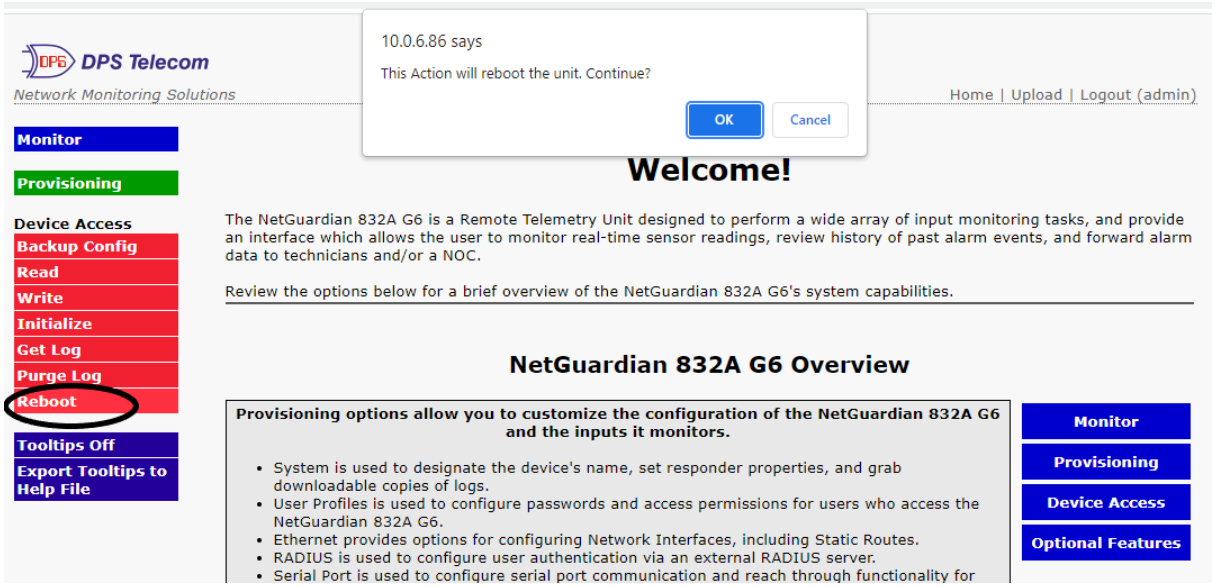
8 Device Access Menu

8.1 Rebooting the NetGuardian

Rebooting the the NetGuardian unit maybe necessary after writing changes to the NVRAM. The window footer will display the text **Reboot Needed** if a reboot is necessary to initiate changes.

To Reboot the unit follow these steps:

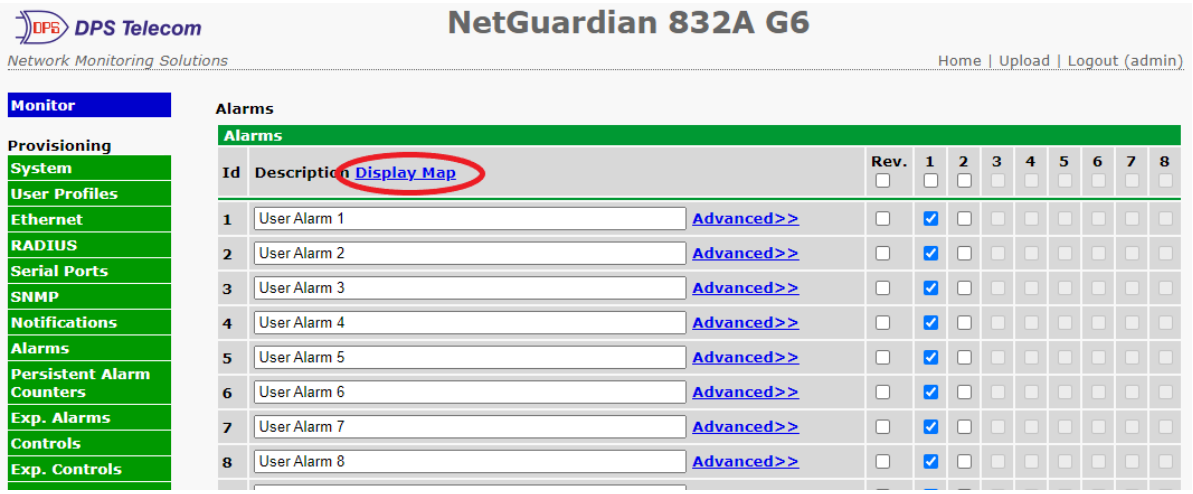
1. Click on the **Reboot** link from the **Device Access** menu
2. A prompt "This Action will reboot the unit. Continue?"
3. Click OK to reboot the unit, Click Cancel to cancel the operation.



9 Appendixes

9.1 Appendix A — Display Mapping

Display mapping can be accessed throughout various parts of the web interface. Access the display mapping by clicking on the hyperlink labeled "Diplay Map" (see image below).
This is just the first part of the reference table, which would cover dozens of printed pages. To keep this manual to a manageable length, and to allow for dynamic updates based on build options purchased, only a few selected sections are presented here.



The Display Map that is visible from many points of the web interface, covers every alarm in the G6, including:

- Discrete alarms
- Analog thresholds
- HVAC controls
- Ping Targets 1-32
- Accumulation Timers
- MODBUS Registers

Here is an example of what you will see:

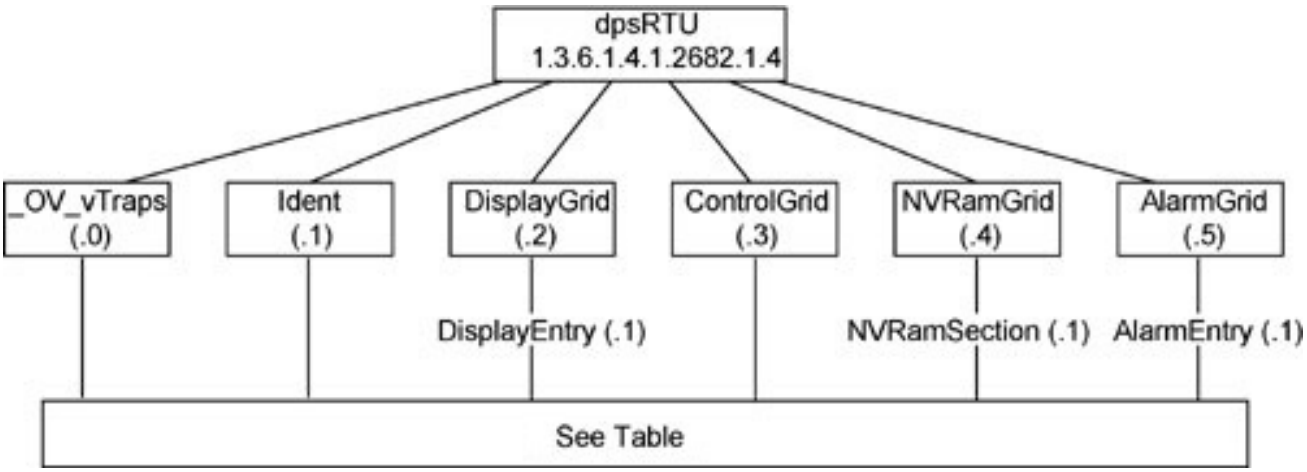
Port	Address	Display	Point	Description	Trap (Set, Clear)	Description Get OID	State Get OID
99	1	1	**1-32**	Discrete Alarms **1-32**	Set: 8001-8032 Clear: 9001-9032	.1.3.6.1.4.1.2682.1.2.5.1.5.99.1.1.**{1-32}**	.1.3.6.1.4.1.2682.1.2.5.1.6.99.1.1.**{1-32}**
99	1	11	24	Dwire not Detected	Set: 8664 Clear: 9664	.1.3.6.1.4.1.2682.1.2.5.1.5.99.1.11.24	.1.3.6.1.4.1.2682.1.2.5.1.6.99.1.11.24
99	1	11	28	XBee Down	Set: 8668 Clear: 9668	.1.3.6.1.4.1.2682.1.2.5.1.5.99.1.11.28	.1.3.6.1.4.1.2682.1.2.5.1.6.99.1.11.28
99	1	11	38	Net 1 Down	Set: 8678 Clear: 9678	.1.3.6.1.4.1.2682.1.2.5.1.5.99.1.11.38	.1.3.6.1.4.1.2682.1.2.5.1.6.99.1.11.38
99	1	11	39	Net 2 Down	Set: 8679 Clear: 9679	.1.3.6.1.4.1.2682.1.2.5.1.5.99.1.11.39	.1.3.6.1.4.1.2682.1.2.5.1.6.99.1.11.39

Table A.1. Small excerpt of *alarm point Displays/Points and System Alarms Trap numbers for the G6.*

* The number ranges shown in these reference tables cover every integer in the range. For example, the SNMP Trap "Set" number for alarm 1 (in Display 1) is 8001, "Set" for alarm 2 is 8002, "Set" for alarm 3 is 8003, etc.

9.2 Appendix B — 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. Table B.1 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 1.3.6.1.4.1.2682.1.4. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the Control Grid is 1.3.6.1.4.1.2682.1.4.3.3 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 (1.3.6.1.4.1.2682.1.4.0)
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 (1.3.6.1.4.1.2682.1.4.1)
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 (1.3.6.1.4.1.2682.1.4.2.1)
Port (.1)
Address (.2)
Display (.3)
DispDesc (.4)*
PntMap (.5)*

Tbl. B3 (.3) ControlGrid points
ControlGrid (1.3.6.1.4.1.2682.1.4.3)
Port (.1)
Address (.2)
Display (.3)
Point (.4)
Action (.5)

Tbl. B5 (.5) AlarmEntry points
AlarmEntry (1.3.6.4.1.2682.1.4.5.1)
Aport (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)
APntDesc (.5)*
AState (.6)
* For specific alarm points, see Table B6

	Description	Port	Address	Display	Points
Disp 1	Discrete Alarms	99	1	1	1-32
	Undefined**	99	1	1	33-64
Disp	Ping Targets	99	1	2	1-32

2	Undefined**	99	1	2	33-64
Disp 3	Analog 1	99	1	3	1-4
	Undefined**	99	1	3	5-64
Disp 4	Analog 2	99	1	4	1-4
	Undefined**	99	1	4	5-64
Disp 5	Analog 3	99	1	5	1-4
	Undefined**	99	1	5	5-64
Disp 6	Analog 4	99	1	6	1-4
	Undefined**	99	1	6	5-64
Disp 7	Analog 5	99	1	7	1-4
	Undefined**	99	1	7	5-64
Disp 8	Analog 6	99	1	8	1-4
	Undefined**	99	1	8	5-64
Disp 9	Analog 7	99	1	9	1-4
	Undefined**	99	1	9	5-64
Disp 10	Analog 8	99	1	10	1-4
	Undefined**	99	1	10	5-64
Disp 11	Relays 1-8	99	1	11	1-8
	Relays 9-16	99	1	11	9-16
	Timed Tick	99	1	11	17
	Exp. Module Callout	99	1	11	18
	Network Time Server	99	1	11	19
	Accumulation Event	99	1	11	20
	Duplicate IP Address	99	1	11	21
	WAN Disconnected	99	1	11	22
	ECU EmergencyUnlock	99	1	11	23
	D-Wire Sensor Not Detected	99	1	11	24
	Undefined	99	1	11	25-26
	DSCP Timeout	99	1	11	27
	Wireless Sensor Power Fault	99	1	11	28
	Wireless Sensor Power Low	99	1	11	29
	Undefined**	99	1	11	30-32
	Unit Reset	99	1	11	33
	Undefined**	99	1	11	34-35
	Lost	99	1	11	36
	DCP poll inactive	99	1	11	37
	NET 1 not active	99	1	11	38
	NET 2 not active	99	1	11	39
	NET link down	99	1	11	40

	Modem not	99	1	11	41
	No dial-tone	99	1	11	42
	SNMP trap not	99	1	11	43
	Pager Que	99	1	11	44
	Notification	99	1	11	45
	Craft RCVQ full	99	1	11	46
	Modem RCVQ	99	1	11	47
	Data 1-8 RCVQ	99	1	11	48-55
	NGDdx 1-3 fail	99	1	11	56-58
	GLD/BSU 1-3 fail	99	1	11	59-61
	CHAN timeout	99	1	11	62
	CRFT timeout	99	1	11	63

Table B.6. *Alarm Point Descriptions*

* "No data" indicates that the alarm point is defined but there is no description entered.
** "Undefined" indicates that the alarm point is not used.

9.3 Appendix C — SNMP Granular Trap Packets

Tables C.1 and C.2 provide a list of the information contained in the SNMP Trap packets sent by the NetGuardian.

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)

OR

2. The SNMP manager reads the description from the Trap.

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

Table C.1. *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 216 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

Table C.2. *SNMP Headers and descriptions*

9.4 Appendix D — ASCII Conversion

The information contained in Table D.1 is a list of ASCII symbols and their meanings. Refer to the bulleted list below to interpret the ASCII data transmitted or received through the data ports. Port transmit and receive activity can be viewed from the Web Browser Interface.

- Printable ASCII characters will appear as ASCII.
- Non-printable ASCII characters will appear as labels surrounded by { } brackets (e.g. **{NUL}**).
- Non-ASCII characters will appear as hexadecimal surrounded by [ ] brackets (e.g. **[IF]**).
- A received BREAK will appear as <BRK>.

Abbreviation	Description	Abbreviation	Description
NUL	Null	DLE	Data Link Escape
SOH	Start of Heading	DC	Device Control
STX	Start of Text	NAK	Negative Acknowledge
ETX	End of Text	SYN	Synchronous Idle
EOT	End of Transmission	ETB	End of Transmission Block
ENQ	Enquiry	CAN	Cancel
ACK	Acknowledge	EM	End of Medium
BEL	Bell	SUB	Substitute
BS	Backspace	ESC	Escape
HT	Horizontal Tabulation	FS	File Separator
LF	Line Feed	GS	Group Separator
VT	Vertical Tabulation	RS	Record Separator
FF	Form Feed	US	Unit Separator
CR	Carriage Return	SP	Space (blank)
SO	Shift Out	DEL	Delete
SI	Shift In	BRK	Break Received

Table D.1. *ASCII symbols*

9.5 Appendix E - RADIUS Dictionday File (Available on Resource Disk)

```
# -*- text -*-
#
# dictionary.dps
#
#         DPS Telecom, Inc
#         For assistance or support, please contact support@dpstele.com
#                         v1.0 Released - 1/23/09 (CBH/DPS)

VENDOR              DPS                         2682

#
# Standard attribute for NetGuardian RTU.
# All values are integer with 1 = True, 0 = False.
# If attribure does not exist in Access-Accept packet, default value will be 0.
#
BEGIN-VENDOR        DPS

ATTRIBUTE   dps-admin                           1       integer
ATTRIBUTE   dps-edit                                    2       integer
ATTRIBUTE   dps-monitor                         3       integer
ATTRIBUTE   dps-SD-monitor                              4       integer
#To allow monitor of data port buffer/activity
ATTRIBUTE   dps-reach-through                   5       integer
#To allow proxy to serial ports via TTY interface
ATTRIBUTE   dps-telnet                          6       integer
#To allow telnet in and out of NetGuardian
ATTRIBUTE   dps-control                         7       integer
#To allow manipulation of dry contact relay outputs
ATTRIBUTE   dps-modem                           8       integer
#To allow dial in and out of NetGuardian
ATTRIBUTE   dps-ppp                                     9       integer
#To allow this user PPP (inbound) access to the NetGuardian

END-VENDOR          DPS
```

9.6 Appendix F - Modbus Registers

Function Code	Action
1	Coil Status (Reads the current status of Relays)
2	Input Status (Reads the current status of Discrete Alarms)
3	Holding Register (Returns the raw value and control of Analogs)
4	Input Register (Returns the raw value and control of Analogs)
5	Write Single Coil (Changes the state of the Relays)

Function Code	Register	Description
1	0-7	Relay 1-8

Function Code	Register	Description
2	0-31	Discrete Alarm 1-32 **(NetGuardian 832A)**
2	0-63	Discrete Alarm 1-64 **(NetGuardian 864A)**

Function Code	Register	Description	Scaling	Bits
3	0	Analog 1 Value	*	16
3	1	Analog 1 Scaling Range	*	1/16-3/16
3	1	Analog 1 Sign	*	7/16
3	2	Analog 2 Value	*	16
3	3	Analog 2 Scaling Range	*	1/16-3/16
3	3	Analog 2 Sign	*	7/16
3	4	Analog 3 Value	*	16
3	5	Analog 3 Scaling Range	*	1/16-3/16
3	5	Analog 3 Sign	*	7/16
3	6	Analog 4 Value	*	16
3	7	Analog 4 Scaling Range	*	1/16-3/16
3	7	Analog 4 Sign	*	7/16
3	8	Analog 5 Value	*	16
3	9	Analog 5 Scaling Range	*	1/16-3/16
3	9	Analog Sign	*	7/16
3	10	Analog 6 Value	*	16
3	11	Analog 6 Scaling Range	*	1/16-3/16
3	11	Analog 6 Sign	*	7/16
3	12	Analog 7 Value	*	16
3	13	Analog 7 Scaling Range	*	1/16-3/16
3	13	Analog 7 Sign	*	7/16

Function Code	Register	Description	Scaling	Bits
3	14	Analog 8 Value	*	16
3	15	Analog 8 Scaling Range	*	1/16-3/16
3	15	Analog 8 Sign	*	7/16

*** See Scaling Range Table Below**

Function Code	Register	Description	Scaling	Bits
4	0	Analog 1 Value	*	16
4	1	Analog 1 Scaling Range	*	1/16-3/16
4	1	Analog 1 Sign	*	7/16
4	2	Analog 2 Value	*	16
4	3	Analog 2 Scaling Range	*	1/16-3/16
4	3	Analog 2 Sign	*	7/16
4	4	Analog 3 Value	*	16
4	5	Analog 3 Scaling Range	*	1/16-3/16
4	5	Analog 3 Sign	*	7/16
4	6	Analog 4 Value	*	16
4	7	Analog 4 Scaling Range	*	1/16-3/16
4	7	Analog 4 Sign	*	7/16
4	8	Analog 5 Value	*	16
4	9	Analog 5 Scaling Range	*	1/16-3/16
4	9	Analog 5 Sign	*	7/16
4	10	Analog 6 Value	*	16
4	11	Analog 6 Scaling Range	*	1/16-3/16
4	11	Analog 6 Sign	*	7/16
4	12	Analog 7 Value	*	16
4	13	Analog 7 Scaling Range	*	1/16-3/16
4	13	Analog 7 Sign	*	7/16
4	14	Analog 8 Value	*	16
4	15	Analog 8 Scaling Range	*	1/16-3/16
4	15	Analog 8 Sign	*	7/16

*** See Scaling Range Table Below**

Function Code	Register	Description
5	0-7	Relay 1-8

Function Code	Register	Description
2	1200-1215	NetGuardian E16 DX Expansion 1 Alarm 1-16
1	1300-1315	NetGuardian E16 DX Expansion 1 Relay 1-16
2	1400-1415	NetGuardian E16 DX Expansion 2 Alarm 1-16

Function Code	Register	Description
1	1500-1515	NetGuardian E16 DX Expansion 2 Relay 1-16
2	1600-1615	NetGuardian E16 DX Expansion 3 Alarm 1-16
1	1700-1715	NetGuardian E16 DX Expansion 3 Relay 1-16

Function Code	Register	Description
5	1300-1315	NetGuardian E16 DX Expansion 1 Relay 1-16
5	1500-1515	NetGuardian E16 DX Expansion 2 Relay 1-16
5	1700-1715	NetGuardian E16 DX Expansion 3 Relay 1-16

Function Code	Register	Description
2	1200-1263	NetGuardian 480 (as DX) Alarm 1-64
2	1316-1331	NetGuardian 480 (as DX) Alarm 65-80
1	1300-1303	NetGuardian 480 (as DX) Relay 1-4

Function Code	Register	Description
5	0-7	NetGuardian 480 (as DX) Relay 1-4

Function Code	Register	Description
2	1200-1247	NetGuardian DX48 Expansion 1 Alarm 1-48
1	1300-1307	NetGuardian DX48 Expansion 1 Relay 1-8
2	1400-1447	NetGuardian DX48 Expansion 2 Alarm 1-48
1	1500-1507	NetGuardian DX48 Expansion 2 Relay 1-8
2	1600-1647	NetGuardian DX48 Expansion 3 Alarm 1-48
1	1700-1707	NetGuardian DX48 Expansion 3 Relay 1-8

Function Code	Register	Description
5	1300-1315	NetGuardian DX48 Expansion 1 Relay 1-8
5	1500-1515	NetGuardian DX48 Expansion 2 Relay 1-8
5	1700-1715	NetGuardian DX48 Expansion 3 Relay 1-8

Function Code	Register	Description
2	1200-1231	NetGuardian 832A (as DX)

Function Code	Register	Description
		Expansion 1 Alarm 1-32
1	1300-1307	NetGuardian 832A (as DX) Expansion 1 Relay 1-8
2	1400-1431	NetGuardian 832A (as DX) Expansion 2 Alarm 1-32
1	1500-1507	NetGuardian 832A (as DX) Expansion 1 Relay 1-8
2	1600-1631	NetGuardian 832A (as DX) Expansion 3 Alarm 1-32
1	1700-1707	NetGuardian 832A (as DX) Expansion 1 Relay 1-8

Function Code	Register	Description
2	1200-1263	NetGuardian 864A (as DX) Expansion 1 Alarm 1-64
1	1300-1307	NetGuardian 864A (as DX) Expansion 1 Relay 1-8
2	1400-1463	NetGuardian 864A (as DX) Expansion 2 Alarm 1-64
1	1500-1507	NetGuardian 864A (as DX) Expansion 1 Relay 1-8
2	1600-1663	NetGuardian 864A (as DX) Expansion 3 Alarm 1-64
1	1700-1707	NetGuardian 864A (as DX) Expansion 1 Relay 1-8

Function Code	Register	Description
5	1300-1307	NetGuardian 832/864(as DX) Expansion 1 Relay 1-8
5	1500-1507	NetGuardian 832/864(as DX) Expansion 2 Relay 1-8
5	1700-1707	NetGuardian 832/864(as DX) Expansion 3 Relay 1-8

Function Code	Register	Description	Scaling	Bits
3	100	NetGuardian (832/864 as DX) Expansion 1 Analog 1 Value	*	16
3	101	NetGuardian (832/864 as DX) Expansion 1 Analog 1 Scaling	*	1/16-3/16
3	101	NetGuardian (832/864 as DX) Expansion 1 Analog 1 Sign	*	7/16
3	102	NetGuardian (832/864 as DX) Expansion 1 Analog 2 Value	*	16
3	103	NetGuardian	*	1/16-3/16

Function Code	Register	Description	Scaling	Bits
		(832/864 as DX) Expansion 1 Analog 2 Scaling		
3	103	NetGuardian (832/864 as DX) Expansion 1 Analog 2 Sign	*	7/16
3	104	NetGuardian (832/864 as DX) Expansion 1 Analog 3 Value	*	16
3	105	NetGuardian (832/864 as DX) Expansion 1 Analog 3 Scaling	*	1/16-3/16
3	105	NetGuardian (832/864 as DX) Expansion 1 Analog 3 Sign	*	7/16
3	106	NetGuardian (832/864 as DX) Expansion 1 Analog 4 Value	*	16
3	107	NetGuardian (832/864 as DX) Expansion 1 Analog 4 Scaling	*	1/16-3/16
3	107	NetGuardian (832/864 as DX) Expansion 1 Analog 4 Sign	*	7/16
3	108	NetGuardian (832/864 as DX) Expansion 1 Analog 5 Value	*	16
3	109	NetGuardian (832/864 as DX) Expansion 1 Analog 5 Scaling	*	1/16-3/16
3	109	NetGuardian (832/864 as DX) Expansion 1 Analog 5 Sign	*	7/16
3	110	NetGuardian (832/864 as DX) Expansion 1 Analog 6 Value	*	16
3	111	NetGuardian (832/864 as DX) Expansion 1 Analog 6 Scaling	*	1/16-3/16
3	111	NetGuardian (832/864 as DX)	*	7/16

Function Code	Register	Description	Scaling	Bits
		Expansion 1 Analog 6 Sign		
3	112	NetGuardian (832/864 as DX) Expansion 1 Analog 7 Value	*	16
3	113	NetGuardian (832/864 as DX) Expansion 1 Analog 7 Scaling	*	1/16-3/16
3	113	NetGuardian (832/864 as DX) Expansion 1 Analog 7 Sign	*	7/16
3	114	NetGuardian (832/864 as DX) Expansion 1 Analog 8 Value	*	16
3	115	NetGuardian (832/864 as DX) Expansion 1 Analog 8 Scaling	*	1/16-3/16
3	115	NetGuardian (832/864 as DX) Expansion 1 Analog 8 Sign	*	7/16

*** See Scaling Range Table Below**

Function Code	Register	Description	Scaling	Bits
3	200	NetGuardian (832/864 as DX) Expansion 2 Analog 1 Value	*	16
3	201	NetGuardian (832/864 as DX) Expansion 2 Analog 1 Scaling	*	1/16-3/16
3	201	NetGuardian (832/864 as DX) Expansion 2 Analog 1 Sign	*	7/16
3	202	NetGuardian (832/864 as DX) Expansion 2 Analog 2 Value	*	16
3	203	NetGuardian (832/864 as DX) Expansion 2 Analog 2 Scaling	*	1/16-3/16
3	203	NetGuardian (832/864 as DX) Expansion 2 Analog 2 Sign	*	7/16

Function Code	Register	Description	Scaling	Bits
3	204	NetGuardian (832/864 as DX) Expansion 2 Analog 3 Value	*	16
3	205	NetGuardian (832/864 as DX) Expansion 2 Analog 3 Scaling	*	1/16-3/16
3	205	NetGuardian (832/864 as DX) Expansion 2 Analog 3 Sign	*	7/16
3	206	NetGuardian (832/864 as DX) Expansion 2 Analog 4 Value	*	16
3	207	NetGuardian (832/864 as DX) Expansion 2 Analog 4 Scaling	*	1/16-3/16
3	207	NetGuardian (832/864 as DX) Expansion 2 Analog 4 Sign	*	7/16
3	208	NetGuardian (832/864 as DX) Expansion 2 Analog 5 Value	*	16
3	209	NetGuardian (832/864 as DX) Expansion 2 Analog 5 Scaling	*	1/16-3/16
3	209	NetGuardian (832/864 as DX) Expansion 2 Analog 5 Sign	*	7/16
3	210	NetGuardian (832/864 as DX) Expansion 2 Analog 6 Value	*	16
3	211	NetGuardian (832/864 as DX) Expansion 2 Analog 6 Scaling	*	1/16-3/16
3	211	NetGuardian (832/864 as DX) Expansion 2 Analog 6 Sign	*	7/16
3	212	NetGuardian (832/864 as DX) Expansion 2 Analog 7 Value	*	16
3	213	NetGuardian	*	1/16-3/16

Function Code	Register	Description	Scaling	Bits
		(832/864 as DX) Expansion 2 Analog 7 Scaling		
3	213	NetGuardian (832/864 as DX) Expansion 2 Analog 7 Sign	*	7/16
3	214	NetGuardian (832/864 as DX) Expansion 2 Analog 8 Value	*	16
3	215	NetGuardian (832/864 as DX) Expansion 2 Analog 8 Scaling	*	1/16-3/16
3	215	NetGuardian (832/864 as DX) Expansion 2 Analog 8 Sign	*	7/16

*** See Scaling Range Table Below**

Function Code	Register	Description	Scaling	Bits
3	300	NetGuardian (832/864 as DX) Expansion 3 Analog 1 Value	*	16
3	301	NetGuardian (832/864 as DX) Expansion 3 Analog 1 Scaling	*	1/16-3/16
3	301	NetGuardian (832/864 as DX) Expansion 3 Analog 1 Sign	*	7/16
3	302	NetGuardian (832/864 as DX) Expansion 3 Analog 2 Value	*	16
3	303	NetGuardian (832/864 as DX) Expansion 3 Analog 2 Scaling	*	1/16-3/16
3	303	NetGuardian (832/864 as DX) Expansion 3 Analog 2 Sign	*	7/16
3	304	NetGuardian (832/864 as DX) Expansion 3 Analog 3 Value	*	16
3	305	NetGuardian (832/864 as DX) Expansion 3 Analog	*	1/16-3/16

Function Code	Register	Description	Scaling	Bits
		3 Scaling		
3	305	NetGuardian (832/864 as DX) Expansion 3 Analog 3 Sign	*	7/16
3	306	NetGuardian (832/864 as DX) Expansion 3 Analog 4 Value	*	16
3	307	NetGuardian (832/864 as DX) Expansion 3 Analog 4 Scaling	*	1/16-3/16
3	307	NetGuardian (832/864 as DX) Expansion 3 Analog 4 Sign	*	7/16
3	308	NetGuardian (832/864 as DX) Expansion 3 Analog 5 Value	*	16
3	309	NetGuardian (832/864 as DX) Expansion 3 Analog 5 Scaling	*	1/16-3/16
3	309	NetGuardian (832/864 as DX) Expansion 3 Analog 5 Sign	*	7/16
3	310	NetGuardian (832/864 as DX) Expansion 3 Analog 6 Value	*	16
3	311	NetGuardian (832/864 as DX) Expansion 3 Analog 6 Scaling	*	1/16-3/16
3	311	NetGuardian (832/864 as DX) Expansion 3 Analog 6 Sign	*	7/16
3	312	NetGuardian (832/864 as DX) Expansion 3 Analog 7 Value	*	16
3	313	NetGuardian (832/864 as DX) Expansion 3 Analog 7 Scaling	*	1/16-3/16
3	313	NetGuardian (832/864 as DX) Expansion 3 Analog 7 Sign	*	7/16

Function Code	Register	Description	Scaling	Bits
3	314	NetGuardian (832/864 as DX) Expansion 3 Analog 8 Value	*	16
3	315	NetGuardian (832/864 as DX) Expansion 3 Analog 8 Scaling	*	1/16-3/16
3	315	NetGuardian (832/864 as DX) Expansion 3 Analog 8 Sign	*	7/16

*** See Scaling Range Table Below**

Function Code	Register	Description	Scaling	Bits
4	100	NetGuardian (832/864 as DX) Expansion 1 Analog 1 Value	*	16
4	101	NetGuardian (832/864 as DX) Expansion 1 Analog 1 Scaling	*	1/16-3/16
4	101	NetGuardian (832/864 as DX) Expansion 1 Analog 1 Sign	*	7/16
4	102	NetGuardian (832/864 as DX) Expansion 1 Analog 2 Value	*	16
4	103	NetGuardian (832/864 as DX) Expansion 1 Analog 2 Scaling	*	1/16-3/16
4	103	NetGuardian (832/864 as DX) Expansion 1 Analog 2 Scaling	*	7/16
4	104	NetGuardian (832/864 as DX) Expansion 1 Analog 3 Value	*	16
4	105	NetGuardian (832/864 as DX) Expansion 1 Analog 3 Scaling	*	1/16-3/16
4	105	NetGuardian (832/864 as DX) Expansion 1 Analog 3 Scaling	*	7/16
4	106	NetGuardian (832/864 as DX)	*	16

Function Code	Register	Description	Scaling	Bits
		Expansion 1 Analog 4 Value		
4	107	NetGuardian (832/864 as DX) Expansion 1 Analog 4 Scaling	*	1/16-3/16
4	107	NetGuardian (832/864 as DX) Expansion 1 Analog 4 Scaling	*	7/16
4	108	NetGuardian (832/864 as DX) Expansion 1 Analog 5 Value	*	16
4	109	NetGuardian (832/864 as DX) Expansion 1 Analog 5 Scaling	*	1/16-3/16
4	109	NetGuardian (832/864 as DX) Expansion 1 Analog 5 Scaling	*	7/16
4	110	NetGuardian (832/864 as DX) Expansion 1 Analog 6 Value	*	16
4	111	NetGuardian (832/864 as DX) Expansion 1 Analog 6 Scaling	*	1/16-3/16
4	111	NetGuardian (832/864 as DX) Expansion 1 Analog 6 Scaling	*	7/16
4	112	NetGuardian (832/864 as DX) Expansion 1 Analog 7 Value	*	16
4	113	NetGuardian (832/864 as DX) Expansion 1 Analog 7 Scaling	*	1/16-3/16
4	113	NetGuardian (832/864 as DX) Expansion 1 Analog 7 Scaling	*	7/16
4	114	NetGuardian (832/864 as DX) Expansion 1 Analog 8 Value	*	16
4	115	NetGuardian (832/864 as DX) Expansion 1 Analog	*	1/16-3/16

Function Code	Register	Description	Scaling	Bits
		8 Scaling		
4	115	NetGuardian (832/864 as DX) Expansion 1 Analog 8 Scaling	*	7/16

*** See Scaling Range Table Below**

Function Code	Register	Description	Scaling	Bits
4	200	NetGuardian (832/864 as DX) Expansion 2 Analog 1 Value	*	16
4	201	NetGuardian (832/864 as DX) Expansion 2 Analog 1 Scaling	*	1/16-3/16
4	201	NetGuardian (832/864 as DX) Expansion 2 Analog 1 Sign	*	7/16
4	202	NetGuardian (832/864 as DX) Expansion 2 Analog 2 Value	*	16
4	203	NetGuardian (832/864 as DX) Expansion 2 Analog 2 Scaling	*	1/16-3/16
4	203	NetGuardian (832/864 as DX) Expansion 2 Analog 2 Sign	*	7/16
4	204	NetGuardian (832/864 as DX) Expansion 2 Analog 3 Value	*	16
4	205	NetGuardian (832/864 as DX) Expansion 2 Analog 3 Scaling	*	1/16-3/16
4	205	NetGuardian (832/864 as DX) Expansion 2 Analog 3 Sign	*	7/16
4	206	NetGuardian (832/864 as DX) Expansion 2 Analog 4 Value	*	16
4	207	NetGuardian (832/864 as DX) Expansion 2 Analog 4 Scaling	*	1/16-3/16
4	207	NetGuardian	*	7/16

Function Code	Register	Description	Scaling	Bits
		(832/864 as DX) Expansion 2 Analog 4 Sign		
4	208	NetGuardian (832/864 as DX) Expansion 2 Analog 5 Value	*	16
4	209	NetGuardian (832/864 as DX) Expansion 2 Analog 5 Scaling	*	1/16-3/16
4	209	NetGuardian (832/864 as DX) Expansion 2 Analog 5 Sign	*	7/16
4	210	NetGuardian (832/864 as DX) Expansion 2 Analog 6 Value	*	16
4	211	NetGuardian (832/864 as DX) Expansion 2 Analog 6 Scaling	*	1/16-3/16
4	211	NetGuardian (832/864 as DX) Expansion 2 Analog 6 Sign	*	7/16
4	212	NetGuardian (832/864 as DX) Expansion 2 Analog 7 Value	*	16
4	213	NetGuardian (832/864 as DX) Expansion 2 Analog 7 Scaling	*	1/16-3/16
4	213	NetGuardian (832/864 as DX) Expansion 2 Analog 7 Sign	*	7/16
4	214	NetGuardian (832/864 as DX) Expansion 2 Analog 8 Value	*	16
4	215	NetGuardian (832/864 as DX) Expansion 2 Analog 8 Scaling	*	1/16-3/16
4	215	NetGuardian (832/864 as DX) Expansion 2 Analog 8 Sign	*	7/16

*** See Scaling Range Table Below**

Function Code	Register	Description	Scaling	Bits
4	300	NetGuardian (832/864 as DX) Expansion 3 Analog 1 Value	*	16
4	301	NetGuardian (832/864 as DX) Expansion 3 Analog 1 Scaling	*	1/16-3/16
4	301	NetGuardian (832/864 as DX) Expansion 3 Analog 1 Sign	*	7/16
4	302	NetGuardian (832/864 as DX) Expansion 3 Analog 2 Value	*	16
4	303	NetGuardian (832/864 as DX) Expansion 3 Analog 2 Scaling	*	1/16-3/16
4	303	NetGuardian (832/864 as DX) Expansion 3 Analog 2 Sign	*	7/16
4	304	NetGuardian (832/864 as DX) Expansion 3 Analog 3 Value	*	16
4	305	NetGuardian (832/864 as DX) Expansion 3 Analog 3 Scaling	*	1/16-3/16
4	305	NetGuardian (832/864 as DX) Expansion 3 Analog 3 Sign	*	7/16
4	306	NetGuardian (832/864 as DX) Expansion 3 Analog 4 Value	*	16
4	307	NetGuardian (832/864 as DX) Expansion 3 Analog 4 Scaling	*	1/16-3/16
4	307	NetGuardian (832/864 as DX) Expansion 3 Analog 4 Sign	*	7/16
4	308	NetGuardian (832/864 as DX) Expansion 3 Analog 5 Value	*	16
4	309	NetGuardian	*	1/16-3/16

Function Code	Register	Description	Scaling	Bits
		(832/864 as DX) Expansion 3 Analog 5 Scaling		
4	309	NetGuardian (832/864 as DX) Expansion 3 Analog 5 Sign	*	7/16
4	310	NetGuardian (832/864 as DX) Expansion 3 Analog 6 Value	*	16
4	311	NetGuardian (832/864 as DX) Expansion 3 Analog 6 Scaling	*	1/16-3/16
4	311	NetGuardian (832/864 as DX) Expansion 3 Analog 6 Sign	*	7/16
4	312	NetGuardian (832/864 as DX) Expansion 3 Analog 7 Value	*	16
4	313	NetGuardian (832/864 as DX) Expansion 3 Analog 7 Scaling	*	1/16-3/16
4	313	NetGuardian (832/864 as DX) Expansion 3 Analog 7 Sign	*	7/16
4	314	NetGuardian (832/864 as DX) Expansion 3 Analog 8 Value	*	16
4	315	NetGuardian (832/864 as DX) Expansion 3 Analog 8 Scaling	*	1/16-3/16
4	315	NetGuardian (832/864 as DX) Expansion 3 Analog 8 Sign	*	7/16

*** See Scaling Range Table Below**

Scaling Range Table	
Scaling Range	Scaling Value*
0	0.001522821
1	0.003863678
2	0.008098398
3	0.01819765
4	0.02306719

*Get correct Scaling Value by using corresponding Scaling Range

Example 1:

Modbus Response:

Analog 1 Value: [08][72] = 2162
Analog 1 Scaling Range: 2 = 0.008098398
Analog 1 Sign = 0

Scaled Value:

2162 * 0.008098398 = 17.5087
(if Analog Sign = 1 then multiply by -1)
Scaled Value = 17.5087

Example 2:

Modbus Response:

Analog 1 Value: [0A][47] = 2631
Analog 1 Scaling Range: 3 = 0.01819765
Analog 1 Sign = 1

Scaled Value:

2631 * 0.01819765 = 47.8780
(if Analog Sign = 1 then multiply by -1)
Scaled Value = 47.8780 * -1
Scaled Value = -47.8780

10 Frequently Asked Questions

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

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

10.1 General FAQs

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

Q. How can I back up the current configuration of my NetGuardian?
A. There are two ways. NGEdit can read the configuration of your NetGuardian and save the configuration to your PC's hard disk or a flash drive. With NGEdit you can also make changes to the configuration file and write the changed configuration to the NetGuardian's NVRAM.

Q. Can I use my NetGuardian as a proxy server to access TTY interfaces on my third-party serial equipment?
A. You can use Data Ports 1–8, located on the back of the NetGuardian, to connect to serial devices, as long as your devices support RS-232. To make a proxy connection, you must define the correct TCP port for each serial port. To define TCP ports, you must first connect directly to the NetGuardian through its IP address. Once you have connected to the NetGuardian, you can define the TCP ports through the NetGuardian's TTY or Web Browser Interface configuration interfaces.

Q. What do the terms alarm point, display, port, and address mean?
A. These terms define the exact location of a network alarm, from the most specific (an individual alarm point) to the most general (an entire monitored device). An alarm point is a number representing an actual contact closure that is activated when an alarm condition occurs. For example, an alarm point might represent a low oil sensor in a generator or a open/closed sensor in a door. A display is a logical group of 64 alarm points. A port is traditionally the actual physical serial port through which the monitoring device collects data. The address is a number representing the monitored device. The terms port and address have been extended to refer to logical, or virtual, ports and addresses. For example, the NetGuardian reports internal alarms on Port 99, address 1.

Q. What characteristics of an alarm point can I configure through software? For instance, can I configure Point 4 to sense an active-low (normally closed) signal, or Point 5 to sense a level or edge?
A. The NetGuardian alarm points are level sensed and can be software-configured to generate an alarm on either a high (normally open) or low (normally closed) level.

Q. When I connect to the NetGuardian 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. The standard settings for the craft port are 9600 baud, 8 bits, no parity, and 1 stop bit. 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.

Q. I just changed the port settings for one of my data ports, but the changes did not seem to take effect even after I wrote the NVRAM.
A. In order for data port and craft port changes (including changes to the baud rate and word format) to take effect, the NetGuardian must be rebooted. Whenever you make changes, remember to write them to the NetGuardian's NVRAM so they will be saved when the unit is rebooted.

Q. How do I get my NetGuardian on the network?
A. Before the NetGuardian will work on your LAN, the unit address (IP address), the subnet mask, and the

default gateway must be set. 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

Always remember to save your changes by writing to the NVRAM. Any modifications of the NetGuardian's IP configuration will also require a reboot.

Q. I'm using HyperTerminal to connect to the NetGuardian through the craft port, but the unit won't accept input when I get to the first level menu.

A. Make sure you turn off all handshaking in HyperTerminal.

Q. The LAN line LED is green on my NetGuardian, but I can't poll it from my T/MonXM master.

A. Some routers will not forward to an IP address until the MAC address has been registered with the router. You need to enter the IP address of your T/MonXM system or your gateway in the ping table.

10.2 SNMP FAQs

Q. Which version of SNMP is supported by the SNMP agent on the NetGuardian?
A. SNMP v1, v2C, and v3 on the NetGuardian G6 series.

Q. How do I configure the NetGuardian to send traps to an SNMP manager? Is there a separate MIB for the NetGuardian? 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 begins sending traps as soon as the SNMP managers are defined. The NetGuardian MIB is included on the NetGuardian Resource CD. The MIB should be compiled on your SNMP manager. (**NOTE:** MIB versions may change in the future.) The unit supports a main SNMP manager, which is configured by entering its IP address in the trap address field of Ethernet Port Setup. You can also configure up to eight secondary SNMP managers, which is configured by selecting the secondary SNMP managers as pager recipients. Community strings are configured globally for all SNMP managers. To configure the community strings, choose System from the Edit menu, and enter appropriate values in the Get, Set, and Trap fields.

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

Q. Does the NetGuardian SNMP agent support both NetGuardian and T/MonXM variables?
A. The NetGuardian SNMP agent manages an embedded MIB that supports only the NetGuardian'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, but there are two exception to this rule.
Exception 1: the first alarm in an all clear condition generates an additional summary point set trap.
Exception 2: the final clear alarm that triggers an all clear condition generates an additional summary point clear 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 manual talks about eight 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. For more information about the set commands, see Reference Information, Display Mapping, in any of the NetGuardian software configuration guides.

Q. How can I associate descriptive information with a point for the RTU granular traps?
A. The NetGuardian alarm point descriptions are individually defined using the Web Browser Interface, TTY, or NGEdit configuration interfaces.

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 and the SNMP manager are both on the network. Use the NetGuardian's ping command to ping the SNMP manager.

11 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.dpstelecom.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.*

12 End User License Agreement

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

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

DPS Telecom's warranty and limitation on its liability for the Software is as described in the warranty information provided to End User in the Product Manual. End User shall indemnify DPS Telecom and hold it harmless for and against any and all claims, damages, losses, costs, expenses, obligations, liabilities, fees and costs and all amounts paid in settlement of any claim, action or
suit which may be asserted against DPS Telecom which arise out of or are related to the non-fulfillment of any covenant or obligation of End User in connection with this Agreement.

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

Warranty

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

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

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

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

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

Technical Support

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

Free Tech Support is Only a Click Away

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

www.DpsTelecom.com

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

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

- Expert tips on using your alarm monitoring equipment — advanced techniques that will save you hours of work
- Educational White Papers deliver fast informal tutorials on SNMP, ASCII processing, TL1 and other alarm monitoring technologies
- New product and upgrade announcements keep you up to date with the latest technology
- Exclusive access to special offers for DPS Telecom Factory Training, product upgrade offers and discounts

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

Free Tech Support on the Web: MyDPS

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

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

DPS Telecom
"Your Partners in Network Alarm Monitoring"

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

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