DPS Telecom
"Your Partners in Network Alarm Monitoring"

NetGuardian SUI

USER MANUAL

D-PK-NGSUI

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

Revision History

August 15, 2019	Added Support for IP Meters
July 9, 2018	Added Master Trigger for Latch Delay
July 6, 2016	Initial Release

Contents

1   NetGuardian DIN Overview

The NetGuardian SUI

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

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

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

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

The NetGuardian SUI reports alarms as SNMP traps over LAN and supports DCP polling over LAN. The

NetGuardian SUI supports simultaneous SNMP and DCP operation.

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

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

2   Specifications

Discrete Alarm Inputs:	8 (Optional build with 6 alarms and 2 controls)
Control Relays:	6 (Form A) user defined NO/NC (Optional)
Analog Inputs	N/A
Analog Input Range:	N/A
Analog Accuracy:	N/A
Ping Targets:	32
Protocols:	SNMPv1, SNMPv2c, SNMPv3, DCPx, TELNET, HTTP, HTTPS, Email, TRIP
Dimensions:	2.1" H x 7.250" W x 5.150" D
Weight:	1.13 lbs (.513 kg)
Mounting:	SUI mount, Wall mount option (brackets sold separately)
Power Input:	–48 VDC nominal (–36 to –72 VDC) (Optional) –24 VDC nominal (–18 to –36 VDC) (Optional) Wide Range –24/–48 VDC (–18 to –58 VDC) (Optional) +24VDC (+18 to +36 VDC) (Optional) +12VDC (+11 to +18 VDC) (Optional) Power Over Ethernet (POE
Fuse:	Internal Resetable
Current Draw:	140 mA @ 24VDC
Interfaces:	1 RJ45 10/100BaseT full-duplex Ethernet port 1 USB front-panel craft port 1-4 RJ11 connector for D-Wire sensor network (Optional) 1 RJ11 Connector for Telco
Visual Interface:	7 Front Panel LEDs
Operating Temperature:	32° - 140° F (0° - 60° C)
Industrial Temperature Option:	-22° to 158° F (-30° to 70° C)
Operating Humidity:	0% - 95% non-condensing
MTBF:	60 years
Windows Compatibility:	XP, Vista, 7 (32 or 64 bit)
RoHS	5/6
Sensors:	Up to15 dwire sensors 1 built-in temp sensor (Optional)

3 Shipping List

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

NetGuardian SUI
D-PK-NGSUI

NetGuardian SUI Resource CD

NetGuardian SUI User Manual
D-UM-NGSUI

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

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

14ft. Ethernet Cable
D-PR-932-10B-14
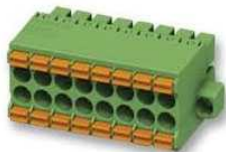
x 1
8-Pin Alarm Connector
2-821-20835-00
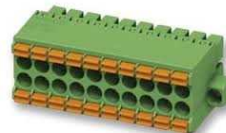
x 1
10-Pin Alarm Connector
2-821-21035-00

3.1 Optional Shipping Items - Available by Request

**Temp Sensor Node
D-PK-DSNSR-12001**

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

4   Installation

4.1   Mounting

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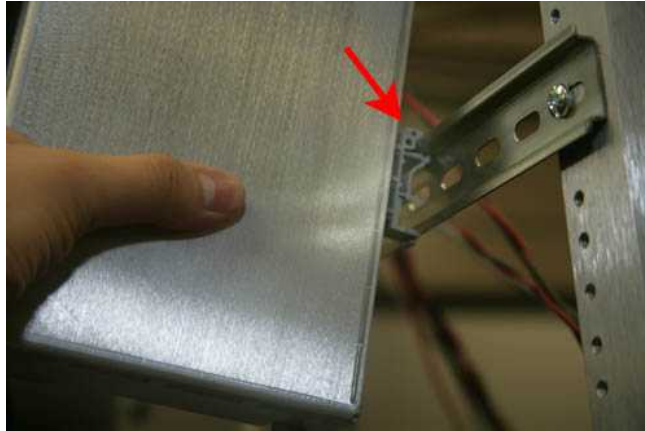
First connect the top of the DIN clip to the rack.
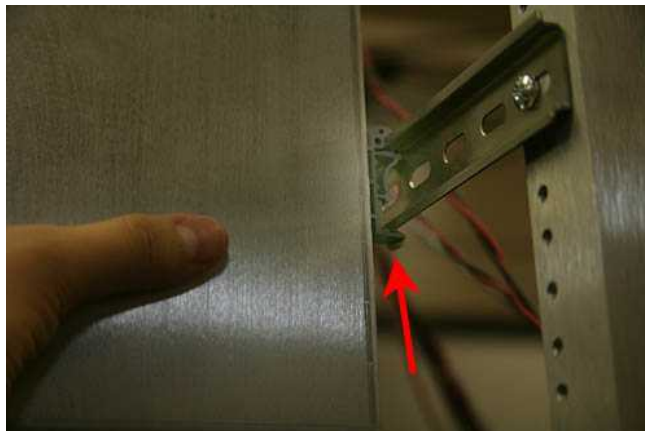
Then snap the bottom of the DIN clip to the bottom of the rack.

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

4.2   Power Connection

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

NetGuardian SUI Power Terminal

To connect the NetGuardian SUI to a power supply:

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

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

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

4.3   Configuration

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

5 NetGuardian DIN Front Panel
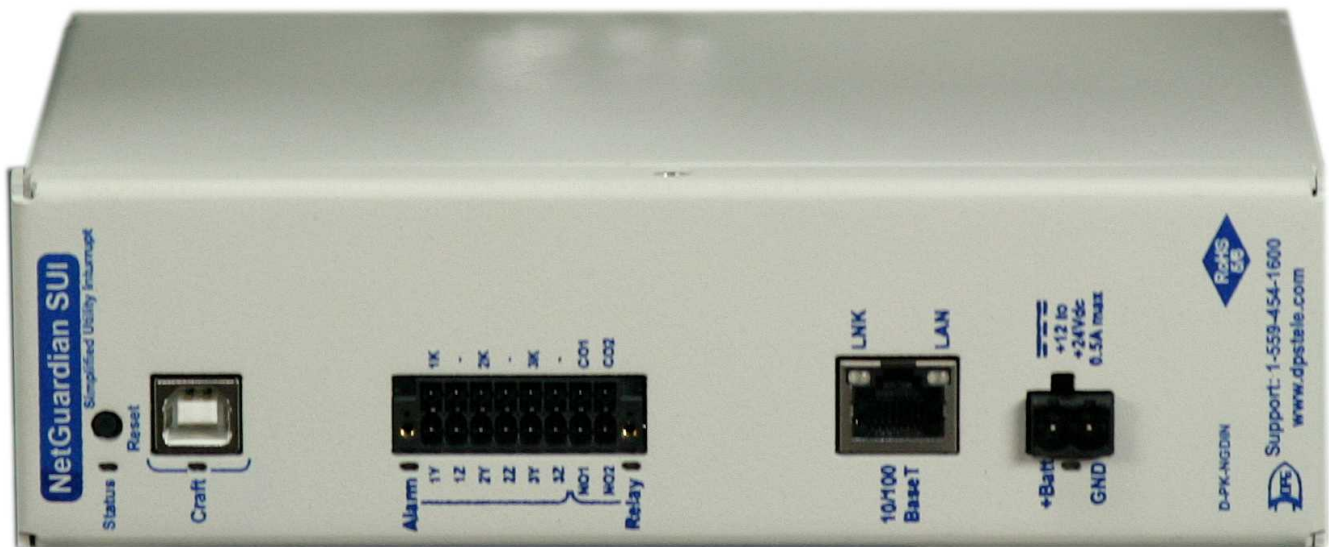
NetGuardian SUI Front Panel

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

Front Panel LED Descriptions

6   Quick Start: How to Connect to the NetGuardian DIN

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

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

6.1   ...via LAN

NetGuardian SUI Ethernet Port

To connect to the NetGuardian SUI via LAN, all you need is the unit's IP address (Default IP address is 10.0.6.100).

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

1. Get a LAN crossover cable and plug it directly into the NetGuardian SUI's LAN port.
2. Look up your PC's current IP address and subnet mask, and write this information down.
3. Reset your PC's IP address to **10.0.6.200**. Contact your IT department if you are unsure how to do this.
4. Reset your PC's subnet mask to **255.255.0.0** and gateway to **10.0.6.1.** You may have to reboot your PC to apply your changes.
5. Once the IP address and subnet mask of your computer coincide with the unit, you can access the unit via a Telnet session or via Web browser by using the unit's default IP address of **10.0.6.100**.
6. Provision the NetGuardian SUI with the appropriate information, then **change your computer's IP address and subnet mask back to their original settings.**

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

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

NetGuardian SUI Craft Port

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

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

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

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

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

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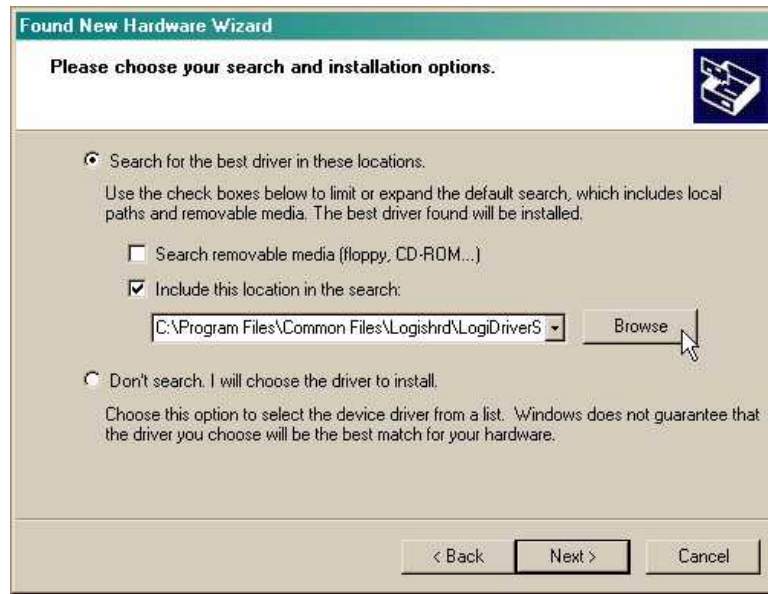
4. Select "Search for the best driver in these locations."
5. Insert NetGuardian SUI Resource Disc (CD) into your PC.
6. Click "Browse"
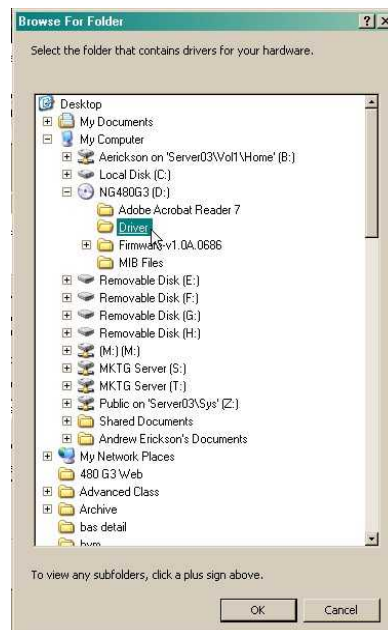
7. Select the "Driver" folder of your NetGuardian SUI Resource Disc Disc (CD) and click "OK"

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

8. Click "Finish" to close the Wizard.

Now that the driver has been installed, a new COM port is being emulated on your PC. Before using hyperterminal, you must confirm the identity of that new COM port (COM1, COM2, COM3...) in the Windows Device Manager.
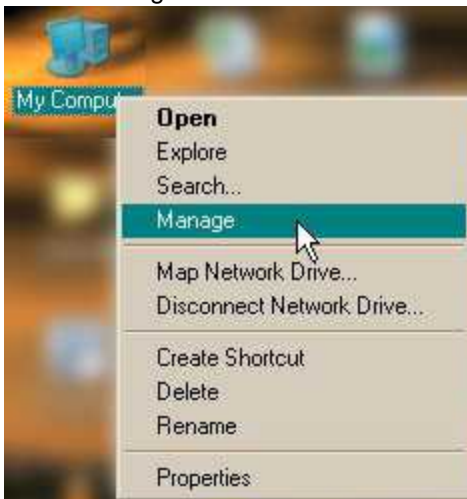
9. Right-click the "My Computer" icon on your desktop, then click "Manage"
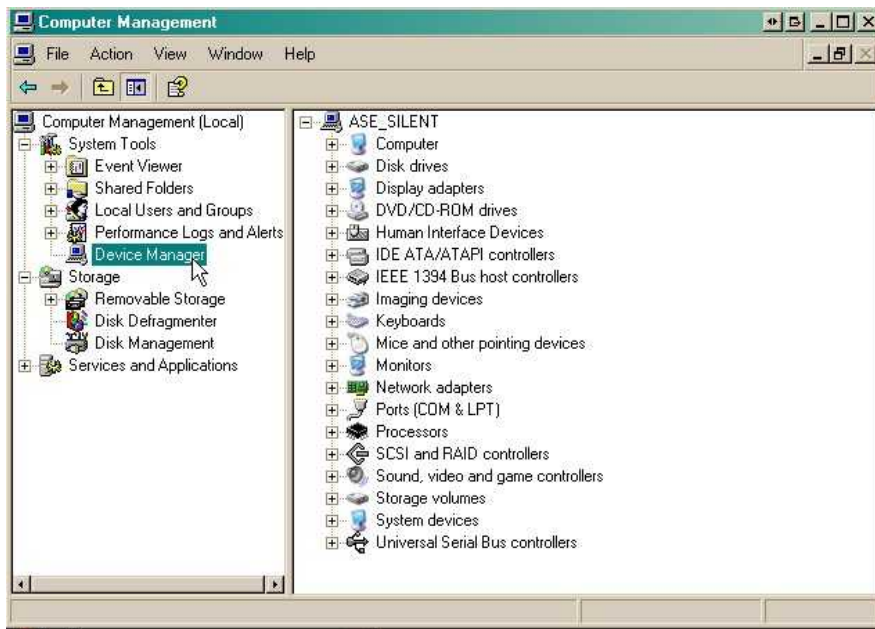
10. Click "Device Manager" in the left pane.
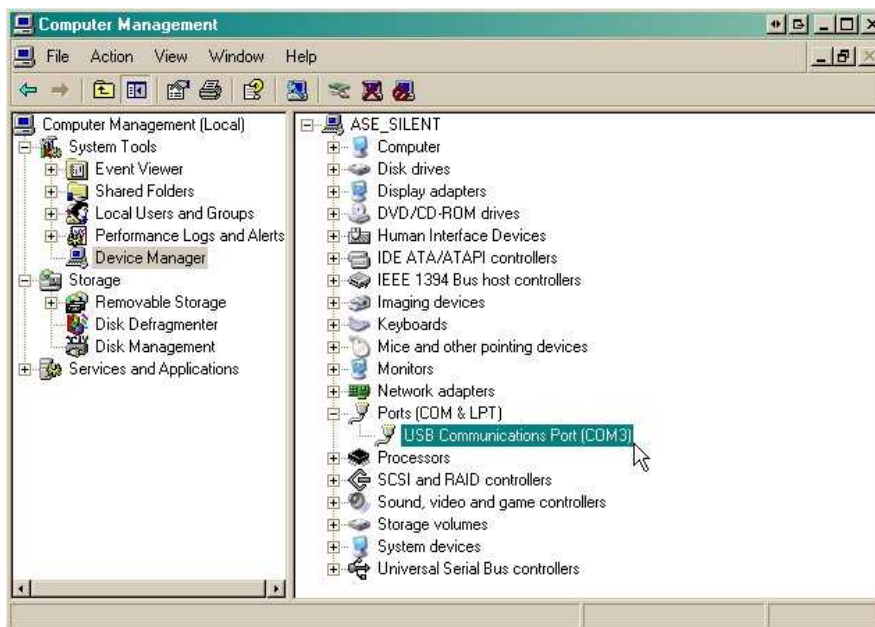
11. Expand the "Ports (COM & LPT)" section in the right pane. Look for "USB Communications Port (COMx)". Note the number of the COM port ("COM3" in the example above).

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

13. At the Connection Description screen, enter a name for this connection. You may also select an icon. The

14. At the Connect To screen, use the drop-down menu to select the COM port you found earlier in the

name and icon do <u>not</u> affect your ability to connect to the unit.

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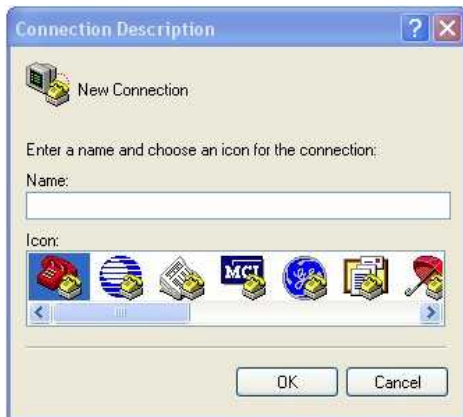
15. Select the following COM port options:
   • Bits per second: 9600
   • Data bits: 8
   • Parity: None
   • Stop bits: 1
   • Flow control: **None**

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

16. When prompted, enter the default user name **admin** and password **dpstelecom**. <u>NOTE</u>**:** If you don't receive a prompt for your user name and password, check the Com port you are using on your PC and make sure you are using the cable provided. Additional cables can be ordered from DPS Telecom.
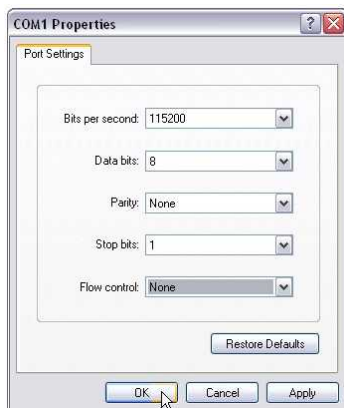
17. The NetGuardian SUI's main menu will appear. Type C for C)onfig, then E for E)thernet. Configure the unit's IP address, subnet mask, and default gateway.

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

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

7   TTY Interface

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

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

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

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

If you're using Windows 7, then you'll need to install telnet before you can use the TTY interface. To install telnet, open up your command line (type "cmd" into the search bar in the **Start Menu**). Select **cmd.exe** to run the command line.
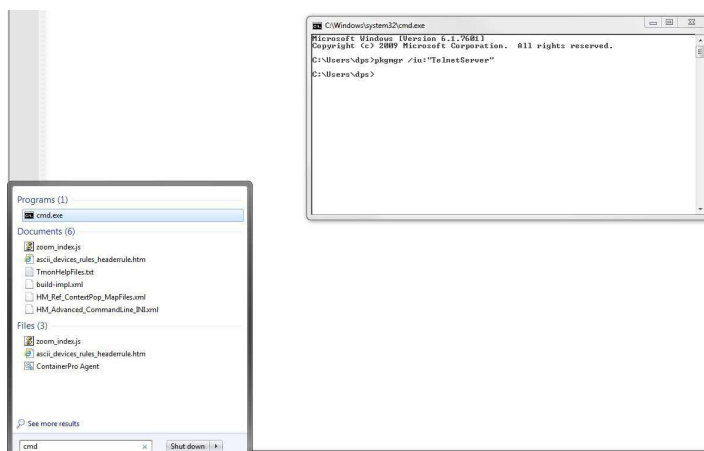
From the command line, type in **pkgmgr /iu:"TelnetClient"** then press **enter**. When the command prompt appears again, the installation is complete.

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

To reset unit to factory default settings:

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

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

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

8   Quick Turn Up

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

8.1 How to Send Email Notifications

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

Notifications

Id	Notify On	Type	Details		
1	Disabled			Edit	Test
2	Disabled			Edit	Test
3	Disabled			Edit	Test
4	Disabled			Edit	Test
5	Disabled			Edit	Test
6	Disabled			Edit	Test
7	Disabled			Edit	Test
8	Disabled			Edit	Test

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

Notification 1

Status	Notify on Alarms only ▼
Type	⦿ **Send Email** ○ **Send SNMP**

[Back] [Save and Next]

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

Notification 1 (Email)

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

How to authenticate

⦿ **No authentication**
○ **POP before SMTP authentication**
○ **SMTP authentication**

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

[Back] [Save and Next]

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

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

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

8.2   How to Send SNMP Traps

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

SNMP

Global Settings	
Get Community	dps_public
Set Community	dps_public
Read and Write Access	Access disabled
SNMPv3 Engine ID	80000a7a03001081002f85

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

Save

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.

Notifications

Summary				
Id	Notify On	Type	Details	
1	Disabled			Edit Test
2	Disabled			Edit Test
3	Disabled			Edit Test
4	Disabled			Edit Test
5	Disabled			Edit Test
6	Disabled			Edit Test
7	Disabled			Edit Test
8	Disabled			Edit Test

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

Notification 1

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

Back   Save and Next

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

Notification 1 (SNMP)

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

[Back] [Save and Next]

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

Notification 1 (Schedule)

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

[Back] [Save and Finish]

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

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

8.3   How to Send TRIP Notifications

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

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

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

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

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

9   Provisioning Menu Field Descriptions

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

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

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

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

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

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

9.1   System

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

System Settings

Global Settings	
Name	NetGuardian_DIN
Location	Fresno, CA
Contact	559-454-1600
TRIP Unit ID	0 (Disabled)

DCP Responder Settings Display Map	
⦿ Disable DCP ○ DCP over LAN	
DCP Unit ID / Protocol	1 / DCPx ▾
DCP over LAN port / Protocol	2001 / UDP ▾

Sensors History	
Get history	history.csv
Erase history	Erase

Save

The Provisioning > System menu

Global System Settings	
Name	A name for this NetGuardian SUI unit. {Optional field}
Location	The location of this NetGuardian SUI unit. {Optional field}
Contact	Contact telephone number for the person responsible for this NetGuardian SUI unit. {Optional field}
TRIP Unit ID	Site number used when communicating over dialup with T/Mon.
DCP Responder Settings *(For use with T/Mon)*	
DCP Unit ID	User-definable ID number for the target unit (DCP Address)
DCP Unit Protocol	Drop-down menu of available protocols for use with DCP Address
DCP over LAN port	Enter the DCP port for the target unit (UDP/TCP port)
LAN Protocol	Drop-down menu of available protocols for use over LAN
Sensors History	
Get History	Download a log of all configured analog and sensor values.
Erase History	Erase the log of all configured analog and sensor values.

9.2 User Profiles

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

Configure access privileges for users in the User Profile screen

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

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

User profile field descriptions

9.3 Ethernet

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

The Provisioning > Ethernet menu

Ethernet Settings	
MAC Address	Hardware address of the NetGuardian SUI. (Not editable - For reference only.)
Host Name	Used only for web browsing. Example: If you don't want to remember this NetGuardian SUI's IP address, you can type in a name is this field, such as "MyNetGuardian SUI". Once you save and reboot the unit, you can now browse to it locally by simply typing in "MyNetGuardian SUI" 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 SUI.
Subnet Mask	A road sign to the NetGuardian SUI, 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 SUI which machine is the gateway out of your local network. Set to 255.255.255.255 if not using. Contact your network administrator for this info.
DNS Server 1	Primary IP address of the domain name server. Set to 255.255.255.255 if not using.
DNS Server 2	Secondary IP address of the domain name server. Set to 255.255.255.255 is not using.

Advanced TCP Settings	
Force Max TCP Window Size	The defined TCP window size is used. (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.

9.4   DNP3 Configuration

DNP3 Configuration

Outstation Settings   DNP3 Points

DNP3 Mode of Operation: ● LAN ○ Disabled

Station Address | 101

DNP3 Network | **Primary Port:** 2101 | **Protocol:** TCP ∨
| **Additional Port:** 2102 | (Not Configurable. Set to Primary Port+1)

[Save]

DNP3 Mode of Operation: This option allows to activate DNP3 over LAN or to Disable the feature Station Address: This is the DNP3 polling address of the NetGuardian. This value can range from 0 - 65519. DNP3 Network: This option allows you to select the port for DNP3 polling over LAN.

SUI Meters	
DNP3 Mode of Operation	This option allows to activate DNP3 over LAN or to Disable the feature
Station Address	This is the DNP3 polling address of the NetGuardian. This value can range from 0 - 65519.
DNP3 Network	This option allows you to select the port for DNP3 polling over LAN.

9.5   Serial Port

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

Serial Port Settings

Location	Port Configuration				Reach-Through
Primary port located on the left side of the unit.	Port Type: 232 ▼ RTS head: 0	Baud: 9600 ▼ RTS tail: 0	Parity: 8-bit data, no parity ▼	Stop Bits: 1 ▼	☐ Enable Reach-Through Port: 3000 Type: TCP ▼
Primary port located on the right side of the unit.	Port Type: 485 ▼ RTS head: 30	Baud: 9600 ▼ RTS tail: 20	Parity: 8-bit data, no parity ▼ 485 Communication: 2-Wire ▼	Stop Bits: 1 ▼	Not Supported

[Save]

The Provisioning > Serial Ports menu

Location	
A reminder that your primary serial port is located on the back of the NetGuardian SUI chassis.	
Port Configuration	
Port Type	Select the serial port for your build of the NetGuardian SUI. Choose from 232, 485...
Baud, Parity, and Stop Bits	Select the appropriate settings from the drop-down menu.
RTS Head	Only used if your NetGuardian SUI was built with a 202

	modem. The most commonly used value is 30.
RTS Tail	Only used if your NetGuardian SUI was built with a 202 modem. The most commonly used value is 10.
Reach-Through	
Enable Reach-through	Checking this box enables the port to be used as a terminal server. Most commonly used to Telnet through the port over LAN to a hub, switch, or router. From a command prompt, type the following *(note the spaces between each entry)*: telnet [IP address] [port] **Example**: telnet 192.168.1.100 3000
Port	Port number used for reach-through to a serial device.
Type	Select TCP or UDP traffic to be passed through to a serial device.

9.6   RADIUS

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

Fig. 2.1. RADIUS configuration screen

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

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

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

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

9.7   SNMP

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

SNMP Menu

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

Fields in the Provisioning > SNMP settings

9.8   Notifications

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

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

9.8.1   Notification Settings

Email Notification Fields

Editing Email Notification Settings

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

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

SNMP Notification Fields

Notification 1 (SNMP)

SNMP Trap Server IP	126.10.218.3
Trap Port No. (Usually Use 162)	162
Trap Community	
Trap Type	SNMPv2c ▼

Back Save and Next

Editing SNMP notification settings

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

TRIP Dialup (T/Mon) Notification Fields

Notification 1 (TRIP Dialup)

T/Mon Phone Number	
☐ Only dial if DCP poller inactive alarm is set.	

Back Save and Next

Editing Call notification settings

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

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

Syslog Notification Fields

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

	Severity: Used to determine the severity of the message being logged.

9.8.2   Schedule

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

The Schedule creation screen

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

9.9   Alarms

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

The Provisioning > Alarms menu

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

9.10 SUI Meters

SUI Meters

History Timer			
Record Interval	15min		

SUI Meters

Enab	Description	Demand Interval	Pulse Constant
☐	**Meter 1**	5min	1.0000
☐	**Meter 2**	5min	1.0000
☐	**Meter 3**	5min	1.0000

Save

SUI Meters	
Record Interval	Interval at which a History record will be created of Meter Readings
Enable	Enable or Disable meter monitoring with this option
Demand Interval	Interval at which Meter counts will be displayed and calculated
Pulse Constant	Scaling factor used to calculate Interval Energy

9.11   IP Meters

IP Meters

DNP3 Interrogator Settings						
	Poll Delay		20sec	(5sec - 2min)		
IP Meters						
Id	**Enable**	**Description**	**IP or Host**	**TCP Port**	**DNP3 Address**	**DNP3 Poll Type**
1	☑	Meter 1	10.0.200.90	2102	101	Class 3 ○ **Channels<<**

- Channel 1	**Description:** Meter 1 Alg 0	**Units:** VDC	
- Channel 2	**Description:** Meter 1 Alg 1	**Units:** VDC	
- Channel 3	**Description:** Meter 1 Alg 2	**Units:** VDC	

2	☐	Meter 2	10.0.6.201	20000	1	Class 0 ○ **Channels<<**

- Channel 1	**Description:** Meter 2 Alg 0	**Units:** VDC	
- Channel 2	**Description:** Meter 2 Alg 1	**Units:** VDC	
- Channel 3	**Description:** Meter 2 Alg 2	**Units:** VDC	

3	☐	Meter 3	10.0.6.202	20000	1	Class 0 ○ **Channels<<**

- Channel 1	**Description:** Meter 3 Alg 0	**Units:** VDC	
- Channel 2	**Description:** Meter 3 Alg 1	**Units:** VDC	
- Channel 3	**Description:** Meter 3 Alg 2	**Units:** VDC	

Save

The Provisioning > IP Meters menu

IP Meter Settings	
Id	ID number for the IP Meter
Enable Polling	Check this box to enable polling of the meter.
Description	User-definable description for the IP meter.
IP or Host Name	The Internet layer address of the meter to be polled.
TCP Port	The port on the meter that will receive traffic from the NetGuardian.
DNP3 Address	The DNP3 address of the meter.
Poll Type	The type of polling that the NetGuardian will use to monitor the meter.
Channel	**Description** User-definable description for the channel. **Units** The unit(s) of measurement reported by the channel.

9.12 Analogs

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

The Provisioning > User Analogs menu

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

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

9.13 Controls

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

Controls

Id	Description Display Map	1	2	3	4	5	6	7	8
1	Generator Details<<	☐	☐	☐	☐	☐	☐	☐	☐

Derived Description: [   ] [Parse]

Momentary time (e.g. 500ms, 5s, 1m): [1sec]

Id	Description Display Map	1	2	3	4	5	6	7	8
2	Server Temp Details>>	☐	☐	☐	☐	☐	☐	☐	☐

Control 2 Automation Settings

Control 2 will follow master trigger control automatically. If master trigger is latched, control 2 will auto latch after "Latch Delay" time. If master trigger is released, control 2 will be auto released immediately.

Latch Delay (0s - 15m)	5sec

[Save]

The Provisioning > Controls screen

Basic Controls Configuration	
ID	ID number for the control relay.
Description	User-definable description for the NetGuardian SUI's control relay.
Derived Description	Formula to control relay operation. Control relays and virtual alarms can be created from derived formulas using the following operations: **_OR** : Set the current operation to OR. **_AN** : Set the current operation to AND. **_XR** : Set the current operation to XOR. **D** : Tag to change the active display number. **.** : Used like a comma to delimit numbers. **-** : Used to specify a range of points.
Momentary Time	Control on time (in milliseconds) when you execute the MOM command. Max limit of 600 seconds.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for the control relay.
Automation Settings	Select the amount of time that it will take for Control 2 to latch after the master trigger is latched.

9.14 Sensors

D-Wire Sensors

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

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

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

The Provisioning > Sensors menu

Basic Sensor Configuration	
ID	Sensor ID number.
ROM ID	The ID number found on the sticker of the temperature sensor node. Your NetGuardian SUI will automatically detect the sensor ID when you plug a sensor into the unit. The color of the sensor ID field will tell you the status of the connected sensor. **Green** - The sensor is connected and properly configured. **Yellow** - The sensor is connected but has not yet been configured (fill in your configuration fields and click **Save** to configure the sensor). **Red** - The sensor is not detected and configured (i.e. a previous configured sensor is no longer connected). **Blue** - The sensor is not supported by the NetGuardian SUI. To reconfigure or disable the Sensor ID, simply delete any data in this field and click

	Save. The unit will refresh the sensor ID on that channel.
Description	User-definable description for the sensor channel.
Parse	Checks to see if the **Description** field contains a valid equation.
Notification Devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for that alarm point.
Advanced Sensor Configuration (Details>>)	
Record Freq	The amount of time, in minutes (min) or seconds (s), between each recorded sensor value.
Deadband	The amount (in native units) that the channel needs to go above or below a threshold in order to cause an alarm.
Qual Time (Qualification Time)	The length of time that must pass, without interruption, in order for the condition to be considered an Alarm or a Clear.
Qual. Type (Qualification Type)	Allows you to choose whether you want to apply the Qualification Time to the alarm Set, Clear, or Both.
Thresholds	These settings are set to indicate the severity of the alarm depenSUlg on which threshold values have been passed. Enter values for Major Under (MjU), Minor Under (MnU), Minor Over (MnO), and Major Over (MjO).
Analog Gauge Type	Select the color-coded gauge that best represents your data. Selecting **None** will disable the analog gauge and only a numerical representation of the value will be displayed under **Monitor** > **Sensors**.

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

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

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

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

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

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

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

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

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

1. Division is NOT executed if the denominator's absolute value is less than 1!

2. An equation is evaluated until it reaches the Conditional Halt. If the running value at that point is zero, then the evaluation stops, otherwise the evaluation continues as a new equation.

How equations are evaluated:

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

Example of how an equation is evaluated:

Equation: a8 a5 a6 + * a4 -

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

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

9.15   Ping Targets

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

Ping Targets

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

The Provisioning > Ping Targets menu

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

9.16 System Alarms

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

System Alarms

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

The Provisioning > System Alarms menu

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

9.17   Timers

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

Timers

Web Refresh (1s-60s): How often web browser is refreshed when in monitor mode.	1sec
WebTimeout (1m-30m): Maximum idle time allowed before the web interface will automatically logout.	10min
DCP Poller Timeout (1m-30m, 0s=off): DCP polls must be received within this time interval or the DCP poller inactive alarm will set.	5min
Ping Cycle (30s-30m, 0s=off): Time interval between each ping cycle (0 disables, 30 seconds minimum)	4min
Craft Timeout (0s-120m, 0s=off) Maximum idle time allowed before the Craft connection will automatically disconnect.	5min
Timed Tick (0s-60m, 0s=off): ⚪ This is a 'heartbeat' function that can be used by masters who don't perform integrity checks.	
Timed Tick Variation (used for daily or weekly timed tick): ⚫ Format: Day of Week (optional), Time of Day (military time), Duration. For example: "Mon, 17:10, 10min" or just 17:10, 10min". Use this fomat to toggle "Timed tick" system alarm at specified time and for specified duration. "Timed tick" alarm will be in Alarm for specified duration at specified time.	10:58, 10min

Save

The Provisioning > Timers menu

9.18   Date and Time

The Provisioning > Date and Time menu

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

10 Monitoring via the Web Browser

10.1 Alarms

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

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

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

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

10.2 SUI Meters

SUI Meters

Description	Total Count	Energy Count	Interval Energy		Interval Demand		Interval Countdown
Meter 1	0	0	0.00	kWh	0.00	kW	04:37
Meter 2	0	0	0.00	kWh	0.00	kW	04:37
Meter 3	0	0	0.00	kWh	0.00	kW	04:37

SUI Meters	
Total Count	Total count of pulses detected by NetGuardian SUI
Energy Count	Count of pulses detected by NetGuardian SUI during Demand Interval
Interval Energy	Value calculated by multiplying Energy Count with Pulse Constant
Interval Demand	Value calculated by dividing Energy Count by Demand Interval
Interval Countdown	Time remaining in Demand Interval

10.3 IP Meters

IP Meters, Current Values

Id	Meter Description	
1	Meter 1	

	Id	Channel Description	Reading	
	1	Meter 1 Alg 0	1	VDC
	2	Meter 1 Alg 1	2	VDC
	3	Meter 1 Alg 2	3	VDC

Id	Meter Description	
2	Meter 2	

	Id	Channel Description	Reading	
	1	Meter 2 Alg 0	4	VDC
	2	Meter 2 Alg 1	5	VDC
	3	Meter 2 Alg 2	6	VDC

Id	Meter Description	
3	Meter 3	

	Id	Channel Description	Reading	
	1	Meter 3 Alg 0	7	VDC
	2	Meter 3 Alg 1	8	VDC
	3	Meter 3 Alg 2	9	VDC

IP Meters	
Id	ID number for the IP Meter
Meter Description	User-definable description for the IP meter.

Channel	Id	ID number for the channel.
	Channel Description	User-definable description for the channel.
	Reading	The reading reported by the channel.

10.4 Controls

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

View and operate control relays from the Monitor > Controls menu

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

Operating the **Master Trigger Control** will latch control #1 after 1 second, and then latch control #2 after the amount of time specified in **Provisioning > Controls** (0s - 15m). Operating the **Device Reset Control** will reboot the NetGuardian.

10.5   Sensors

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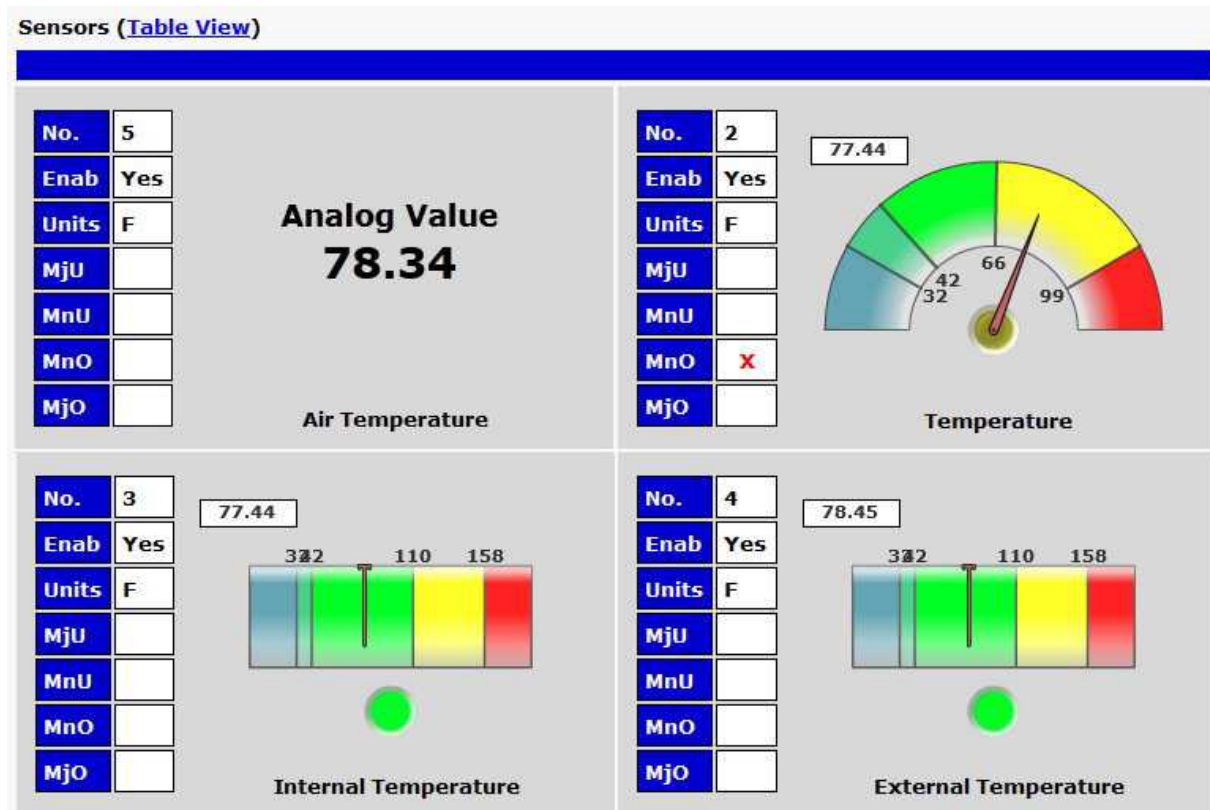
The Monitor > Sensors menu

10.6   Ping Targets

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

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

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

10.7   System Alarms

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

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

System Alarms

Pnt	Description Display Map	State
33	Default configuration	Clear
34	DCP poller inactive	Clear
39	SNMP community error	Clear
41	Notification 1 failed	Clear
42	Notification 2 failed	Alarm
43	Notification 3 failed	Clear
44	Notification 4 failed	Clear

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

10.8   Graph

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

Graph Parameters

Channel	sensor 1	Analogs (a1-a8), Sensors (s1-s32)
Group Interval	1 weeks	1-120 minute(m)/hour(h)/day(d)/week(w)
Group Function	Average ▼	

Start Time

September , 2013 ▼

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Today: Sep 6, 2013
2013-09-06 00:00:00

Time: 00:00:00 ▼

End Time

September , 2013 ▼

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Today: Sep 6, 2013
2013-09-06 23:45:00

Time: 23:45:00 ▼

Build Graph

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

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

Trending Graph

Channel	sensor 1
Start	2013-03-15 00:00:00
End	2013-03-18 00:00:00
Interval	1 hours
Grouping	average

Date: Mar 16, 2013 1:00 AM
Value: 76.61 F

Back

Points

Index	Timestamp	Value
1	Fri Mar 15 2013 00:00:00 GMT-0700 (Pacific Daylight Time)	77.337
2	Fri Mar 15 2013 01:00:00 GMT-0700 (Pacific Daylight Time)	77.094
3	Fri Mar 15 2013 02:00:00 GMT-0700 (Pacific Daylight Time)	76.893
4	Fri Mar 15 2013 03:00:00 GMT-0700 (Pacific Daylight Time)	76.548
5	Fri Mar 15 2013 04:00:00 GMT-0700 (Pacific Daylight Time)	76.285
6	Fri Mar 15 2013 05:00:00 GMT-0700 (Pacific Daylight Time)	76.059

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

11 Device Access Descriptions

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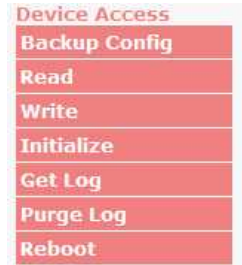
The control menu is located in the bottom left of the web interface

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

12 Backup Configuration

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

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

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

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

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

13 Firmware Upgrade

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

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

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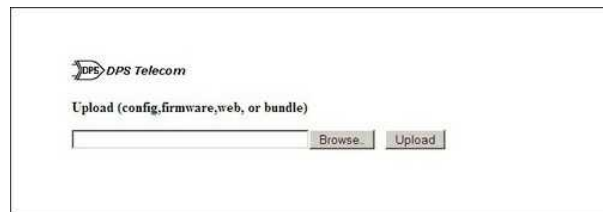
Browse for downloaded firmware upgrade

14 Reference Section

14.1 Display Mapping

Display Mapping

Display	Point	Description
Display 1	1-16	Discrete Alarms
	17-18	Base Controls
	19	Master Trigger Control
	20	Device Reset Control
	21-32	Undefined
	32	(33) Default Configuration
	33	(34) DIP Switch Configuration
	34	(35) MAC Address not set
	35	(36) IP address not set
	36	(37) LAN hardware error
	37	(38) SNMP processing error
	38	(39) SNMP community error
	39	(40) LAN TX packet drop
	40	(41) Notification 1 failed
	41	(42) Notification 2 failed
	42	(43) Notification 3 failed
	43	(44) Notification 4 failed
	44	(45) Notification 5 failed
	45	(46) Notification 6 failed
	46	(47) Notification 7 failed
	47	(48) Notification 8 failed
	48	(49) NTP failed
	49	(50) Time Tick
	50	(51) Serial 1 receive queue full
	51	(52) Dynamic memory full
	52	(53) Unit reset
	53	(54) DCP poller inactive
	54	(55) TRIP error
	55	(56) No dial tone
	56	(57) Modem failed
	57	(58) Meter 1 failed
	58	(59) Meter 2 failed
	59	(60) Meter 3 failed
	60-64	Reserved

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

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

	4	Analog 1 Major Over
	9-16	Control
	17-32	Value
	33	Analog 2 Minor Under
	34	Analog 2 Minor Over
	35	Analog 2 Major Under
	36	Analog 2 Major Over
	41-48	Control
	49-64	Value
Display	Point	Description
	1	Analog 3 Minor Under
	2	Analog 3 Minor Over
	3	Analog 3 Major Under
	4	Analog 3 Major Over
	9-16	Control
	17-32	Value
Display 4	33	Analog 4 Minor Under
	34	Analog 4 Minor Over
	35	Analog 4 Major Under
	36	Analog 4 Major Over
	41-48	Control
	49-64	Value
Display	Point	Description
	1	Analog 5 Minor Under
	2	Analog 5 Minor Over
	3	Analog 5 Major Under
	4	Analog 5 Major Over
	9-16	Control
	17-32	Value
Display 5	33	Analog 6 Minor Under
	34	Analog 6 Minor Over
	35	Analog 6 Major Under
	36	Analog 6 Major Over
	41-48	Control
	49-64	Value
Display	Point	Description
	1	Analog 7 Minor Under
	2	Analog 7 Minor Over
	3	Analog 7 Major Under
	4	Analog 7 Major Over
	9-16	Control
	17-32	Value
Display 6	33	Analog 8 Minor Under
	34	Analog 8 Minor Over
	35	Analog 8 Major Under
	36	Analog 8 Major Over
	41-48	Control
	49-64	Value
Display	Point	Description
	1	Digital sensor 1 Minor Under
Display 7	2	Digital sensor 1 Minor Over
	3	Digital sensor 1 Major Under

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

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

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

Display	Point	Description
	1	Digital sensor 7 Minor Under
	2	Digital sensor 7 Minor Over
	3	Digital sensor 7 Major Under
	4	Digital sensor 7 Major Over
	5	Digital sensor 7 Sensor not detected
Display 10	9-16	Control
	17-32	Value
	33	Digital sensor 8 Minor Under
	34	Digital sensor 8 Minor Over
	35	Digital sensor 8 Major Under
	36	Digital sensor 8 Major Over

	37	Digital sensor 8 Sensor not detected
	41-48	Control
	49-64	Value

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

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

Display	Point	Description
	1	Digital sensor 13 Minor Under
	2	Digital sensor 13 Minor Over
	3	Digital sensor 13 Major Under
	4	Digital sensor 13 Major Over
	5	Digital sensor 13 Sensor not detected
	9-16	Control
	17-32	Value
Display 13	33	Digital sensor 14 Minor Under
	34	Digital sensor 14 Minor Over
	35	Digital sensor 14 Major Under
	36	Digital sensor 14 Major Over
	37	Digital sensor 14 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 15 Minor Under
Display 14	2	Digital sensor 15 Minor Over
	3	Digital sensor 15 Major Under

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

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

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

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

	37	Digital sensor 22 Sensor not detected
	41-48	Control
	49-64	Value

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

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

Display	Point	Description
	1	Digital sensor 27 Minor Under
	2	Digital sensor 27 Minor Over
	3	Digital sensor 27 Major Under
	4	Digital sensor 27 Major Over
	5	Digital sensor 27 Sensor not detected
	9-16	Control
	17-32	Value
Display 20	33	Digital sensor 28 Minor Under
	34	Digital sensor 28 Minor Over
	35	Digital sensor 28 Major Under
	36	Digital sensor 28 Major Over
	37	Digital sensor 28 Sensor not detected
	41-48	Control
	49-64	Value

Display	Point	Description
	1	Digital sensor 29 Minor Under
Display 21	2	Digital sensor 29 Minor Over
	3	Digital sensor 29 Major Under

	4	Digital sensor 29 Major Over
	5	Digital sensor 29 Sensor not detected
	9-16	Control
	17-32	Value
	33	Digital sensor 30 Minor Under
	34	Digital sensor 30 Minor Over
	35	Digital sensor 30 Major Under
	36	Digital sensor 30 Major Over
	37	Digital sensor 30 Sensor not detected
	41-48	Control
	49-64	Value
Display	**Point**	**Description**
	1	Digital sensor 31 Minor Under
	2	Digital sensor 31 Minor Over
	3	Digital sensor 31 Major Under
	4	Digital sensor 31 Major Over
	5	Digital sensor 31 Sensor not detected
	9-16	Control
	17-32	Value
Display 22	33	Digital sensor 32 Minor Under
	34	Digital sensor 32 Minor Over
	35	Digital sensor 32 Major Under
	36	Digital sensor 32 Major Over
	37	Digital sensor 32 Sensor not detected
	41-48	Control
	49-64	Value

14.2 System Alarms

Display	Point	Description
1	33	Default Configuration
	34	DIP Switch Configuration
	35	MAC Address not set
	36	IP address not set
	37	LAN hardware error
	38	SNMP processing error
	39	SNMP community error
	40	LAN TX packet drop
	41	Notification 1 failed
	42	Notification 2 failed
	43	Notification 3 failed
	44	Notification 4 failed
	45	Notification 5 failed
	46	Notification 6 failed
	47	Notification 7 failed
	48	Notification 8 failed
	49	NTP failed
	50	Time Tick
	51	Serial 1 receive queue full
	52	Dynamic memory full
	53	Unit reset
	54	DCP poller inactive
	55	TRIP error
	56	No dial tone
	57	Modem failed
	58	Meter 1 failed
	59	Meter 2 failed
	60	Meter 3 failed

System Alarms

14.3   SNMP Manager Functions

The SNMP Manager allows the user to view alarm status, set date/time, issue controls, and perform a resync. The display and tables below outline the MIB object identifiers. The table below begins with dpsRTU; however, the MIB object identifier tree has several levels above it. The full English name is as follows: root.iso.org.dod.internet.private.enterprises.dps-lnc.dpsAlarmControl.dpsRTU. Therefore, dpsRTU's full object identifier is 1.3.6.1.4.1.2682.1.2. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the Control Grid is 1.3.6.1.4.1.2682.1.2.3.3 because the object identifier of dpsRTU is 1.3.6.1.4.1.2682.1.4 + the Control Grid (.3) + the Display (.3).
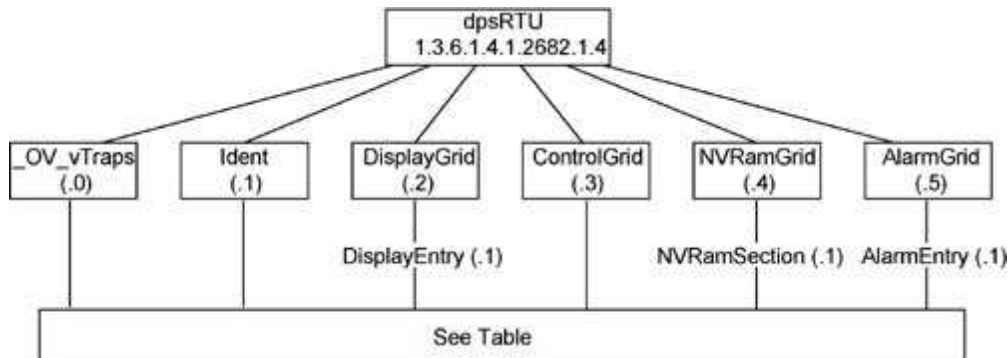
Tbl. B1 (0.)_OV_Traps points
_OV_vTraps (1.3.6.1.4.1.2682.1.2.0)
PointSet (.20)
PointClr (.21)
SumPSet (.101)
SumPClr (.102)
ComFailed (.103)
ComRestored (.014)
P0001Set (.10001) through P0064Set (.10064)
P0001Clr (.20001) through P0064Clr (.20064)

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

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

Tbl. B3 (.3) ControlGrid points
ControlGrid (1.3.6.1.4.1.2682.1.2.3)
Port (.1)
Address (.2)
Display (.3)
Point (.4)
Action (.5)

Tbl. B6 (.6) Analog Channels
Channel Entry (1.3.6.1.4.1.2682.1.4.6.1)
Channel Number (.1)
Enabled (.2)
Description (.3)
Value (.4)
Thresholds (.5)*
*If Mj, Mn is assumed

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

14.4 SNMP Granular Trap Packets

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

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 SUI) **OR**
2. The SNMP manager reads the description from the Trap.

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

UDP Headers and descriptions

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

SNMP Headers and descriptions

14.5   DNP3 Configuration / Interoperability Guide

14.5.1 DNP v3.0 Device Profile

The following table provides a "Device Profile Document" in the standard format defined in the DNP 3.0 Subset Definitions Document. While it is referred to in the DNP 3.0 Subset Definitions as a "Document," it is in fact a table, and only a component of a total interoperability guide.

DNP V3.0	
DEVICE PROFILE DOCUMENT (Also see the DNP 3.0 Implementation Table in Section 4.6.2)	
Vendor Name: **DPS Telecom Inc.**	
Device Name: **NetGuardian SUI**	

Highest DNP Level Supported:
 	
   For Requests: **Level 3**
 	
   For Responses: **Level 3**
	Device Function:
	
	   ☐ Master
	
	   ☒ Slave

Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP Levels Supported (the complete list is described in the attached table): **The read function code for Object 50 (Time and Date), variation 1, is supported.**	

Maximum Data Link Frame Size (octets):
 	
   Transmitted: **292**
   Received: **292**
	Maximum Application Fragment Size (octets):
	
	   Transmitted: **512**
	   Received: **512**

Maximum Data Link Re-tries:
 	
   ☐ None
   ☒ **Fixed (3)**
	Maximum Application Layer Re-tries:
	
	   ☒ **None**
	   ☐ Configurable

Requires Data Link Layer Re-tries:
 	
   Fixed (3)
   ☐ Always
   ☐ Sometimes	

Requires Application Layer Confirmation:

- ☐ Never
- ☐ Always
- ☐ When reporting Event Data (Slave devices only)
- ☒ **When sending multi-fragment responses (Slave devices only)**
- ☐ Sometimes

DNP V3.0

DEVICE PROFILE DOCUMENT
(Also see the DNP 3.0 Implementation Table in Section 4.6.2)

Timeouts while waiting for:

Data Link Confirmation:	**Fixed at 2s**
Complete Appl. Fragment:	**None**
Application Confirm:	**Fixed at 10s**
Complete Appl. Response:	**None**
Other:	**Transmission Delay, 0**

Sends/Executes Control Operations:

WRITE Binary Outputs: **Never**
SELECT/OPERATE: **Always**
DIRECT OPERATE: **Never**
DIRECT OPERATE - NO ACK: **Never**

Count > 1: **Never**
Pulse On: **Never**
Pulse Off: **Never**
Latch On: **Always**
Latch Off: **Always**

Queue: **Never**
Clear Queue: **Never**

Reports Binary Input Change Events when no specific variation requested:	Reports time-tagged Binary Input Change Events when no specific variation requested:
☒ **Never**	☒ **Never**
☐ Only time-tagged	☐ Binary Input Change With Time
☐ Only non-time-tagged	☐ Binary Input Change with Relative Time
Sends Unsolicited Responses	Sends Static Data in Unsolicited Responses:
☒ **Never**	☒ **Never**
☐ Only certain objects	☐ When Device Restarts
☐ Sometimes (attach explanation)	☐ When Status Flags Change
☐ ENABLE/DISABLE UNSOLICITED Function codes supported	

Default Counter Object/Variation: ☒ **No Counters Reported** ☐ Default Object	Counters Roll Over at: ☒ **No Counters Reported** ☐ Configurable (attach explanation) ☐ 16 Bits ☐ 32 Bits ☐ Other Value: _____ ☐ Point-by-point list attached

DNP V3.0

DEVICE PROFILE DOCUMENT

(Also see the DNP 3.0 Implementation Table in Section 4.6.2)

Sends Multi-Fragment Responses:
☒ **No**

☐Yes

Sequential File Transfer Support: **No**
Append File Mode: **No**
Custom Status Code Strings: **No**
Permissions Field: **No**
File Events Assigned to Class: **No**
File Events Send Immediately: **No**
Multiple Blocks in a Fragment: **No**
Max Number of Files Open: **0**

14.5.2 DNP V3.0 Implementation Table

The following table identifies which object variations, function codes, and qualifiers the NetGuardian SUI supports in both request messages and in response messages. For static (non-change-event) objects, request send with qualifiers 00, 01, 06, 07, or 08 will be responded with qualifiers 00 or 01.

OBJECT			REQUEST (Library will parse)		RESPONSE (Library will respond with)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifiers Codes (hex)	Function Codes (dec)	Qualifiers Codes (hex)
1	1	Binary Input	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
10	2	Binary Output Status	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
12	1	Control Relay Output Block	5 (direct op) 6 (dir. op, noack)	17, 28 (index)	129 (response)	echo of request
30	3	32-Bit Analog Input Without Flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
50	1	Time and Date	1 (read)	07 (limited qty = 1)	129 (response)	07 (limited qty = 1)
			2 (write)	07 (limited qty = 1)		
60	1	Class 0 Data	1 (read)	06 (no range, or all)		
60	2	Class 1 Data	1 (read)	06 (no range, or all)		
60	3	Class 2 Data	1 (read)	06 (no range, or all)		
60	4	Class 3 Data	1 (read)	06 (no range, or all)		

14.5.3 DNP V3.0 Point List

The tables below identify all the default data points provided by the NetGuardian 216 G3 DNP3.

Binary Input Points

Binary Input Points Static Variation: Obj 01 Var 01 - Binary Input w/o status Request function codes supported: 1 (read)		
Point Index	**Description**	**Class**
0-5	Discrete Alarms	1
6-15	Unused	1
16-17	Base Controls	1
18-31	Unused	1
32	(33) Default Configuration	1
33	(34) DIP Switch Configuration	1
34	(35) MAC Address not set	1
35	(36) IP address not set	1
36	(37) LAN hardware error	1
37	(38) SNMP processing error	1
38	(39) SNMP community error	1
39	(40) LAN TX packet drop	1
40	(41) Notification 1 failed	1
41	(42) Notification 2 failed	1
42	(43) Notification 3 failed	1
43	(44) Notification 4 failed	1
44	(45) Notification 5 failed	1
45	(46) Notification 6 failed	1
46	(47) Notification 7 failed	1
47	(48) Notification 8 failed	1
48	(49) NTP failed	1
49	(50) Time Tick	1
50	(51) Serial 1 receive queue full	1
51	(52) Dynamic memory full	1
52	(53) Unit reset	1
53	(54) DCP poller inactive	1
54	(55) TRIP error	1
55	(56) No dial tone	1
56	(57) Modem failed	1
57	(58) Meter 1 failed	1
58	(59) Meter 2 failed	1
59	(60) Meter 3 failed	1

Binary Output Status Points and Control Relay Output Blocks

The following table lists both the Binary Output Status Points (Object 10) and the Control relay Output Blocks (Object 12).

Binary Output Status Points Static Variation: Obj 10 Var 02 - Binary Output Status Control Variation: Obj 12 Var 01 - Control Relay Output Block Request function codes supported: 3 (select), 4 (operate) Supported relay output: Latch on, Latch off.		
Point ID	**Description**	**Class**
0	Base control 1	2
1	Base control 2	2

Analog Inputs

The following table lists Analog Inputs (Object 30). It is important to note that Analog Inputs, Analog Output Control Blocks, and Analog Output Statuses are transmitted through DNP as signed numbers.

Analog Inputs Static Variation: Obj 30 Var 03 - 32-Bit analog w/o flag Request function codes supported: 1 (read)				
Point ID	**Description**	**Default Unit**	**Scaling**	**Class**
0	Meter 1 Interval Demand	kW	0.01	3
1	Meter 2 Interval Demand	kW	0.01	3
2	Meter 3 Interval Demand	kW	0.01	3
3	Meter 1 Interval Energy	kWh	0.01	3
4	Meter 2 Interval Energy	kWh	0.01	3
5	Meter 3 Interval Energy	kWh	0.01	3
6	Meter 1 Energy Count	Count	1	3
7	Meter 2 Energy Count	Count	1	3
8	Meter 3 Energy Count	Count	1	3
9	Meter 1 Total Count	Count	1	3
10	Meter 2 Total Count	Count	1	3
11	Meter 3 Total Count	Count	1	3

15 Frequently Asked Questions

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

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

15.1 General FAQs

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

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

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

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

15.2   SNMP FAQs

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

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

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

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

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

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

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

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

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

16 Technical Support

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

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

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

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

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

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

17 End User License Agreement

All Software and firmware used in, for, or in connection with the Product, parts, subsystems, or derivatives thereof, in whatever form, incluSUlg, without limitation, source code, object code and microcode, incluSUlg 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 excluSUlg the provisions of the UN Convention on Contracts for the International Sale of Goods. Any dispute arising out of the Agreement shall be commenced and maintained only in Fresno County, California. In the event suit is brought or an attorney is retained by any party to this Agreement to seek interpretation or construction of any term or provision of this Agreement, to enforce the terms of this Agreement, to collect any money due, or to obtain any money damages or equitable relief for breach, the prevailing party shall be entitled to recover, in addition to any other available remedy, reimbursement for reasonable attorneys' fees, court costs, costs of investigation, and other related expenses.

Warranty

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

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

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

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

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

Technical Support

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

Free Tech Support is Only a Click Away

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

www.DpsTelecom.com

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

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

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

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

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

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

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

Free Tech Support on the Web: MyDPS

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

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

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