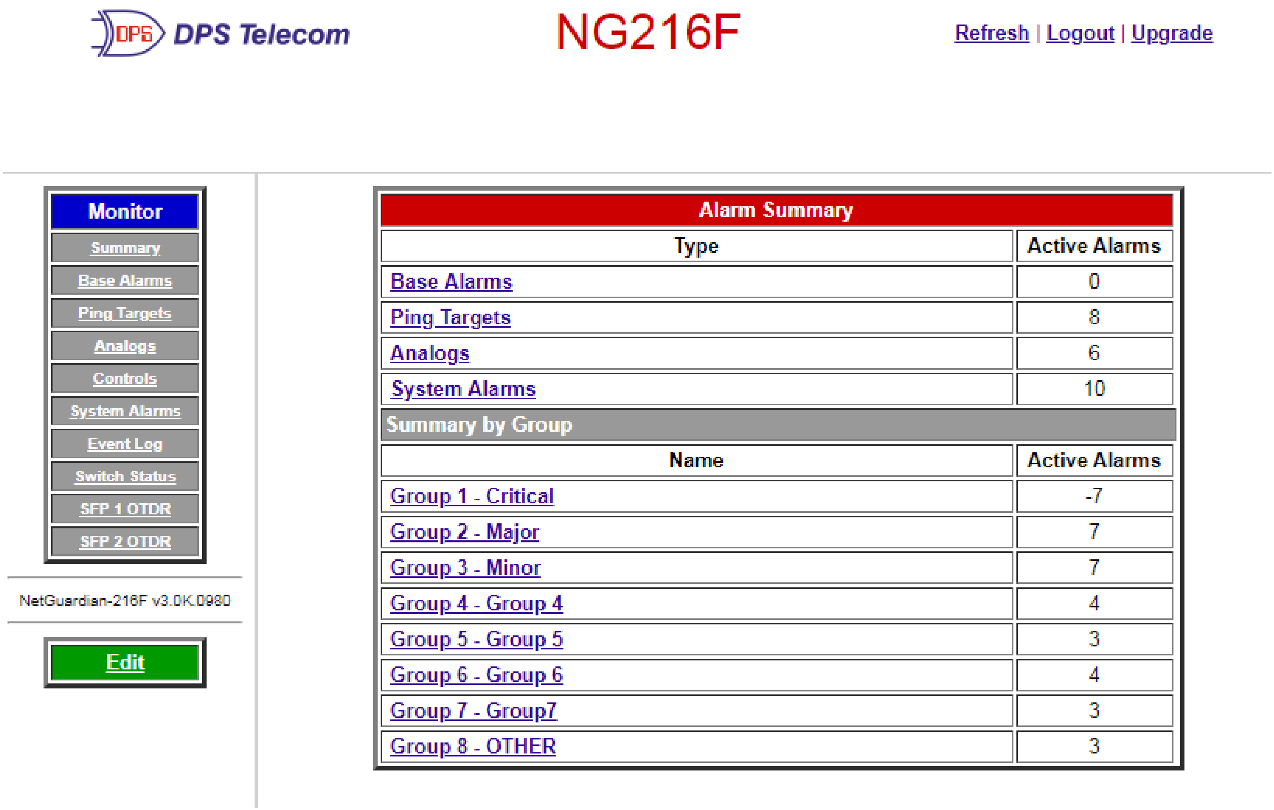
DPS Telecom
"Your Partners in Network Alarm Monitoring"

NetGuardian 216F Web Browser

USER MANUAL



Alarm Summary	
Type	Active Alarms
Base Alarms	0
Ping Targets	8
Analogs	6
System Alarms	10
Summary by Group	
Name	Active Alarms
Group 1 - Critical	-7
Group 2 - Major	7
Group 3 - Minor	7
Group 4 - Group 4	4
Group 5 - Group 5	3
Group 6 - Group 6	4
Group 7 - Group7	3
Group 8 - OTHER	3

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

March 19, 2019 **D-UM-216FW**

Revision History

March 19, 2019	Minor updates
March 27, 2018	General Updates. Added SFP 1&2 sections. Added Point Group Sections. Updated images throughout.
May 20, 2011	Added instructions for new VLAN tagging feature
March 10, 2011	Included instructions for enabling periodic analog traps and the alternative analog trap format
June 3, 2009	Revisions for Building Access Controller
December 18, 2008	NetGuardian 216F Web Browser UM (D-OC-UM08C.18100) released.

Notice

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

Contents

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

1 Overview 1

1.1 Introduction 1

1.2 Potential Problems using Web Interface in a Secure Proxy Network 3

1.3 NetGuardian 216F Features 3

2 Unit Configuration 4

2.1 Logging on to the NetGuardian 4

2.2 Entering System Settings 4

2.3 Changing the Logon Password 5

2.3.1 User Logons 6

2.4 Configuring Port Parameters 7

2.4.1 Ethernet Ports 7

2.4.2 Setting Up SNMP 8

2.4.3 Trusted Hosts Config and Operation 9

2.4.4 Changing Craft Port Communication Settings 11

2.5 Defining Point Groups 11

2.6 Configuring Base Discrete Alarms 11

2.7 Event Qualification Timers 13

2.8 Setting System Alarm Notifications 14

2.9 Configuring Ping Targets 15

2.10 Analog Parameters 15

2.10.1 Integrated Temperature and Battery Sensor 16

2.10.2 Analog Polarity Override 17

2.10.3 Analog Step Sizes 17

2.10.4 SFP 1&2 Analog Readings 17

2.11 Configuring the Control Relays 19

2.11.1 Activating Relays from an Alarm Point's Change of Status 19

2.11.2 Derived Control Relays and Virtual Alarming 19

2.11.3 Relay Operating 20

2.11.3.1 Normal Mode 20

2.11.4 Override Default Relay Momentary Time Using Event Qualification 20

2.12 Setting System Timers 21

2.13 Setting the System Date and Time 22

2.14 Saving Changes or Resetting Factory Defaults 23

2.15 Rebooting the NetGuardian 23

3 Web Server Monitoring 24

3.1 Alarm Summary Window 24

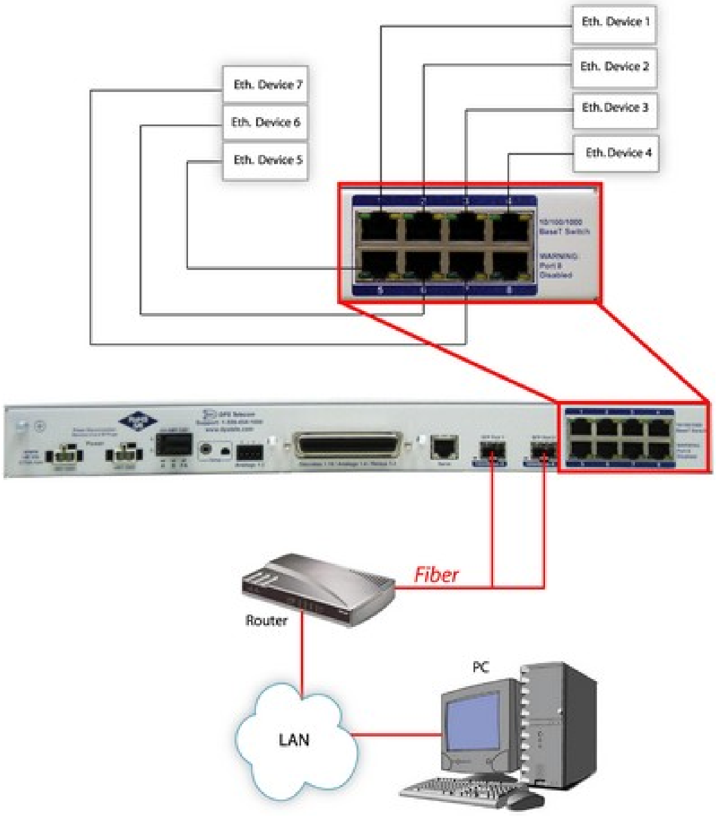
3.2 Monitoring Base Alarms 24
3.3 Monitoring Ping Targets 25
3.4 Monitoring Analogs 25
3.5 Operating Controls 25
3.6 Monitoring System Alarms 26
3.7 Event Logging 27
3.8 Monitoring Data Port Activity 28
4 Reference Section 29
4.1 Display Mapping 29
4.1.1 System Alarms Display Map 31
4.2 SNMP Manager Functions 32
4.3 SNMP Granular Trap Packets 34
4.4 ASCII Conversion 35
5 Frequently Asked Questions 36
5.1 General FAQs 36
5.2 SNMP FAQs 39
6 Technical Support 40

1 Overview

The NetGuardian 216F monitors alarms, pings network elements, and reports via SNMP, pager, or email

1.1 Introduction

The NetGuardian's Web Browser Interface lets you manage alarms and configure the unit through the Internet or your Intranet. You can quickly set up alarm point descriptions, view alarm status, issue controls, configure paging information, and more. The NetGuardian supports Internet Explorer versions 4.0 and above and Netscape Navigator versions 4.7 and above.



NetGuardian 216F has the capacity to monitor IP aware devices' network presence and also interfaces discrete alarm points and controls at your network sites.

1.2 Potential Problems using Web Interface in a Secure Proxy Network

Using the Web Browser Interface for the NetGuardian in a secure proxy network can cause certain problems to occur. If you are logged on to the NetGuardian from within your network through a proxy, and another user from within your network tries to access the same NetGuardian, the second user will not need to login to the NetGuardian. Both users will essentially be logged in using the same IP address because of the masking done by the proxy server.

1.3 NetGuardian 216F Features

NetGuardian 216F includes the following features:

Two SFP Ports:
You can use any industry-standard SFP interface.

Integrated 10/100/1000-BaseT Switch: 7 hubed Ethernet ports reduces equipment necessary for your remote site.

SNMPv1, v2c, and v3 Support and Robust Message Delivery
NetGuardian 216F supports SNMP v2c, SNMPv3, and the SNMP INFORM command, which permits robust delivery of alarm notification to your SNMP manager.

Global Support for Dual SNMP Managers
NetGuardian 216F supports sending all SNMP TRAP and INFORM notifications to **two** global SNMP managers. This makes it easier to configure a secondary SNMP manager and frees up your NetGuardian configuration for additional notification devices and more flexible alarm reporting. You can easily send an alarm to your primary SNMP manager at the NOC; to a secondary backup SNMP manager at another location; to the pager of the on-call technician; and the email in-box of the technician's supervisor.

Filter or Reset the NetGuardian Event Log
The NetGuardian Event Log supports the following NetGuardian 216F features:

- You can reset the Event Log, to clear old alarms from the display.
- You can reset the Event Log by Alarm Point Group; for example, clear power alarms while retaining intruder alarms.

2 Unit Configuration

2.1 Logging on to the NetGuardian

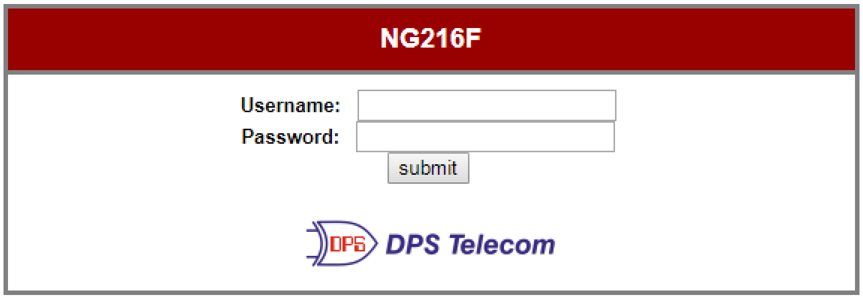
For Web Interface functionality, the unit must first be configured with some basic network information. If this step has not been done, refer to the NetGuardian User Manual for initial software configuration setup.

1. To connect to the NetGuardian from your Web browser, you must know its IP address or domain name if it has been registered with your internal DNS. Enter it in the address bar of your Web browser. It may be helpful to bookmark the login page to simplify access.
2. After connecting to the NetGuardian's IP address, enter your password and click Submit (see image below). Note: The factory default username and password is dpstelecom.
3. In the left frame there is a blue Monitor menu section and a green Edit menu button. Most of the software configuration will occur in the Edit menu. The following sections provide detailed information regarding these functions.

Hot Tip!

If the Edit menu does not appear in the left frame after logging on, it means that another station has already logged on as the primary user. The maximum number of users allowed to simultaneously access the NetGuardian via Web is four. The primary user is the only user with access to the editing features.

Exiting the Web interface without logging out prevents other users from accessing the Editing features, as well. Web sessions are tracked by IP address and the session will time out after twelve minutes of inactivity, unless configured with a longer Web timeout duration. (See section "Setting System Timers" for more information.)

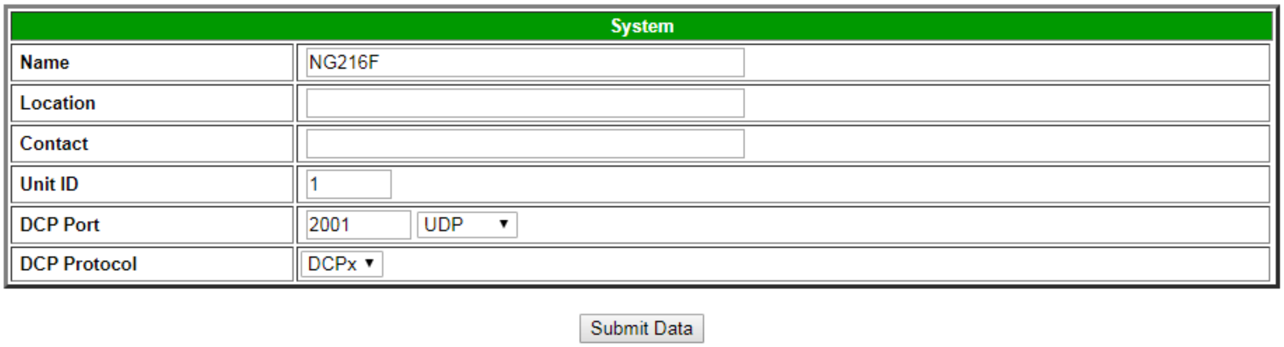


Enter your password to enter the NetGuardian Web Browser Interface.

2.2 Entering System Settings

From the **System** screen you can enter the name, location, contact, features, and SNMP community names.

Use the following steps to define your NetGuardian system information:
1. From the **Edit** menu choose **System** (see image below).
2. Enter the designated user name for your NetGuardian.*
3. Enter the location or address of the NetGuardian.*
4. Set the contact by entering the telephone number or other contact information for the person or group responsible for this NetGuardian.
5. Click **Submit** to save your system information settings.



System

Name	NG216F
Location	
Contact	
Unit ID	1
DCP Port	2001 UDP ▾
DCP Protocol	DCPx ▾

Configure the system information by selecting the System screen from the Edit menu.

Field	Description
Name	Used to set the Name@Location email address. **Note:** Name is the portion before the @ character.
Location	Used to set the Name@Location email address. **Note:** Location is the portion after the @ character, this is a host name or IP address.
Contact	Information for how to contact the person responsible for this NetGuardian.
Unit ID	User definable ID number for this NetGuardian (DCP Address).
DCP Port	Enter the DCP Port for this NetGuardian. (serial or UDP/IP Port)
DCP Protocol	Default DCP protocol is DCPx, but can be changed to DCPf.

System fields

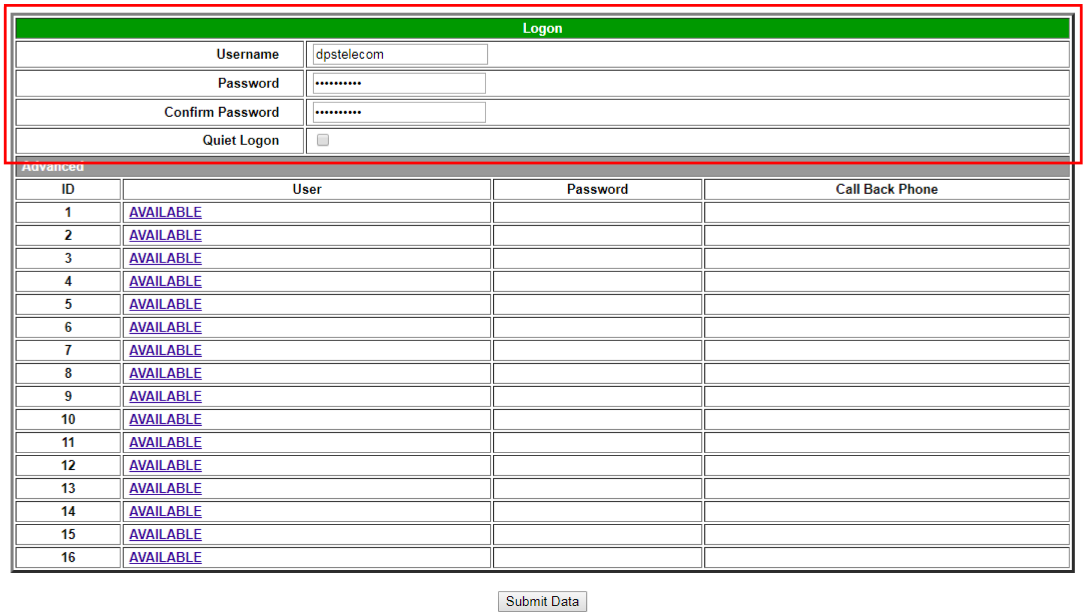
2.3 Changing the Logon Password

The master password can be configured from the **Edit** menu > **Logon** screen, in the top section. The minimum password length is four characters; however, DPS recommends setting the minimum password length to at least five characters. You can also configure security logon profiles to individual access rights in the **Logon Profile** screen.

Note: The factory default username and password is **dpstelecom**. DPS Telecom strongly recommends that these defaults be changed.

Use the following steps to change the logon password:

1. From the **Edit** menu select **Logon**.
2. Enter your new password in the **Password** and **Confirm Password** fields.
3. Click the **Submit Data** button.



Logon

Username	dpstelecom
Password	••••••••••
Confirm Password	••••••••••
Quiet Logon	□

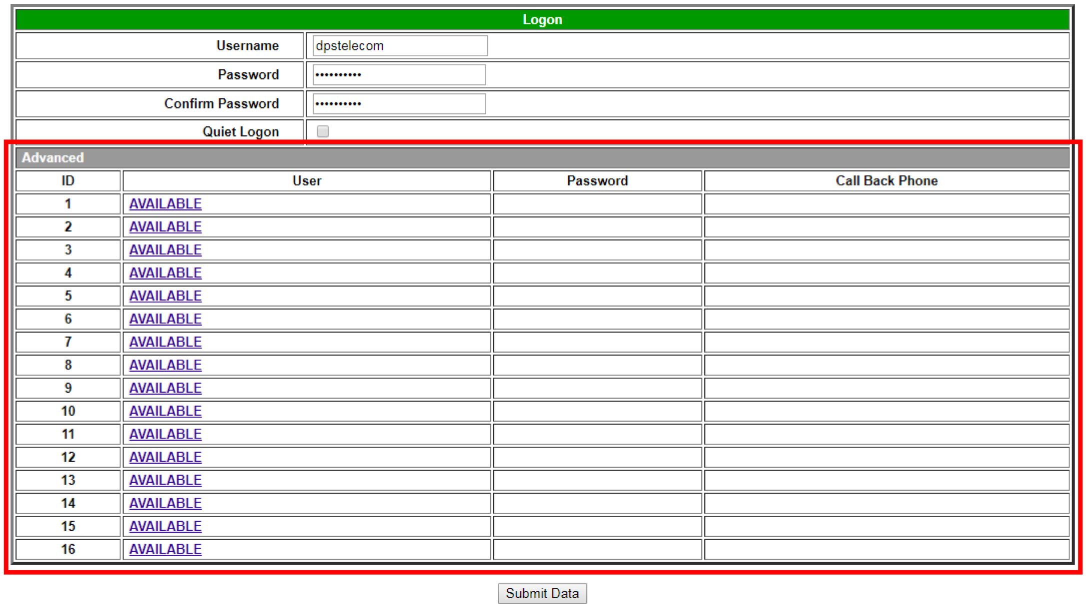
Advanced

ID	User	Password	Call Back Phone
1	AVAILABLE		
2	AVAILABLE		
3	AVAILABLE		
4	AVAILABLE		
5	AVAILABLE		
6	AVAILABLE		
7	AVAILABLE		
8	AVAILABLE		
9	AVAILABLE		
10	AVAILABLE		
11	AVAILABLE		
12	AVAILABLE		
13	AVAILABLE		
14	AVAILABLE		
15	AVAILABLE		
16	AVAILABLE		

Configure the password parameters from the Logon screen.

2.3.1 User Logons

In the Advanced section of the **Edit** menu **> Logon** page, you have the ability to define up to 16 user profiles.



Logon

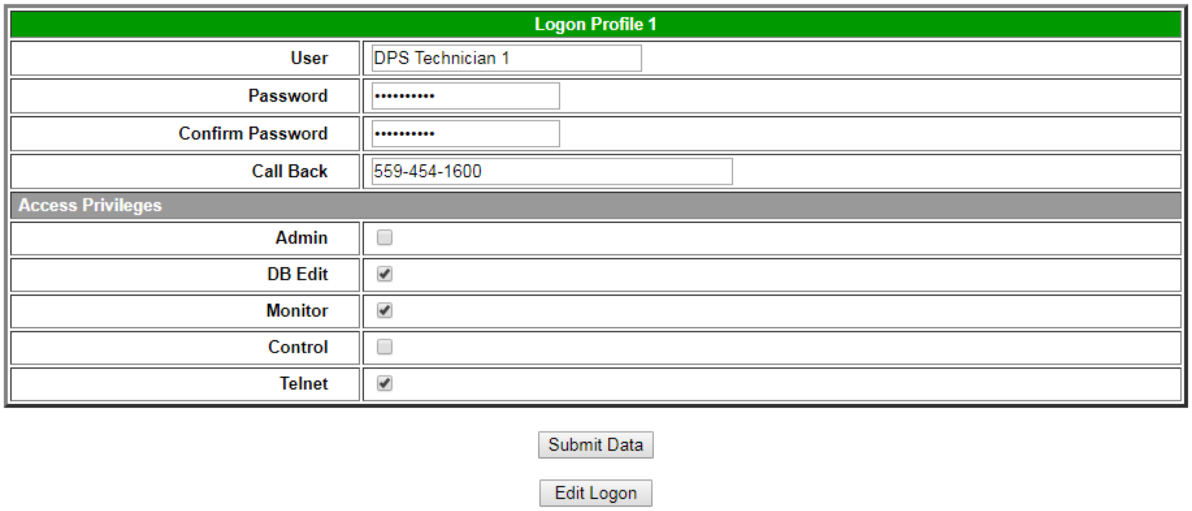
Username	dpstelecom
Password	••••••••••
Confirm Password	••••••••••
Quiet Logon	□

Advanced

ID	User	Password	Call Back Phone
1	AVAILABLE		
2	AVAILABLE		
3	AVAILABLE		
4	AVAILABLE		
5	AVAILABLE		
6	AVAILABLE		
7	AVAILABLE		
8	AVAILABLE		
9	AVAILABLE		
10	AVAILABLE		
11	AVAILABLE		
12	AVAILABLE		
13	AVAILABLE		
14	AVAILABLE		
15	AVAILABLE		
16	AVAILABLE		

*Advanced section of the **Edit** menu **> Logon** page.*

By clicking on the AVAILABLE link under the **User** column of this menu, you will be able to configure individual credentials and access rights for each user, as shown below.



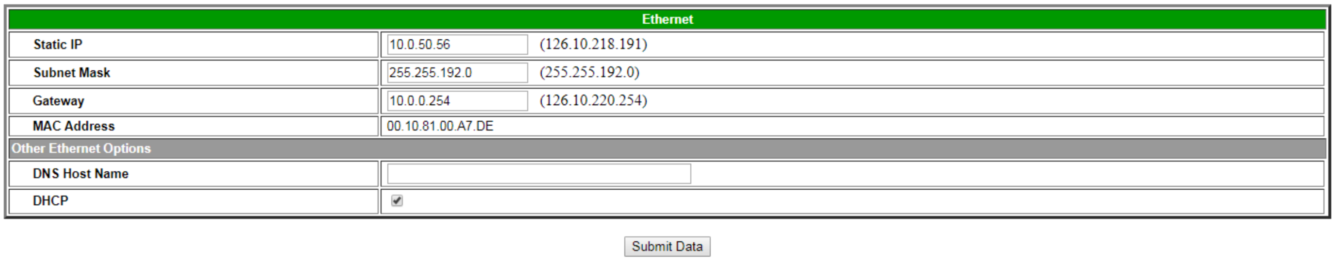
Logon Profile 1	
User	DPS Technician 1
Password	••••••••••
Confirm Password	••••••••••
Call Back	559-454-1600
Access Privileges	
Admin	□
DB Edit	☑
Monitor	☑
Control	□
Telnet	☑

Configure user credentials and access rights.

2.4 Configuring Port Parameters

2.4.1 Ethernet Ports

Use the following steps to configure the Ethernet port settings:
1. Configure the NetGuardian ethernet port by clicking on the Ethernet link from the Edit menu.
2. Enter the appropriate information for your ethernet port in the corresponding fields. Refer to the image below.
3. Click Submit Data to save your configuration settings.



Ethernet		
Static IP	10.0.50.56	(126.10.218.191)
Subnet Mask	255.255.192.0	(255.255.192.0)
Gateway	10.0.0.254	(126.10.220.254)
MAC Address	00.10.81.00.A7.DE	
Other Ethernet Options		
DNS Host Name		
DHCP	☑	

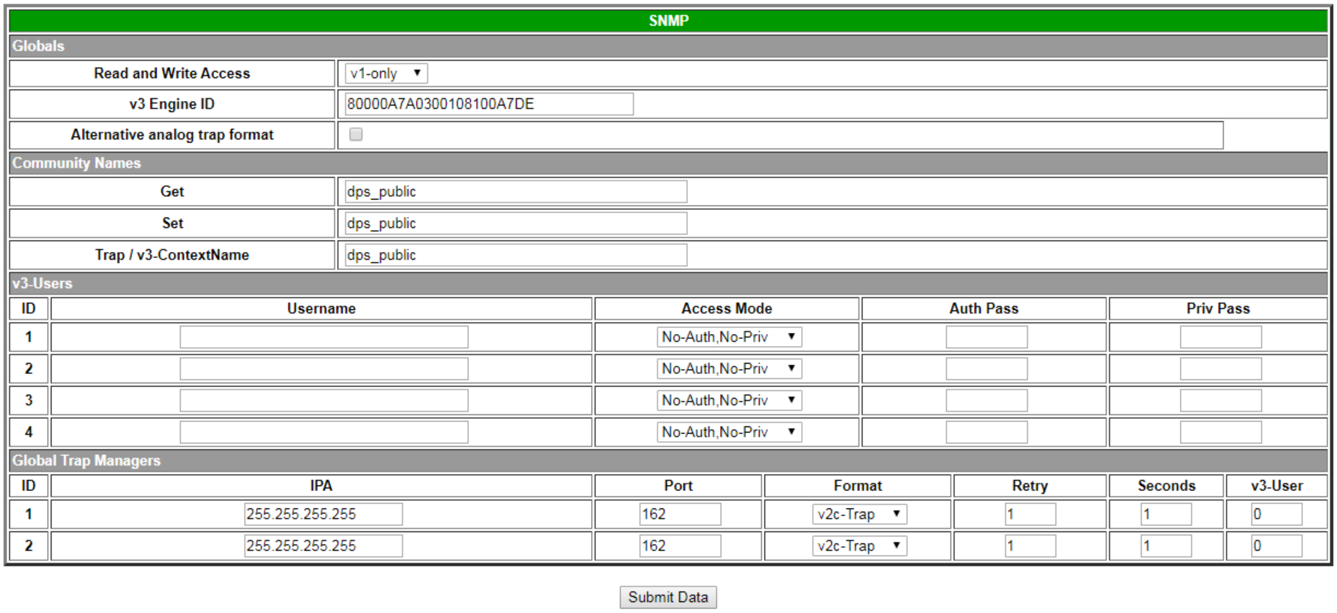
Ethernet port configuration is accomplished from the Edit menu > Ethernet screen.

Field	Description
Static Address	IP address of the NetGuardian
Subnet Mask	The Subnet mask is a road sign to the NetGuardian telling it whether your packets should stay on your local network or be forwarded somewhere else on a wide area network.
Default Gateway	An important parameter if you are on a network that is connected to a wide area network. It tell the NetGuardian which machine is the gateway out of your local network. Set to 255.255.255.255 if not using .
MAC Address	Hardware address of the NetGuardian (not editable, for reference only).
DNS Address	IP address of the domain name server. Set to 255.255.255.255 if not using.
DHCP	Toggles the Dynamic Host Connection Protocol On or Off

Fields in the Edit > Ethernet screen

2.4.2 Setting Up SNMP

Use the following steps to define your NetGuardian system information:
1. From the **Edit** menu choose **SNMP** (see image below).
2. Set **Read and Write Access** to **All**, **v1-Only**, **v2c-Only**, or **v3-Only.**
3. Enter the community name for SNMP GET requests.
4. Enter the community name for SNMP SET requests.
5. In the Trap/v3-ContextName field, enter the community name for SNMP TRAPs.
6. Under Global Trap Managers, define the IP address of your trap manager. (Set to 255.255.255.255 if not using.)
7. Define the UDP port set by the SNMP manager to receive traps; usually 162.
8. Select the Format in which you want your traps to be sent to your manager in.
9. Click **Submit** to save your system information settings.



SNMP

Globals

Read and Write Access	v1-only ▼
v3 Engine ID	80000A7A0300108100A7DE
Alternative analog trap format	☐

Community Names

Get	dps_public
Set	dps_public
Trap / v3-ContextName	dps_public

v3-Users

ID	Username	Access Mode	Auth Pass	Priv Pass
1		No-Auth,No-Priv ▼		
2		No-Auth,No-Priv ▼		
3		No-Auth,No-Priv ▼		
4		No-Auth,No-Priv ▼		

Global Trap Managers

ID	IPA	Port	Format	Retry	Seconds	v3-User
1	255.255.255.255	162	v2c-Trap ▼	1	1	0
2	255.255.255.255	162	v2c-Trap ▼	1	1	0

SNMP Menu

Globals	
Read and Write Access	This field defines how the NetGuardian unit may be accessed via SNMP. This can be set to the following: • All- Allows you to read or write using any version of SNMP (v1, v2c, v3) • Disabled- Restricts all access to unit via SNMP • v1-Only- Allows SNMPv1 access only • v2c-Only- Allows SNMPv2c access only • v3-Only- Allows SNMPv3 access only
v3 Engine ID	Specifies the v3 Engine ID for your NetGuardian device. DPS recommends using the default ID for the unit, which is automatically generated by the unit.The default ID is generated according to RFC3411 and is based on the unit's unique MAC address and DPS Telecom's SNMP enterprise number. **Note:** To have the unit generate a unique Engine ID, clear the **v3 Engine ID** field and press the **Submit** key.
Community Names	
Get	Community name for SNMP requests
Set	Community name for SNMP SET requests
Trap - v3-ContextName	Community name for SNMP TRAP requests. In SNMP v3, defines the context name field of a v3-Trap. **Note:** Make sure that your community strings match those used by the SNMP manager. In v1 and v2c, community strings are security passwords; if the strings do

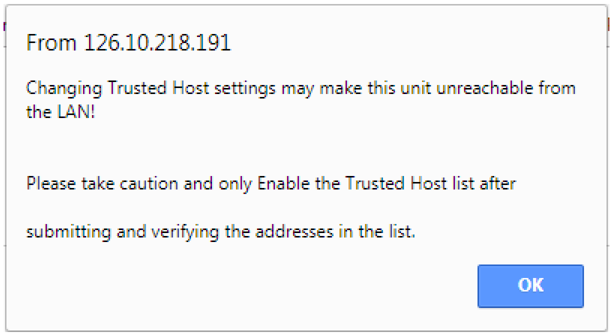
	not match, the SNMP manager will not accept Traps from the NetGuardian 216F. Community strings are case sensitive.
v3 Users	
ID	The user number designated for a v3-user. The NetGuardian G5 supports up to four v3-User profiles.
User Name	The name of the user for which an SNMPv3 management operation is performed.
Access Mode	This identifies the security modes available when SNMPv3 is utilitized. The modes are as follows: • **No-Auth, No-Priv-** This access mode does not require authentication and does not require encryption. This mode is the least secure and is comparable to v1 and v2c. • **Auth-MD5,No-Priv-** Provides authentication based on the MD5 algorithm and does not require encryption. • **Auth-SHA,No-Priv-** Provides authentication based on the SHA algorithm and does not require encryption. • **Priv Auth-MD5-** Provides authentication based on the MD5 algorithm and provides DES 56-bit encryption based on the CBC-DES standard. • **Priv Auth-SHA-** Provides authentication based on the SHA algorithm and provides DES 56-bit encryption based on the CBC-DES standard.
Auth Pass	This field contains the password used with either MD5 or SHA authentication algorithms.
Priv Pass	This field contains the password used with privatization encryption.
Global Trap Managers	
IPA	Defines the SNMP trap manager's IP address. Set to 255.255.255.255 if not using.
Port	The SNMP port is the UDP port set by the SNMP manager to receive traps, usually set to 162
Format	Select between SNMPv1 TRAP, v2c TRAP, v2c INFORM, and v3 TRAP.
Retry	Number of times the NetGuardian 216F will resend SNMP v2c-Informs
Seconds	Time interval in seconds between attempts to resend SNMP v2c-Informs.
v3 User	Association to the v3-User Table is made to specify the username, security mode, and passwords that should be used for sending a v3-Trap.

Fields in the Edit > SNMP settings

2.4.3 Trusted Hosts Config and Operation

The Trusted Host List allows you to increase the NetGuardian's network security by allowing or blocking packets from specified IP addresses. Addresses which appear in the table will be processed by the NetGuardian. Defined IP addresses associated with network cameras or the network time server are automatically processed and will not be filtered out by this feature. Broadcast packets of 255.255.255.255 and ARP requests for the NetGuardian IP address are also not filtered.

1. From the **Edit** menu select **Trusted Hosts**.
2. A warning prompt will appear (see image below). Click OK to continue, or exit to cancel.



From 126.10.218.191

Changing Trusted Host settings may make this unit unreachable from the LAN!

Please take caution and only Enable the Trusted Host list after

submitting and verifying the addresses in the list.

Trusted Host warning prompt

3. Once enabled, only the IP addresses in the table will be allowed access to the NetGuardian.
4. In the **Trusted Host List**, enter the IP address of the machine(s) you would like to give access to the NetGuardian.
5. Click **Submit** to save the configuration settings.

⚠ ***Hot Tip!***

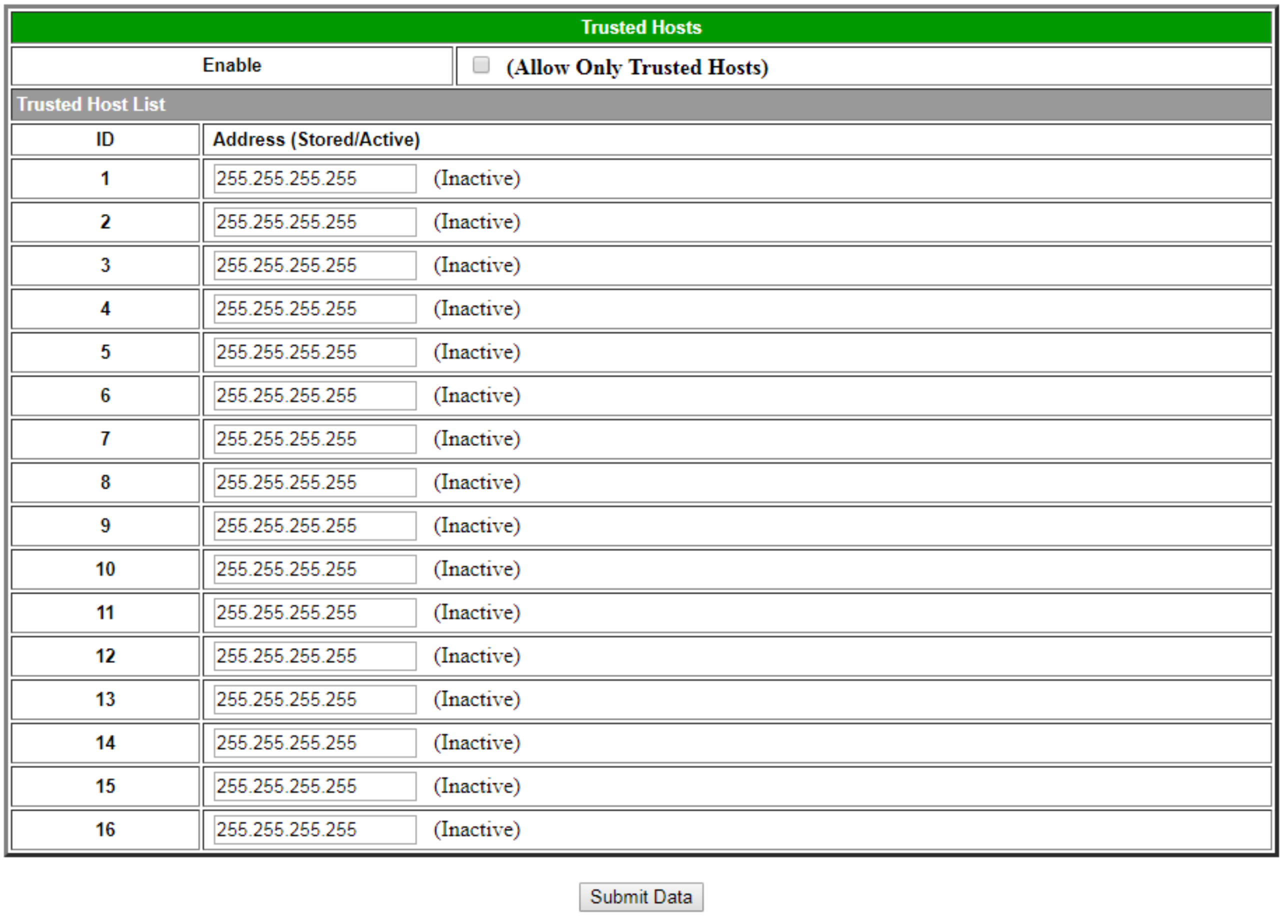
Entering a zero in any of the octet fields will declare that part of the octet to be a wildcard.

WARNING: Does not work with networks that assign IP addresses. Use the wildcard field to open an entire subnet.

Two Modes:
Firewall: Block specific addresses
Filter table: only allow specific addresses

⚠ ***Hot Tip!***

The Trusted Host List is primarily used for diagnostic purposes and should not be required unless needed to increase security.



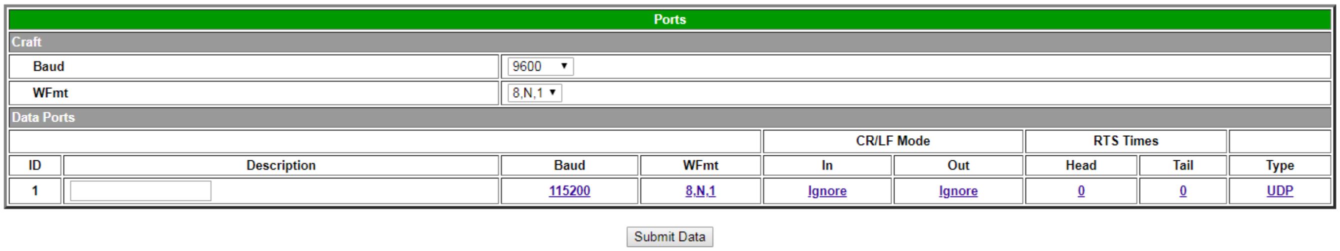
Trusted Hosts	
Enable	□ (Allow Only Trusted Hosts)
Trusted Host List	
ID	Address (Stored/Active)
1	255.255.255.255 (Inactive)
2	255.255.255.255 (Inactive)
3	255.255.255.255 (Inactive)
4	255.255.255.255 (Inactive)
5	255.255.255.255 (Inactive)
6	255.255.255.255 (Inactive)
7	255.255.255.255 (Inactive)
8	255.255.255.255 (Inactive)
9	255.255.255.255 (Inactive)
10	255.255.255.255 (Inactive)
11	255.255.255.255 (Inactive)
12	255.255.255.255 (Inactive)
13	255.255.255.255 (Inactive)
14	255.255.255.255 (Inactive)
15	255.255.255.255 (Inactive)
16	255.255.255.255 (Inactive)

Select Trusted Hosts from the Edit menu to configure your Trusted Host List.

2.4.4 Changing Craft Port Communication Settings

Use the following steps to change the craft port communication settings:

1. Click on the **Edit** menu > **Ports** screen to edit the **Craft** port section (see image below).
2. You can set the baud rate for the craft port to 300, 1200, 2400, 9600, 19200, 38400, 57600, 115200. (Default Baud is 9600)
3. Under the **Wfmt** (word format) field, select the appropriate data bits, parity, and stop bits setting to match your terminal emulation software or device connected to the NetGuardian craft port. (Default designation is 8,N,1)
4. Click **Submit Data** to save the craft port settings.



Ports

Craft

Baud	9600 ▼
WFmt	8,N,1 ▼

Data Ports

				CR/LF Mode		RTS Times		
ID	Description	Baud	WFmt	In	Out	Head	Tail	Type
1		115200	8,N,1	Ignore	Ignore	0	0	UDP

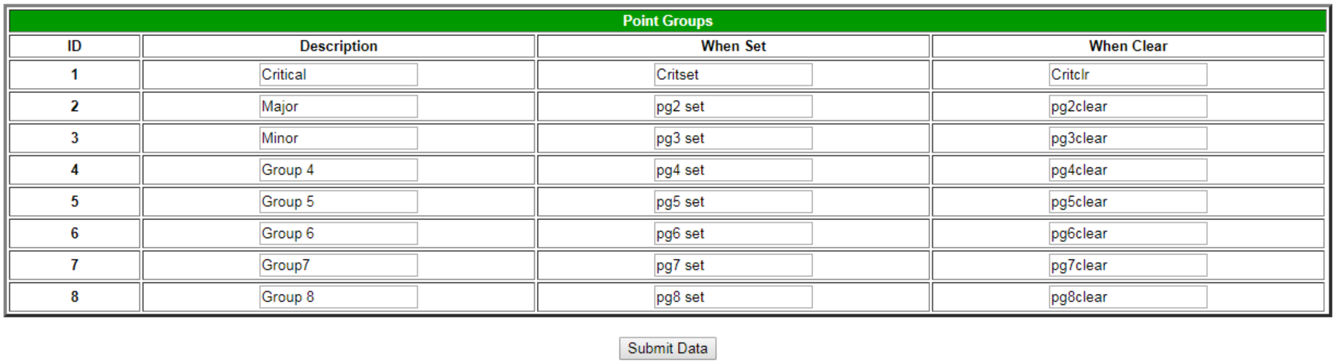
Configure the front panel craft port parameters from the Ports screen

2.5 Defining Point Groups

Each NetGuardian Alarm point can be assigned to one of eight groups, which are identified with a user-defined label. Once the point groups are defined, the Point Group IDs can be used to group base and system alarms, see section "Configuring Base Discrete Alarms."

Use the following steps to define alarm messages for alarm point groups:

1. To define the point groups, select **Point Groups** from the **Edit** menu.
2. Then enter the appropriate descriptions in the **Description**, **When Set** and **When Clear** fields for each point group.
3. Click **Submit Data** to save the point group settings.



Point Groups

ID	Description	When Set	When Clear
1	Critical	Critset	Critclr
2	Major	pg2 set	pg2clear
3	Minor	pg3 set	pg3clear
4	Group 4	pg4 set	pg4clear
5	Group 5	pg5 set	pg5clear
6	Group 6	pg6 set	pg6clear
7	Group7	pg7 set	pg7clear
8	Group 8	pg8 set	pg8clear

Define the Alarm and Clear messages for up to eight different point groups

2.6 Configuring Base Discrete Alarms

All of the NetGuardian's 16 discrete alarms are configured from the **Edit** menu **> Base Alarms** screen. Descriptions of the alarm point, polarity (normal or reversed), whether to use an SNMP Trap or not, and the primary and secondary pager used to report the alarm, and group assignments, are configured in this screen.

Use the following steps to configure base discrete alarm settings:

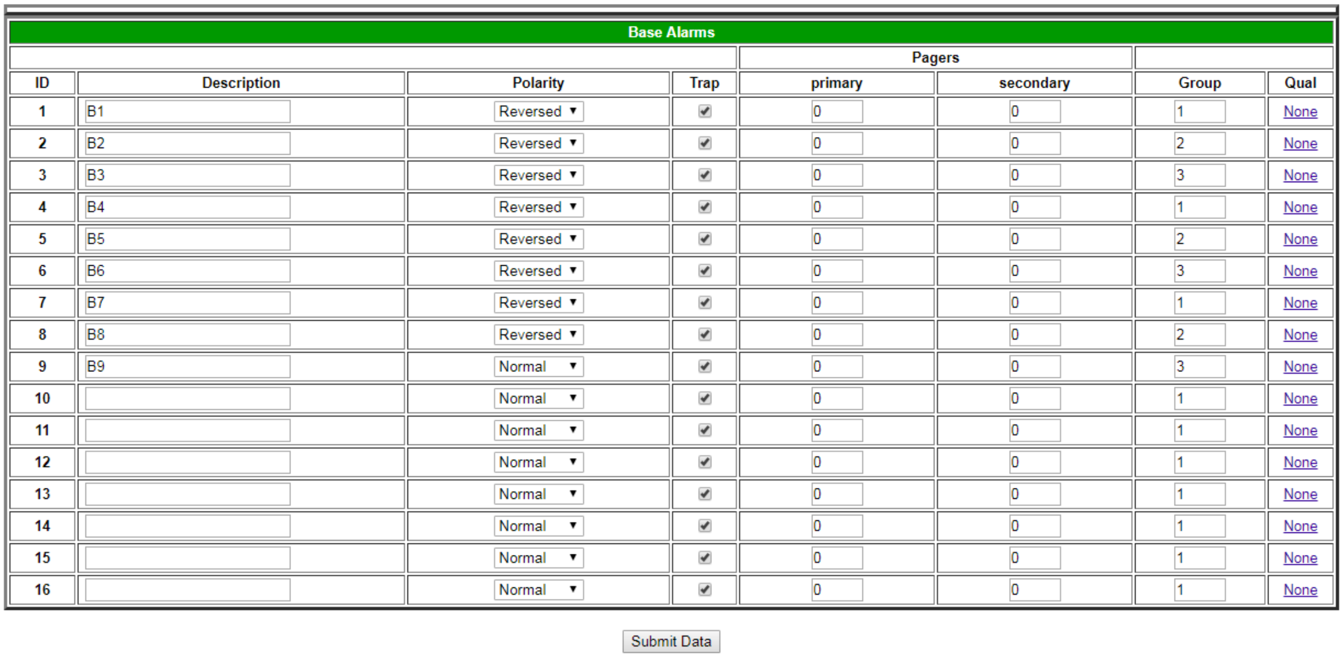
1. From the **Edit** menu select the **Base Alarms** link image below.
2. Enter a description for each discrete input alarm being used in the **Description** field.
3. Under the **Polarity** column, you can choose to reverse the polarity or leave it normal. If you select **Normal**, a contact closure is an alarm. If the **Reverse** option is selected, the alarm is clear when closed.

4. Select the **Trap** check box to send an SNMP trap for that alarm point in the event of an alarm condition. Leave the box blank if you do not wish the NetGuardian to send an SNMP trap.
5. Set the primary and secondary pagers with a pager ID from your defined pager list (see section: "Setting up Notification Methods" for more information).

   Note: The NetGuardian will notify both the primary and the secondary notification device when point status changes (both alarm and clear).
6. The **Group** column is where you ca select which alarm group each alarm point should belong to. You will be able to view alarms by their Group in the **Monitor** menu **> Alarm Summary** section.
7. Under the **Qual** column click the link to configure an event qualification time setting for the alarm point. The **Event Qual** screen will appear (refer to section: "Event Qualification Timers" for more information).
8. Click **Submit Data** to save base alarm configuration settings.

⚠ *Hot Tip!*

The pager device can be an ASCII terminal, T/Mon element manager, email, or multiple SNMP managers.

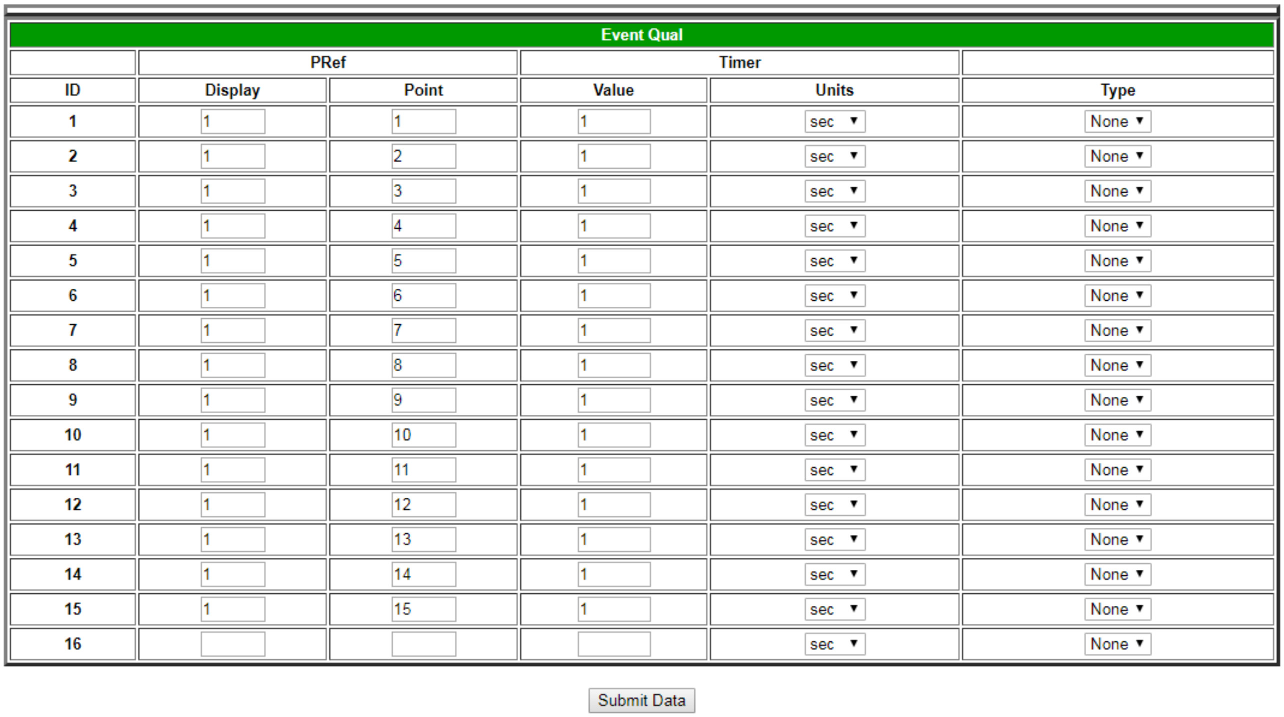


Base Alarms

				Pagers			
ID	Description	Polarity	Trap	primary	secondary	Group	Qual
1	B1	Reversed ▾	☑	0	0	1	None
2	B2	Reversed ▾	☑	0	0	2	None
3	B3	Reversed ▾	☑	0	0	3	None
4	B4	Reversed ▾	☑	0	0	1	None
5	B5	Reversed ▾	☑	0	0	2	None
6	B6	Reversed ▾	☑	0	0	3	None
7	B7	Reversed ▾	☑	0	0	1	None
8	B8	Reversed ▾	☑	0	0	2	None
9	B9	Normal ▾	☑	0	0	3	None
10		Normal ▾	☑	0	0	1	None
11		Normal ▾	☑	0	0	1	None
12		Normal ▾	☑	0	0	1	None
13		Normal ▾	☑	0	0	1	None
14		Normal ▾	☑	0	0	1	None
15		Normal ▾	☑	0	0	1	None
16		Normal ▾	☑	0	0	1	None

Configure the 16 discrete alarms from the Base Alarms screen

2.7 Event Qualification Timers



Event Qual					
	PRef		Timer		
ID	Display	Point	Value	Units	Type
1	1	1	1	sec	None
2	1	2	1	sec	None
3	1	3	1	sec	None
4	1	4	1	sec	None
5	1	5	1	sec	None
6	1	6	1	sec	None
7	1	7	1	sec	None
8	1	8	1	sec	None
9	1	9	1	sec	None
10	1	10	1	sec	None
11	1	11	1	sec	None
12	1	12	1	sec	None
13	1	13	1	sec	None
14	1	14	1	sec	None
15	1	15	1	sec	None
16				sec	None

Edit the Even Qualification Timer settings from the ***Edit > Even Qual*** *screen*

Use the following steps to configure your Event Qual timer settings:

1. From the **Edit** menu select from the **Event Qual** drop-down menu.
2. The standard NetGuardian units can have up to 128 Event Quals, which are grouped into sections of sixteen.
3. Enter the display and point number for the point you wish to qualify in the appropriate **ID** row.

   Note: the ID will correspond to Event Qualification. A list of displays and points can be found in the Reference section.
4. In the **Value** field enter the appropriate amount of time (1 - 127).
5. Under the **Units** column, click on the drop-down menu and select the appropriate unit (min, sec, hour).
6. Under the **Type** column click on the drop-down menu and select the appropriate event type (Alm = alarm, Pri = primary, Sec = secondary).

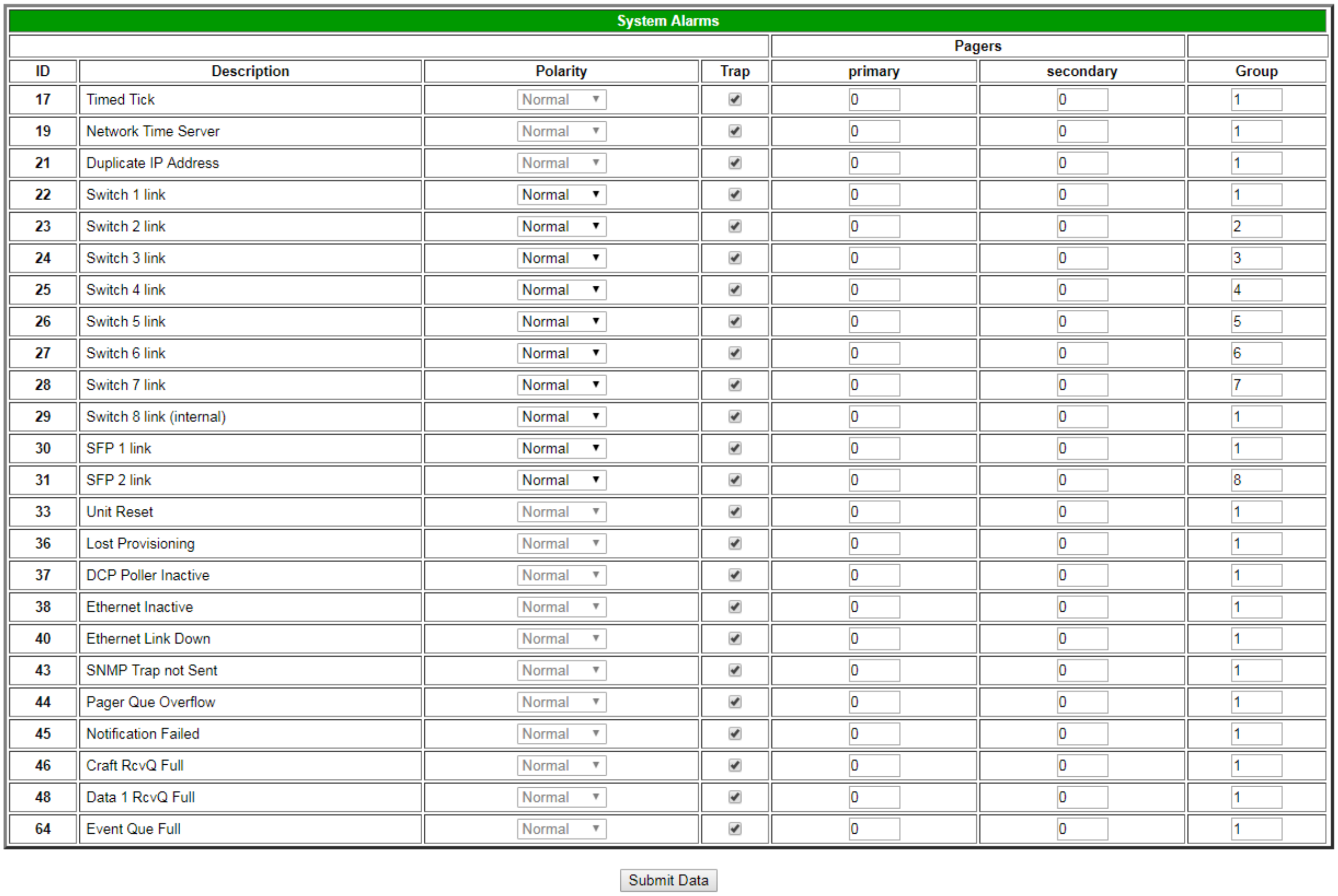
Hot Tip!

To delete the entry, set the **Type** to None.

When you are done making changes, scroll to the bottom of the page and click **Submit Data**.

CAUTION: Set conditions are qualified, clears are not.

2.8 Setting System Alarm Notifications



System Alarms

				Pagers		
ID	**Description**	**Polarity**	**Trap**	**primary**	**secondary**	**Group**
17	Timed Tick	Normal ▼	☑	0	0	1
19	Network Time Server	Normal ▼	☑	0	0	1
21	Duplicate IP Address	Normal ▼	☑	0	0	1
22	Switch 1 link	Normal ▼	☑	0	0	1
23	Switch 2 link	Normal ▼	☑	0	0	2
24	Switch 3 link	Normal ▼	☑	0	0	3
25	Switch 4 link	Normal ▼	☑	0	0	4
26	Switch 5 link	Normal ▼	☑	0	0	5
27	Switch 6 link	Normal ▼	☑	0	0	6
28	Switch 7 link	Normal ▼	☑	0	0	7
29	Switch 8 link (internal)	Normal ▼	☑	0	0	1
30	SFP 1 link	Normal ▼	☑	0	0	1
31	SFP 2 link	Normal ▼	☑	0	0	8
33	Unit Reset	Normal ▼	☑	0	0	1
36	Lost Provisioning	Normal ▼	☑	0	0	1
37	DCP Poller Inactive	Normal ▼	☑	0	0	1
38	Ethernet Inactive	Normal ▼	☑	0	0	1
40	Ethernet Link Down	Normal ▼	☑	0	0	1
43	SNMP Trap not Sent	Normal ▼	☑	0	0	1
44	Pager Que Overflow	Normal ▼	☑	0	0	1
45	Notification Failed	Normal ▼	☑	0	0	1
46	Craft RcvQ Full	Normal ▼	☑	0	0	1
48	Data 1 RcvQ Full	Normal ▼	☑	0	0	1
64	Event Que Full	Normal ▼	☑	0	0	1

SNMP Traps and primary or secondary pager devices can be selected for each system alarm

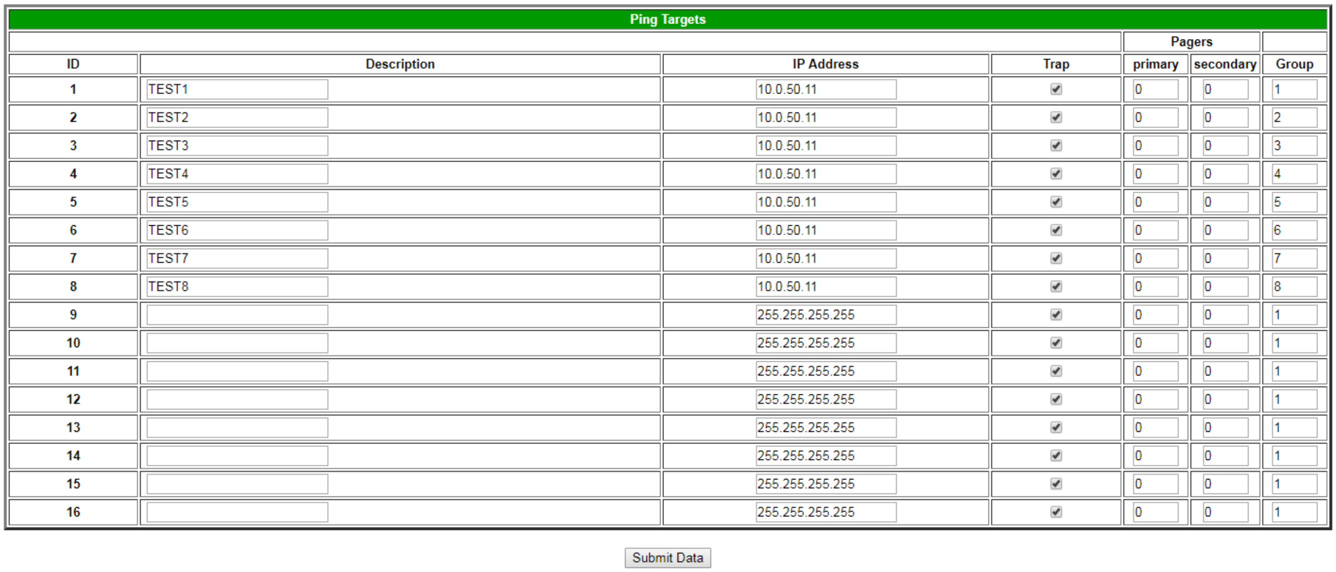
The **System Alarms** screen allows you to individually set the notification method for each system alarm. See the Reference Section for system alarm point descriptions.

Use the following steps to configure your system alarm notification settings:

1. From the **Edit** menu select the **System Alarms** link (see above).
2. Check the **Trap** box to send an SNMP trap for that alarm point. Selecting the box will set that point to send a SNMP trap; leaving the box blank will set that point to not send an SNMP trap.
3. Set the primary and secondary pagers with a pager ID from your defined pager list.

   Note: The NetGuardian will notify both the primary and the secondary notification device when point status changes (both alarm and clear).
4. Under the **Group** column enter the appropriate point group ID.
5. Click **Submit Data** to save the configuration settings.

2.9 Configuring Ping Targets



Ping Targets

				Pagers		
ID	Description	IP Address	Trap	primary	secondary	Group
1	TEST1	10.0.50.11	☑	0	0	1
2	TEST2	10.0.50.11	☑	0	0	2
3	TEST3	10.0.50.11	☑	0	0	3
4	TEST4	10.0.50.11	☑	0	0	4
5	TEST5	10.0.50.11	☑	0	0	5
6	TEST6	10.0.50.11	☑	0	0	6
7	TEST7	10.0.50.11	☑	0	0	7
8	TEST8	10.0.50.11	☑	0	0	8
9		255.255.255.255	☑	0	0	1
10		255.255.255.255	☑	0	0	1
11		255.255.255.255	☑	0	0	1
12		255.255.255.255	☑	0	0	1
13		255.255.255.255	☑	0	0	1
14		255.255.255.255	☑	0	0	1
15		255.255.255.255	☑	0	0	1
16		255.255.255.255	☑	0	0	1

Configure the ping target parameters from the Ping Targets screen

Each of the 16 ping targets can be provisioned with a description, an IP address, a choice whether to send SNMP Traps, and the primary and secondary pager devices being used.

Use the following steps to configure the ping targets:

1. From the **Edit** menu select **Ping Targets** (see image above).
2. In the **Description** field enter a description of the device to be pinged.
3. In the **IP Address** field enter the IP address of the device to be pinged.
4. Under the **Trap** column check the box to designate that an SNMP trap will be sent when an alarm condition exists. Leaving the box blank designates that an SNMP trap will not be sent when an alarm condition exists.
5. Set the primary and secondary pagers with a pager ID from your defined pager list.

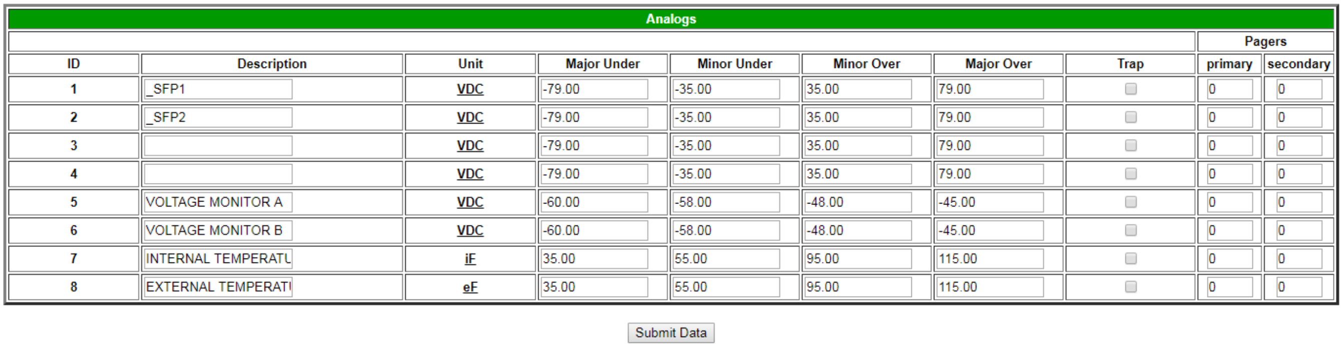
    Note: The NetGuardian 216F will notify both the primary and the secondary notification device when point status changes (both alarm and clear).
6. Under the **Group** column enter the appropriate point group ID.
7. Click **Submit Data** to save the configuration settings.

2.10 Analog Parameters

Each of the NetGuardian 216F's analog channels must be individually configured to monitor data. The ADCs (analog to digital converters) support a range of –70 to 94 VDC. There are four alarm trip points (thresholds) in ascending order: major under, minor under, minor over, and major over. You can choose the values for each of the thresholds on all channels. As with the other alarms, you can designate whether or not to send an SNMP trap when a threshold is crossed. The primary/secondary pager used to report the alarm is also set here. The thresholds must be set from Under to Over in either ascending or descending potential (or current) order. Thus the settings of –10, –5, 5 and 10 corresponding respectively to major under, minor under, minor over, and major over is valid.

The analog alarms are set to measure voltage by default and the thresholds are reported as "native units." For example, you may set Channel 3 to measure outside temperature if you were using a sensor with a measurable temperature range between –4° to 167° Fahrenheit (–20° to 75° Celsius). The voltage for that channel varies between 1 and 5 VDC for that sensor, which is to be reported as ° Fahrenheit (native units) where 1 volt represents –4° Fahrenheit and 5 volts represents 167° Fahrenheit.

To change any one analog alarm to measure current instead, a dipswitch setting must be changed. The jumper inserts a 250 ohm shunt resistor across the input to convert the sensors current output to volts. Use Ohms law to find the voltage drop across the 250 ohm shunt resistor (multiply the current by the resistance 250 ohms). Please refer to the operation manual for your sensor to determine any other conversion factors. This will allow you to correctly set the thresholds for over and under conditions.



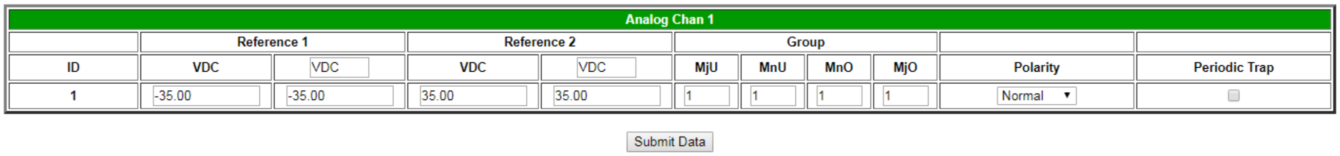
Analogs

								Pagers	
ID	Description	Unit	Major Under	Minor Under	Minor Over	Major Over	Trap	primary	secondary
1	_SFP1	VDC	-79.00	-35.00	35.00	79.00	☐	0	0
2	_SFP2	VDC	-79.00	-35.00	35.00	79.00	☐	0	0
3		VDC	-79.00	-35.00	35.00	79.00	☐	0	0
4		VDC	-79.00	-35.00	35.00	79.00	☐	0	0
5	VOLTAGE MONITOR A	VDC	-60.00	-58.00	-48.00	-45.00	☐	0	0
6	VOLTAGE MONITOR B	VDC	-60.00	-58.00	-48.00	-45.00	☐	0	0
7	INTERNAL TEMPERATU	iF	35.00	55.00	95.00	115.00	☐	0	0
8	EXTERNAL TEMPERATI	eF	35.00	55.00	95.00	115.00	☐	0	0

The Analog Parameters can be viewed and changed from the Analogs screen

Note: _SFP1 and _SFP2 may be used for SFP 1 and SFP 2 respectively, to allow the SFP connection values to appear in the Analog section of the Monitor menu. (See section: "SFP 1&2 Analog Readings" for more information on how to configure this.)

1. From the **Edit** menu click on the **Analogs** link.
2. In the **Description** field enter a description for each analog channel being utilized.
3. Under the Unit column, click on the abbreviated units link (e.g VDC, RH, F, etc.) to convert the reference units and the native units for that analog channel.
4. Set Reference 1 (VDC) to the minimum output (in volts DC) of the analog device being configured.
5. In the box next to VDC (the space may already contain the abbreviation VDC), enter an abbreviation for the native units (e.g. RH for relative humidity, F for ° Fahrenheit, etc.).
6. In the box below the abbreviated native unit setting enter the native unit amount that corresponds to the minimum output entered in the previous step.
7. Set Reference 2 (VDC) to the maximum output (in volts DC) of the analog device being configured.
8. In the box next to VDC enter an abbreviation for the native units (e.g. RH for relative humidity, F for ° Fahrenheit, etc.).
9. In the box below the abbreviated native unit setting enter the native uni
10. t amount that corresponds to the maximum output entered in the previous step.
11. Enter the Point Group ID designated for each alarm level (MjU = Major Under, MnU = Minor Under, MjO = Major Over, MnO = Minor Under).
12. Follow these steps for each analog channel being configured.
13. Click the **Submit Data** button to save the configuration settings.



Analog Chan 1

	Reference 1		Reference 2		Group					
ID	VDC	VDC	VDC	VDC	MjU	MnU	MnO	MjO	Polarity	Periodic Trap
1	-35.00	-35.00	35.00	35.00	1	1	1	1	Normal ▼	☐

Reference 1 and Reference 2 correspond to the minimum and maximum output values of your analog device

2.10.1 Integrated Temperature and Battery Sensor

The integrated temperature and battery sensor allows the user to monitor surrounding temperature as well as the unit's current draw. If you are using the temperature or battery sensor, you must dedicate an analog port to each one (see user manual for connection information).

CAUTION: Abort ambient room temperature cooler than the NetGuardian unit temperature.

Temperature Sensor
In the **Description** field enter a description in the analog channel you are using for the integrated temperature sensor and set it to 7.

Under the **Unit** column, click on the abbreviated units link (e.g VDC, RH, F, etc.) to convert the reference units and the native units for that analog channel.
In **Reference 1** enter **iF** (internal Fahrenheit) in the box next to **VDC** (the space may already contain the abbreviation VDC). This enables the NetGuardian's pre-configured temperature settings. Repeat this step for **Reference 2**.
Set your desired thresholds. (See section: "Analog Parameters" for instructions.)
If you have connected the external temperature sensor, follow the above procedure to configure, except set it to channel 8 and enter eF (external Fahrenheit) in the **Reference** menu.

Current Sensor
In the **Description** field enter a description in the analog channel you are using for the integrated current sensor (5 for power feed A or 6 for power feed B).
Set your desired thresholds. (See section: "Analog Parameters" for instructions.) Be sure to set your thresholds in reference to your NetGuardian's power input (e.g. –24 VDC, –48 VDC, or wide range).

2.10.2 Analog Polarity Override

iF : internal temperature sensor in fahrenheit or iC for celsius
oV+ : override polarity VDC to positive
oV- : override polarity VDC to negative

If you have a positive powered NetGuardian, you may want to use this feature if you are using the internal battery sensor. The Web browser interface will override **oV+** and **oV-** tags and show VDC. So you won't have to view an uncommon looking tag while in monitor mode.

Analog Accuracy:
+/- 1% of analog range.

2.10.3 Analog Step Sizes

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

Analog step sizes

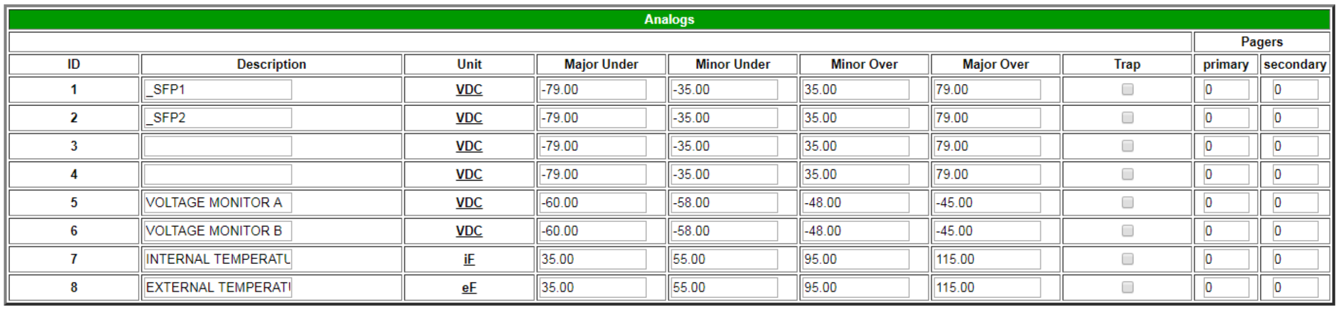
2.10.4 SFP 1&2 Analog Readings

The **Edit** menu **> SFP 1&2** screen is where you can configure the parameters of each endpoint of your fiber line to allow you to monitor the length of one SFP connection to another and any break point across that length. You may run OTDR to monitor up to two separate fiber lines.

To associate an alarm with your SFP connections, _SFP1 and _SFP2 may be used for SFP 1 and SFP 2 respectively, to allow the SFP connection values to appear in the Analog section of the Monitor menu.

To configure the SFP analog complete the following steps:

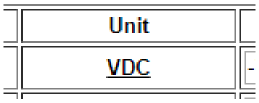
1. Enter "**_SFP1**" or "**_SFP2**" in the **Description** column, depending on the SFP port being configured. (See image below) Other text may follow "**_SFP1**" or "**_SFP2**", but the description must begin with one of these.
2. Save your change by clicking **Submit Data**.



Analogs									
								Pagers	
ID	Description	Unit	Major Under	Minor Under	Minor Over	Major Over	Trap	primary	secondary
1	_SFP1	VDC	-79.00	-35.00	35.00	79.00	☐	0	0
2	_SFP2	VDC	-79.00	-35.00	35.00	79.00	☐	0	0
3		VDC	-79.00	-35.00	35.00	79.00	☐	0	0
4		VDC	-79.00	-35.00	35.00	79.00	☐	0	0
5	VOLTAGE MONITOR A	VDC	-60.00	-58.00	-48.00	-45.00	☐	0	0
6	VOLTAGE MONITOR B	VDC	-60.00	-58.00	-48.00	-45.00	☐	0	0
7	INTERNAL TEMPERATU	iF	35.00	55.00	95.00	115.00	☐	0	0
8	EXTERNAL TEMPERATI	eF	35.00	55.00	95.00	115.00	☐	0	0

*Enter **_SFP1** or **_SFP2** in the **Description** column.*

3. The default unit of measure is VDC. For your SFP alarm you will be measuring distance, (the length of the fiber line), so you will need to adjust this by clicking on the **VDC** link in the **Unit** column.



Unit
VDC

Configure the unit by clicking on the VDC link.

4. In the **Reference** column for your _SFP analog, VDC = KM (kilometers). VDC cannot be changed, it must just be known that it represents kilometers. To configure a different unit of measure, you will enter the conversion of that unit of measure relative to kilometers to scale.
5. In the example shown below, the unit of measurement to be displayed will be M (meters). It will be scaled as follows:

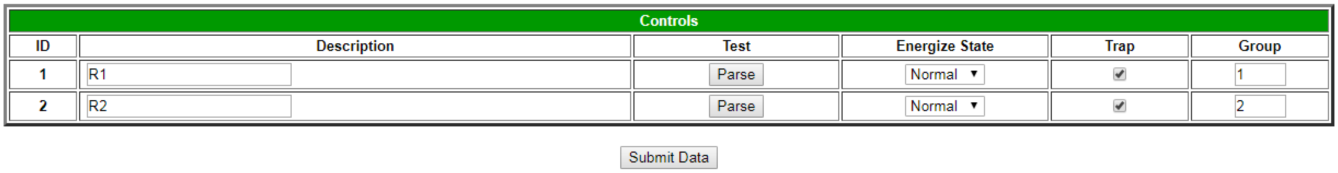
(For this example remember: VDC = KM)

For **Reference 1**:
0 KM = 0 M

For **Reference 2**:
1 KM = 1000 M

How to scale from kilometers to another unit of measure.

2.11 Configuring the Control Relays



Controls

ID	Description	Test	Energize State	Trap	Group
1	R1	Parse	Normal ▼	☑	1
2	R2	Parse	Normal ▼	☑	2

*Configure controls in the **Edit** menu > **Controls** screen*

The Relays of the NetGuardian 216F can be identified and configured using the **Edit** menu > **Controls** screen. A description can be entered for each of the relays. You can also designate whether or not to send SNMP Traps when a relay is activated. Relays are normally open (N/O) by default. A circuit board jumper can be changed for each control to make it normally closed (N/C).

1. From the **Edit** menu, select the **Controls** link (see image above).
2. In the **Description** field enter a description for each control/relay being used.
3. Set the **Energize State** to either **Normal** or **Inverted**. Selecting Normal sets the relay's normal electrical state to **De-energized.** Selecting **Inverted** sets the relay's normal electrical state to **Energized**.
4. Check the **Trap** box to send an SNMP trap for that alarm point. Selecting the box will set that point to send an SNMP trap; leaving the box blank will set that point to not send an SNMP trap.
5. Under the **Group** column enter the appropriate point group ID (see section: "Defining Point Groups)."
6. Click **Submit Data** to save the configuration settings.

Hot Tip!

The Energize State is different than the normal state of the physical contact closure position of each relay, which is determined by circuit board jumpers. This gives you the added benefit of being able to monitor the wire. In the event of a power failure, the relay would de-energize back to it's normal physical contact closure set by the circuit board jumper for that relay. Check your jumper settings and relay connections before setting to Normal or Inverted. Refer to the NetGuardian hardware manual for relay connection options.

2.11.1 Activating Relays from an Alarm Point's Change of Status

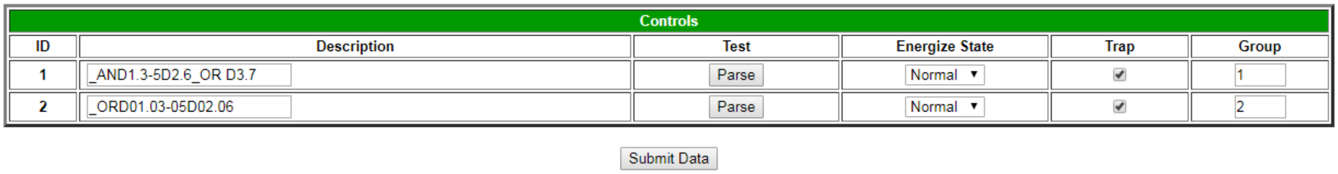
The NetGuardian allows the user to echo an alarm point state to activate a relay. Any of the NetGuardian's discrete alarms, system alarms, ping alarms, or analog alarms may be echoed to activate a relay in the event that alarm is triggered. However, a relay set to echo an alarm point cannot be manually activated. To allow the relay to be manually activated while still maintaining its echoed status, the relay point must be set to **Derived**. See section: "Derived Control Relays and Virtual Alarming" for information regarding echoing and ORing alarm points to relays.

2.11.2 Derived Control Relays and Virtual Alarming

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.
Note: Spaces included here are for readability purposes only.

Hot Tip!

- Precedence of the operations are always left to right.
- All number references can either be one or two digits.



Controls					
ID	Description	Test	Energize State	Trap	Group
1	_AND1.3-5D2.6_OR D3.7	Parse	Normal ▼	☑	1
2	_ORD01.03-05D02.06	Parse	Normal ▼	☑	2

Submit Data

Derived control relays

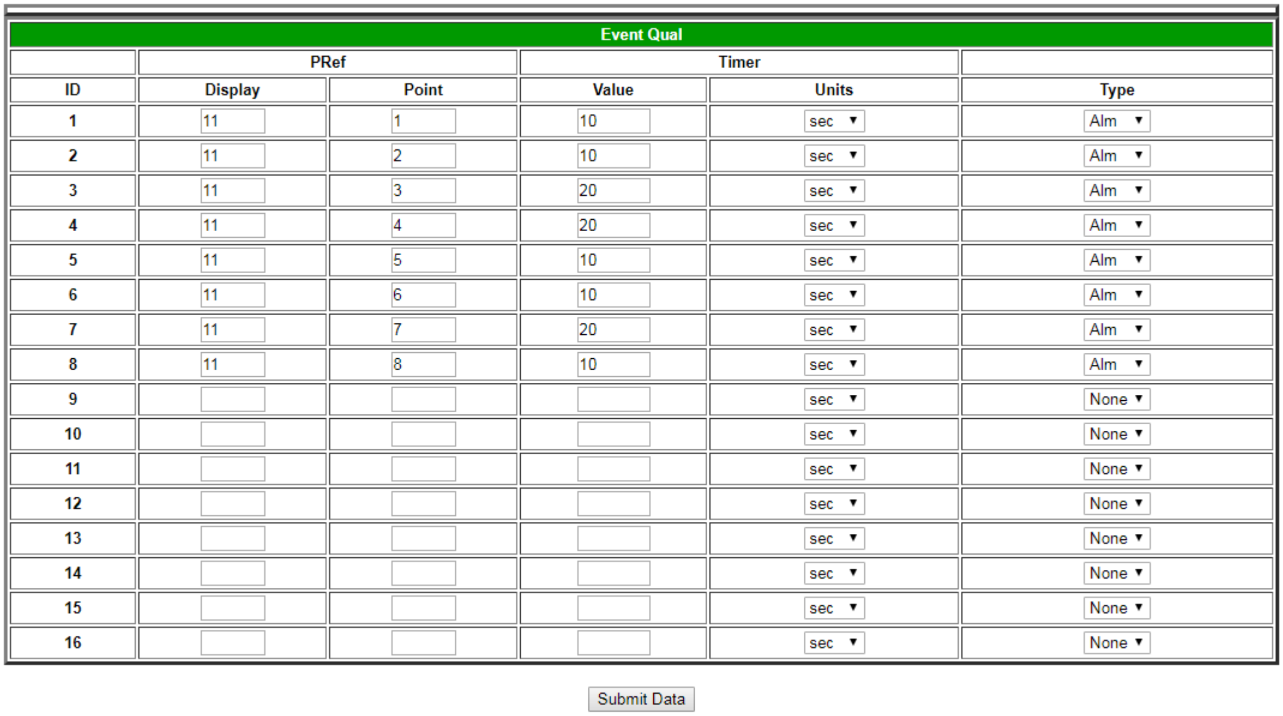
_AN D 1.3-5 D2.6 _OR D3.7 is logically equivalent to ((1.3 && 1.4 && 1.5 && 2.6) || 3.7)
_OR D01.03-05 D02.06 _AN D02.07 D03.10.-12 is logically equivalent to ((1.3 || 1.4 || 1.5 || 2.6&& (2.7 && 3.10 && 3.12))

2.11.3 Relay Operating

2.11.3.1 Normal Mode

Relay energized state is similar to alarm point polarity. A normal control is latched when the relay state is **opr**, and open when the relay state is **rls**. Conversely, an inverted control is latched when the relay state is rls, and open when the relay state is **opr**.

2.11.4 Override Default Relay Momentary Time Using Event Qualification



Event Qual					
	PRef		Timer		
ID	Display	Point	Value	Units	Type
1	11	1	10	sec ▼	Alm ▼
2	11	2	10	sec ▼	Alm ▼
3	11	3	20	sec ▼	Alm ▼
4	11	4	20	sec ▼	Alm ▼
5	11	5	10	sec ▼	Alm ▼
6	11	6	10	sec ▼	Alm ▼
7	11	7	20	sec ▼	Alm ▼
8	11	8	10	sec ▼	Alm ▼
9				sec ▼	None ▼
10				sec ▼	None ▼
11				sec ▼	None ▼
12				sec ▼	None ▼
13				sec ▼	None ▼
14				sec ▼	None ▼
15				sec ▼	None ▼
16				sec ▼	None ▼

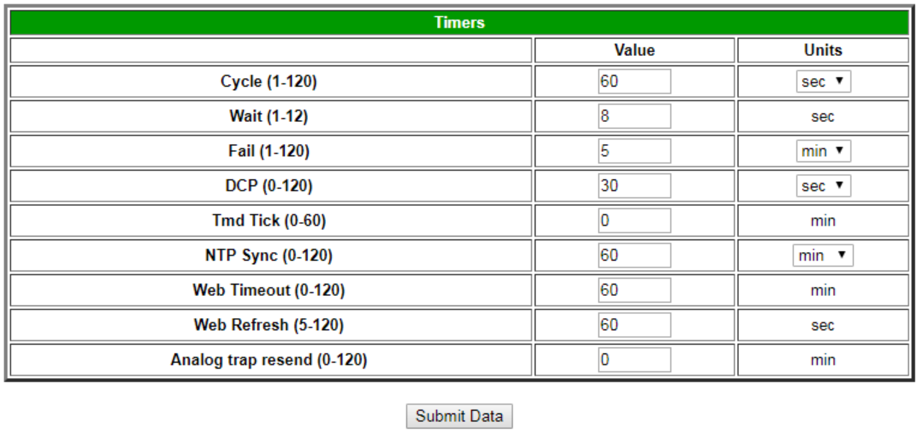
Submit Data

Using Event Qualification to override default relay momentary time

Use the following steps to override default relay momentary time, using the NetGuardian's Event Qualification feature:

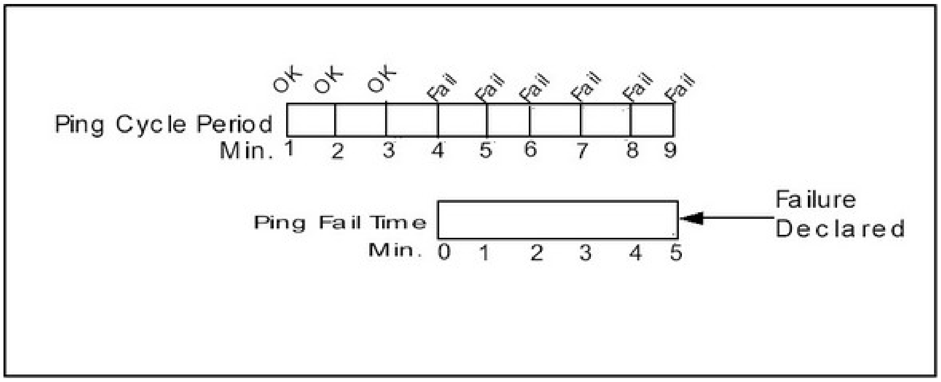
1. From the **Edit** menu click on the **Event Qual** drop-down menu and select the appropriate group.
2. In the **Display** text box, type **11**.
3. In the **Point** text box, type the number of the relay you would like to change.
4. In the **Value** box, type the amount of time. You may not select more than 127 units.
5. In the **Units** box, select the appropriate units (seconds, minutes, or hours).
6. In the **Type** box, select **Alm**.
7. Click **Submit Data** to save the changes.

2.12 Setting System Timers



Timers		
	Value	Units
Cycle (1-120)	60	sec ▼
Wait (1-12)	8	sec
Fail (1-120)	5	min ▼
DCP (0-120)	30	sec ▼
Tmd Tick (0-60)	0	min
NTP Sync (0-120)	60	min ▼
Web Timeout (0-120)	60	min
Web Refresh (5-120)	60	sec
Analog trap resend (0-120)	0	min

When a target fails to respond to a ping within the fail time period, a fault is declared.



Default timer settings

The NetGuardian's System Timers allow you to control the rate of your pinging activity, time of speaker sounding, inactivity time for the data port, and discrete alarm detect time. Ping timer settings allow you to balance network traffic against alarm response times. Although you can change the values from their default settings, it is recommended that you use either the default settings or plan your settings so that there is no conflict among the timers. Specifically, the FAIL time should be set to several times the CYCLE time to allow multiple PINGs before a FAIL is declared. Likewise, the CYCLE time should be set to several times the wait time.

Hot Tip!

The smaller the CYCLE number, the sooner you will find out about failures; however, you will increase traffic on your LAN.

1. From the **Edit** menu select **System Timers** (see image above).
2. Set the **Cycle** time. This determines how often the NetGuardian will go through its list of ping targets and attempts to reach them with an ICMP ping. Set the value between 0 and 120 and set the units to either seconds or minutes. Default is 60 seconds.
3. Set the **Wait** time. The NetGuardian waits after sending a ping request before it determines that the target is unreachable. Set the value between 0 and 12 and set the units to either seconds or minutes. Default is 8 seconds.
4. Set the **Fail** time. This determines the period of time over which, if a unit has not responded, it is considered failed. Set the value between 0 and 120 and set the units to either seconds or minutes. Default is 5 minutes.
5. Set the **DCP** time. Set between 0 and120 (sec or min). This determines the period of time over which, if the NetGuardian does not receive a DCP poll, to trigger an alarm. This option is only available if the primary reporting protocol of the active NetGuardian device is DCP.

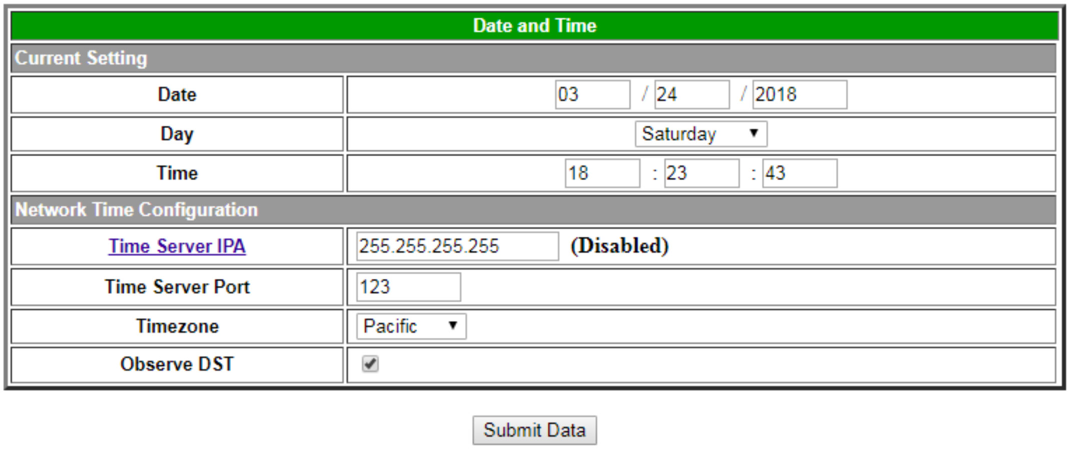
6. Set the **Timed Tick** between 0 and 60 minutes. This is a "keep alive or heartbeat" function that can be used by Masters who don't perform integrity checks. For example, if you entered 30, the NetGuardian would notify you every 30 minutes. See section: "Setting Up Notification Methods" for paging information.

Hot Tip!

The timer settings are accurate to ± one tick. This means that if a timer is set to one minute, it may actually respond anywhere from zero to two minutes. If your target time is one minute, then set the timer to 60 seconds so that it will respond anywhere from 59 to 61 seconds.

7. Set the **Web Timeout** time between 5 and 120 minutes. This determines the period of time a Web edit page may be active without any activity. A logon is required if a Web edit timeout occurs. The default Web edit time is 10 minutes.
   Note: The time units are preset to minutes by default and cannot be changed.
8. Set the **Web Refresh** time between 5 and 120 seconds. This timer enables the user to specify how long the NetGuardian should wait before auto-refreshing a Monitor page to the Web browser. The default Web monitor refresh time is 60 seconds.
   Note: The time units are preset to seconds by default and cannot be changed.
9. Set the Analog Trap Resend timer between 1 and 120 minutes. If you've enabled periodic analog traps (when configuring your analogs), then this timer will tell the NetGuardian how often to send periodic analog traps. Setting the timer to 0 effectively disables this function.

2.13 Setting the System Date and Time



Date and Time	
Current Setting	
Date	03 / 24 / 2018
Day	Saturday ▼
Time	18 : 23 : 43
Network Time Configuration	
Time Server IPA	255.255.255.255 **(Disabled)**
Time Server Port	123
Timezone	Pacific ▼
Observe DST	☑

The current date and time can be entered from the Date and Time screen or from an SNMP manager.

The date is entered in the mm/dd/yyyy format and the time is entered in the hh:mm:ss format.

Hot Tip!

The date and time can also be set from an SNMP manager.

Use the following steps to manually set the system's time and date:
1. From the **Edit** menu, select **Date and Time** (see image above).
2. Enter the appropriate date, the day of the week, and time.
3. Click **Submit Data** to save the data and time settings.

Note: The date and time will need resetting following a power failure or reboot unless your NetGuardian is equipped with the real-time clock option or network time is enabled (see Section 2.15.1 for instructions on setting the network time configuration).

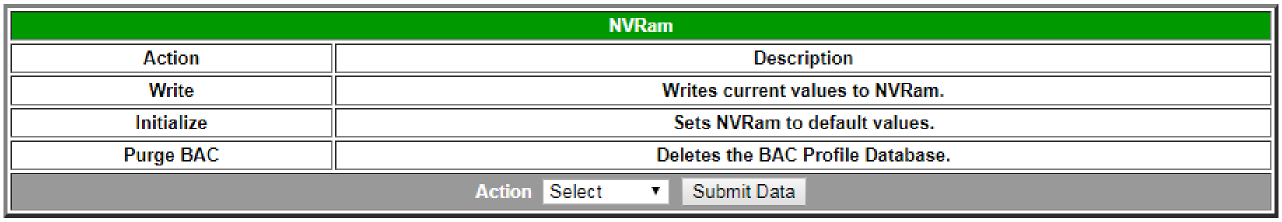
2.14 Saving Changes or Resetting Factory Defaults

Your NetGuardian 216F comes equipped with Non Volatile RAM (NVRAM), which enables the retention of data in the event of power loss. This section allows you to write and initialize the NVRAM.

Note: Some changes require a reboot of the NetGuardian to take effect (see section: "Rebooting the NetGuardian)."

1. From the **Edit** menu select **NVRAM** (see image below).
2. Select **Write** from drop down menu to cause the current data in RAM to be written to NVRAM and then verified.
3. Select **Initialize** to reload factory defaults into NVRAM.

DO NOT SELECT THIS OPTION UNLESS YOU WANT TO RE-ENTER ALL OF YOUR CONFIGURATION INFORMATION AGAIN.



NVRam

Action	Description
Write	Writes current values to NVRam.
Initialize	Sets NVRam to default values.
Purge BAC	Deletes the BAC Profile Database.

NVRAM enables the NetGuardian to retain data even through a power loss

2.15 Rebooting the NetGuardian

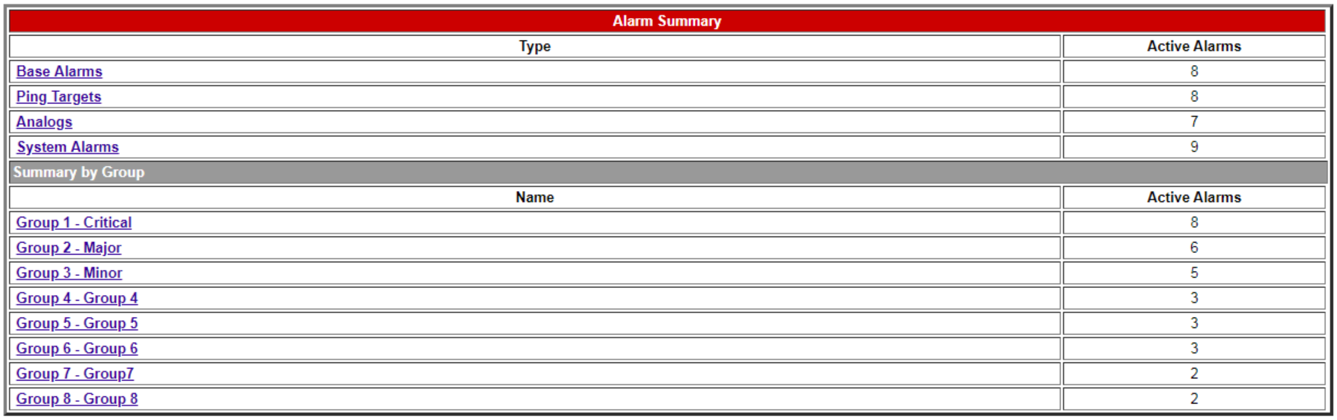
Click on the **Reboot** link from the **Edit** menu to reboot the NetGuardian after writing all changes to NVRAM. Any changes to port settings require a reboot to take effect. The window footer will display the text **Reboot Needed** if a reboot is necessary to initiate changes.

3 Web Server Monitoring

The Web browser allows you to do full-system monitoring for your NetGuardian, which includes all alarms, ping information, relays, analogs and system status. To connect to the NetGuardian from your Web browser, you must know it's IP address or domain name if it has been registered with your internal DNS. Enter it in the address bar of your Web browser (it may be helpful to bookmark the logon page to simplify access). After connecting to the NetGuardian's IP address, enter your password and click **Submit** (factory default password is dpstelecom).

Note: If the **Edit** menu does not appear in the left frame after logging on, it means that another station has already logged on as the primary user.

3.1 Alarm Summary Window



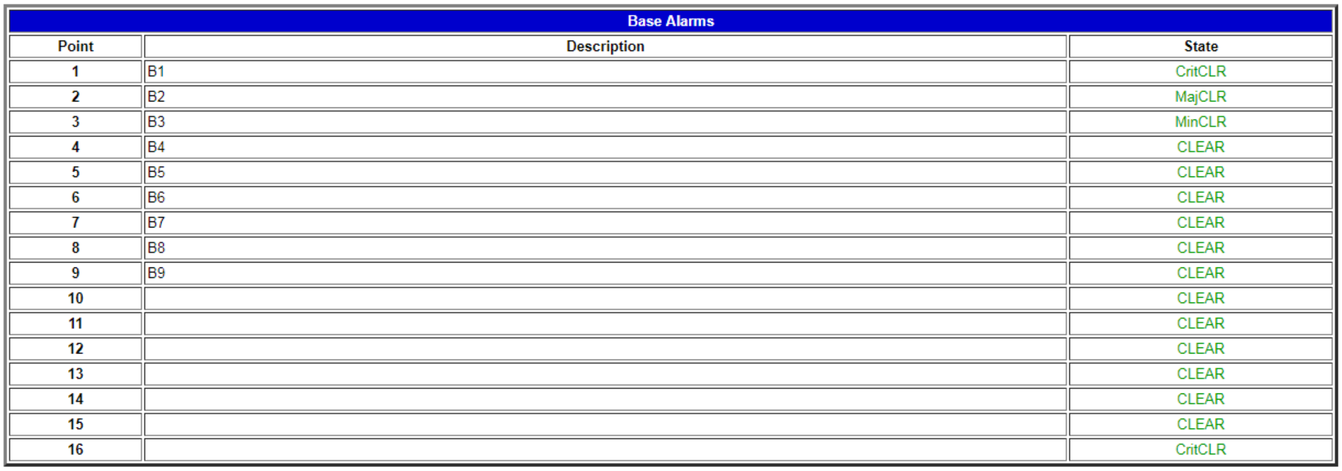
Alarm Summary	
Type	Active Alarms
Base Alarms	8
Ping Targets	8
Analogs	7
System Alarms	9
Summary by Group	
Name	Active Alarms
Group 1 - Critical	8
Group 2 - Major	6
Group 3 - Minor	5
Group 4 - Group 4	3
Group 5 - Group 5	3
Group 6 - Group 6	3
Group 7 - Group7	2
Group 8 - Group 8	2

The Alarm Summary display can be accessed by selecting either the Monitor link

Clicking on the **Monitor** or **Summary** buttons shows the **Alarm Summary** display. The **Summary** screen gives you a quick indication of any alarms that have been triggered in the NetGuardian's base alarms, ping targets, analogs, system alarms, and more.

You can view group specific alarm summaries in this section, at a quick glance of the active alarms in each user defined group.

3.2 Monitoring Base Alarms

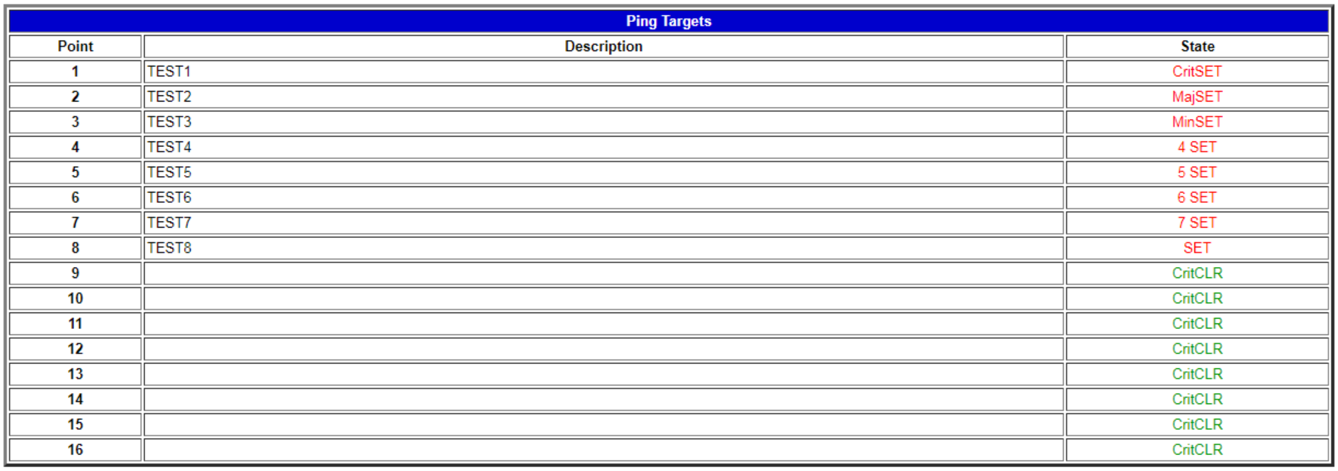


Base Alarms		
Point	Description	State
1	B1	CritCLR
2	B2	MajCLR
3	B3	MinCLR
4	B4	CLEAR
5	B5	CLEAR
6	B6	CLEAR
7	B7	CLEAR
8	B8	CLEAR
9	B9	CLEAR
10		CLEAR
11		CLEAR
12		CLEAR
13		CLEAR
14		CLEAR
15		CLEAR
16		CritCLR

View the status of the Base Alarms from the Monitor > Base Alarms screen

This selection provides the status of the system's base alarms by indicating if an alarm has been triggered. Under the **State** column, the description will appear in red if an alarm has been activated. The state will be displayed in green when the alarm condition is not present. The message that appears under the **State** column, when the alarm is clear or in alarm state, is configurable in the **Edit** menu > **Point Groups**.

3.3 Monitoring Ping Targets



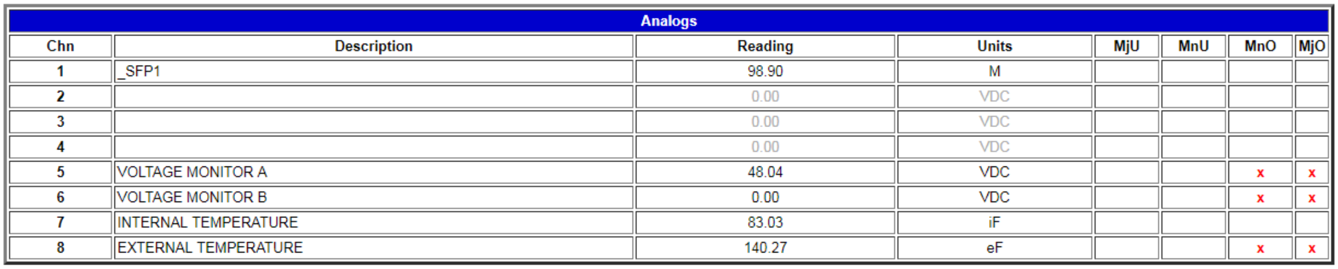
Ping Targets

Point	Description	State
1	TEST1	CritSET
2	TEST2	MajSET
3	TEST3	MinSET
4	TEST4	4 SET
5	TEST5	5 SET
6	TEST6	6 SET
7	TEST7	7 SET
8	TEST8	SET
9		CritCLR
10		CritCLR
11		CritCLR
12		CritCLR
13		CritCLR
14		CritCLR
15		CritCLR
16		CritCLR

View the status of the Ping Targets from the Monitor > Ping Targets screen

This selection provides the status of the system's ping targets by indicating if an alarm has been triggered. Under the **State** column, the description will appear in red if an alarm has been activated. The state will be displayed in green when the alarm condition is not present.

3.4 Monitoring Analogs



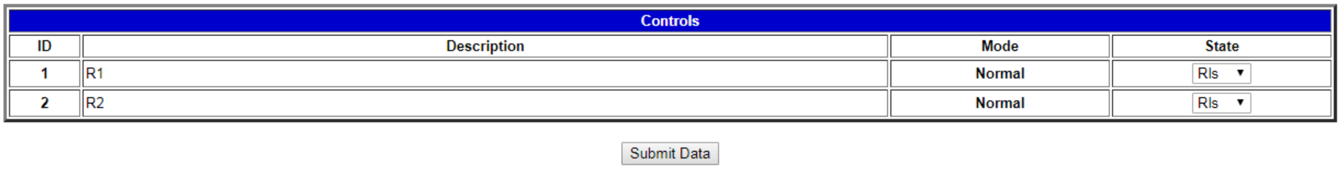
Analogs

Chn	Description	Reading	Units	MjU	MnU	MnO	MjO
1	_SFP1	98.90	M				
2		0.00	VDC				
3		0.00	VDC				
4		0.00	VDC				
5	VOLTAGE MONITOR A	48.04	VDC			x	x
6	VOLTAGE MONITOR B	0.00	VDC			x	x
7	INTERNAL TEMPERATURE	83.03	iF				
8	EXTERNAL TEMPERATURE	140.27	eF			x	x

View the status of the Analogs from the Monitor > Analogs screen

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

3.5 Operating Controls



Controls

ID	Description	Mode	State
1	R1	Normal	Rls
2	R2	Normal	Rls

Issue controls from the Monitor > Controls screen

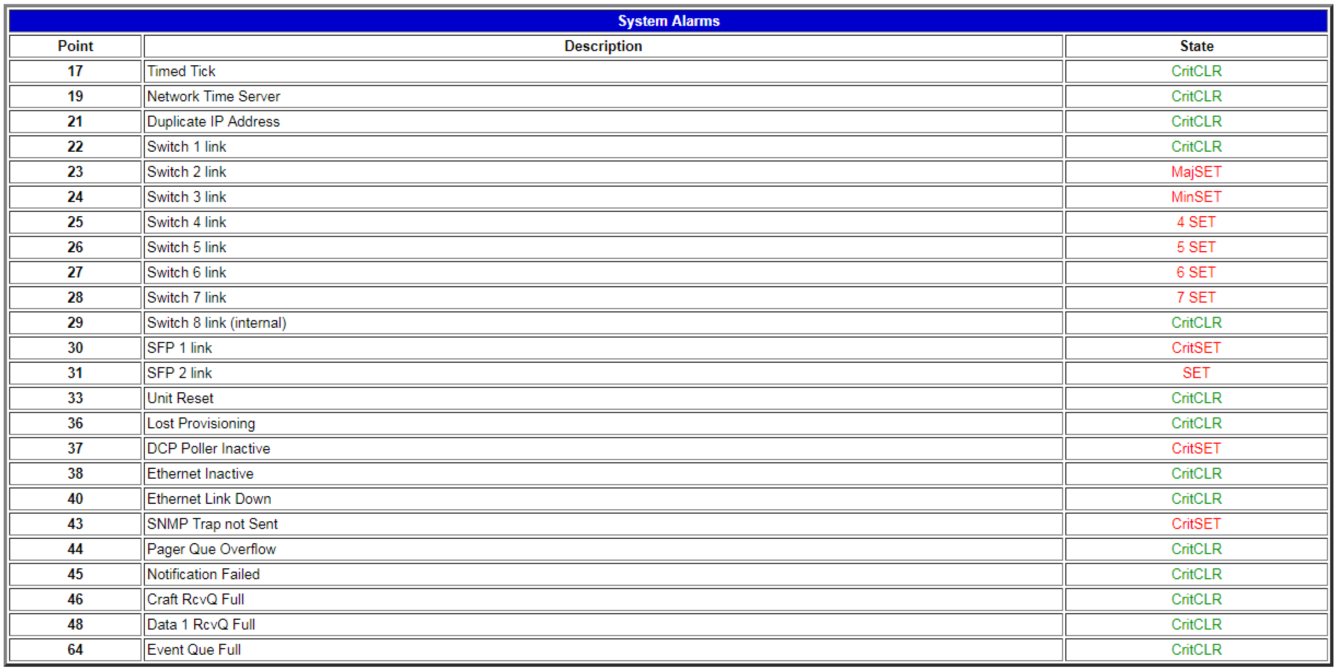
Use the following rules to operate controls:
1. Select **Controls** from the **Monitor** menu.
2. Under the State field, choose a command (Opr - operate, Rls - release, or Mom - momentary).

3. Click **Submit Data** to issue the control.

Hot Tip!

The control relay's normal state - open or closed - is determined by a PCB jumper. Operating a control thus changes the normal state of the relay (energizes it) until it is released (de-energized). The momentary command energizes the relay for approximately one second before it is released again.

3.6 Monitoring System Alarms



System Alarms

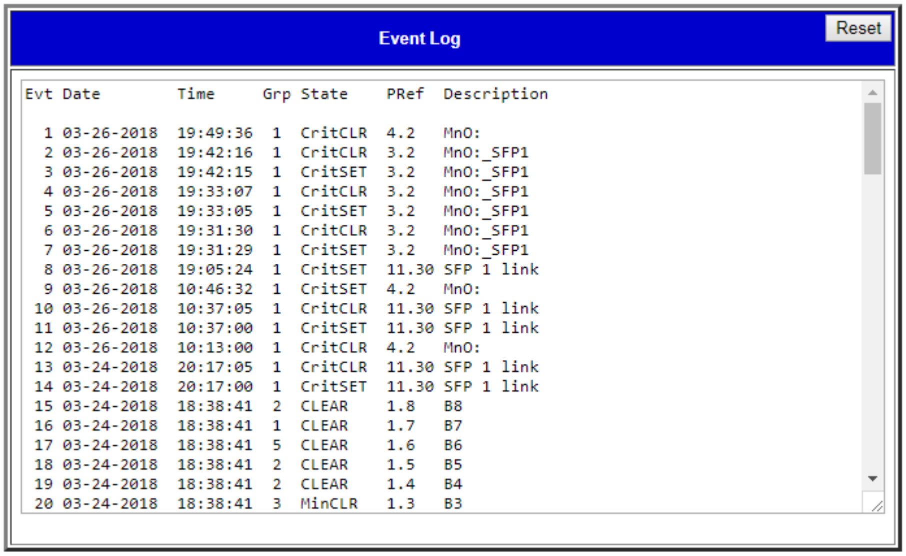
Point	Description	State
17	Timed Tick	CritCLR
19	Network Time Server	CritCLR
21	Duplicate IP Address	CritCLR
22	Switch 1 link	CritCLR
23	Switch 2 link	MajSET
24	Switch 3 link	MinSET
25	Switch 4 link	4 SET
26	Switch 5 link	5 SET
27	Switch 6 link	6 SET
28	Switch 7 link	7 SET
29	Switch 8 link (internal)	CritCLR
30	SFP 1 link	CritSET
31	SFP 2 link	SET
33	Unit Reset	CritCLR
36	Lost Provisioning	CritCLR
37	DCP Poller Inactive	CritSET
38	Ethernet Inactive	CritCLR
40	Ethernet Link Down	CritCLR
43	SNMP Trap not Sent	CritSET
44	Pager Que Overflow	CritCLR
45	Notification Failed	CritCLR
46	Craft RcvQ Full	CritCLR
48	Data 1 RcvQ Full	CritCLR
64	Event Que Full	CritCLR

View the status of the System Alarms from the Monitor > System Alarms screen

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

Refer to the Reference Section for system alarm trap numbers.

3.7 Event Logging



```
Evt Date        Time     Grp State    PRef  Description

  1 03-26-2018  19:49:36  1  CritCLR  4.2   MnO:
  2 03-26-2018  19:42:16  1  CritCLR  3.2   MnO:_SFP1
  3 03-26-2018  19:42:15  1  CritSET  3.2   MnO:_SFP1
  4 03-26-2018  19:33:07  1  CritCLR  3.2   MnO:_SFP1
  5 03-26-2018  19:33:05  1  CritSET  3.2   MnO:_SFP1
  6 03-26-2018  19:31:30  1  CritCLR  3.2   MnO:_SFP1
  7 03-26-2018  19:31:29  1  CritSET  3.2   MnO:_SFP1
  8 03-26-2018  19:05:24  1  CritSET  11.30 SFP 1 link
  9 03-26-2018  10:46:32  1  CritSET  4.2   MnO:
 10 03-26-2018  10:37:05  1  CritCLR  11.30 SFP 1 link
 11 03-26-2018  10:37:00  1  CritSET  11.30 SFP 1 link
 12 03-26-2018  10:13:00  1  CritCLR  4.2   MnO:
 13 03-24-2018  20:17:05  1  CritCLR  11.30 SFP 1 link
 14 03-24-2018  20:17:00  1  CritSET  11.30 SFP 1 link
 15 03-24-2018  18:38:41  2  CLEAR    1.8   B8
 16 03-24-2018  18:38:41  1  CLEAR    1.7   B7
 17 03-24-2018  18:38:41  5  CLEAR    1.6   B6
 18 03-24-2018  18:38:41  2  CLEAR    1.5   B5
 19 03-24-2018  18:38:41  2  CLEAR    1.4   B4
 20 03-24-2018  18:38:41  3  MinCLR   1.3   B3
```

Monitor the last 100 events recorded by the NetGuardian in the Event Log window.

Event Log Field	Description
Evt	Event number (1-100)
Date	Date the event occurred*
Time	Time the event occurred*
St	State of the event (A=alarm, C=clear)
Pref	Point reference. See Reference Section for display descriptions.
Description	User defined description of the event as entered in the alarm point and relay description fields

Event Logging window field descriptions

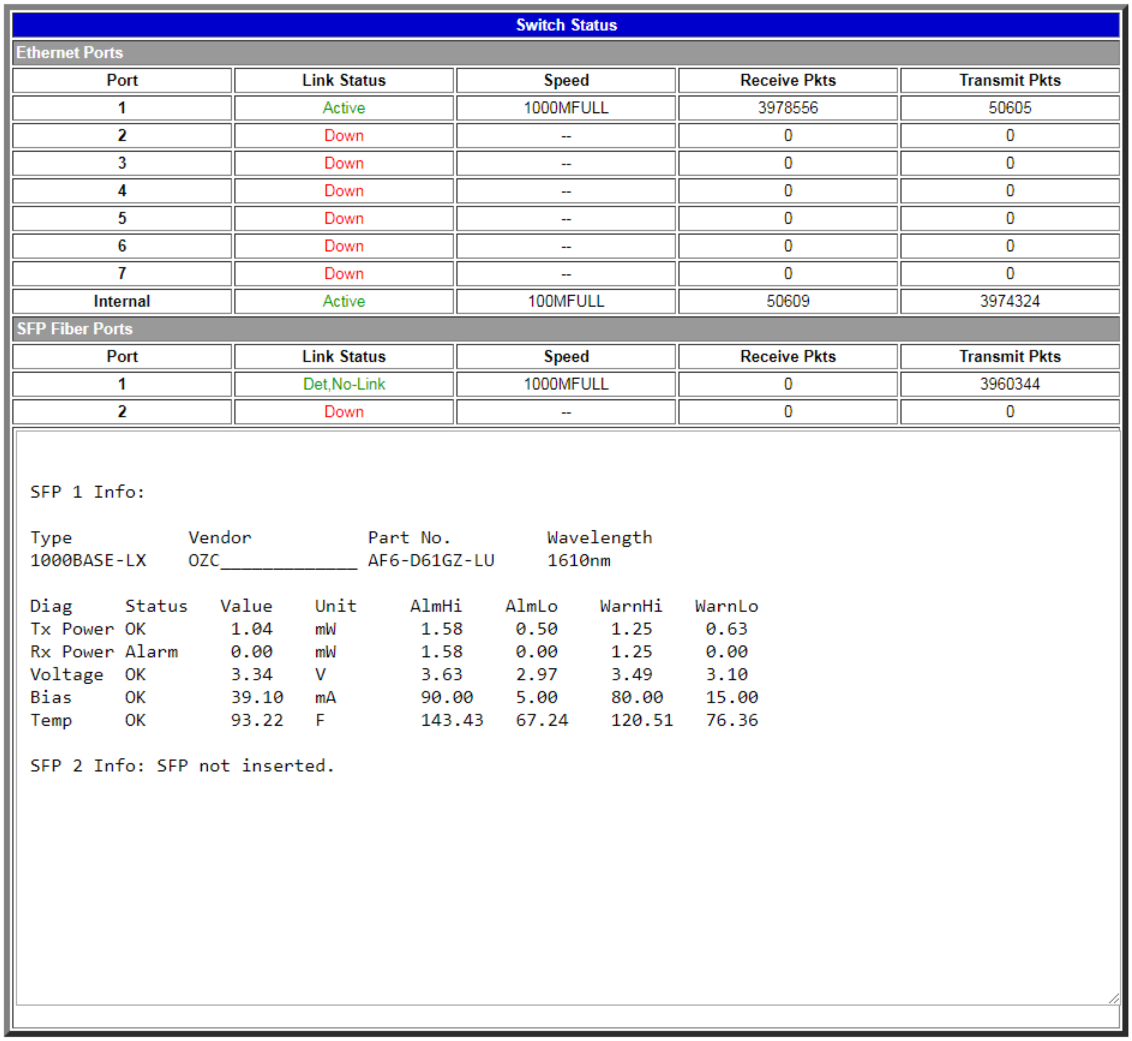
The NetGuardian 216F Event Log supports the following features:
You can filter Event Log entries by Alarm Point Group, to see only the alarms you want.
You can reset the Event Log to clear old alarms from the display.
You can reset the Event Log by Alarm Point Group; for example, clear power alarms while retaining intruder alarms.

Click on the Monitor menu > Event Log link to view the event log. The NetGuardian's Event Log allows the NetGuardian to post and monitor up to 100 events including power up, base and system alarms, ping alarms, analog alarms, and controls. Posted events for the various alarms include both alarm and clear status (see tabe above for Event Alarm field descriptions).

Note: All information in the event log will be erased upon reboot or a power failure.

* DCPx versions of the NetGuardian automatically timestamp events before sending them to the event logs. The time is based on the real-time clock (if installed). If there is no real-time clock installed, the time is based on the NetGuardian's software clock (requires resetting after power failure or power cycle).

3.8 Monitoring Data Port Activity



Switch Status

Ethernet Ports

Port	Link Status	Speed	Receive Pkts	Transmit Pkts
1	Active	1000MFULL	3978556	50605
2	Down	--	0	0
3	Down	--	0	0
4	Down	--	0	0
5	Down	--	0	0
6	Down	--	0	0
7	Down	--	0	0
Internal	Active	100MFULL	50609	3974324

SFP Fiber Ports

Port	Link Status	Speed	Receive Pkts	Transmit Pkts
1	Det,No-Link	1000MFULL	0	3960344
2	Down	--	0	0

```
SFP 1 Info:

Type         Vendor           Part No.        Wavelength
1000BASE-LX  OZC_____________ AF6-D61GZ-LU    1610nm

Diag     Status   Value    Unit     AlmHi    AlmLo    WarnHi   WarnLo
Tx Power OK        1.04    mW        1.58     0.50     1.25     0.63
Rx Power Alarm     0.00    mW        1.58     0.00     1.25     0.00
Voltage  OK        3.34    V         3.63     2.97     3.49     3.10
Bias     OK        39.10   mA        90.00    5.00     80.00    15.00
Temp     OK        93.22   F         143.43   67.24    120.51   76.36

SFP 2 Info: SFP not inserted.
```

To view the data being received by the connected equipment, select Switch Status from the Monitor menu.

The **Ethernet Ports** and **SFP Fiber Ports** tables provide live status information for the data port by displaying transmit or receive activity in ASCII. See Reference Section, "ASCII Conversion" for specific ASCII symbol conversion.

4 Reference Section

4.1 Display Mapping

Port	Address	Display	Description	Set	Clear
99	1	1	Discrete Alarms 1-16	8001-8016	9001-9016
99	1	2	Ping Table	8065-8096	9065-9096
99	1	3	Analog Channel 1**	8129-8132	9129-9132
99	1	4	Analog Channel 2**	8193-8196	9193-9196
99	1	5	Analog Channel 3**	8257-8260	9257-9260
99	1	6	Analog Channel 4**	8321-8324	9321-9324
99	1	7	Analog Channel 5–Power Feed A**	8385-8388	9385-9388
99	1	8	Analog Channel 6–Power Feed B**	8449-8452	9449-9452
99	1	9	Analog Channel 7–Internal Temp Sensor**	8513-8516	9513-9516
99	1	10	Analog Channel 8–External Temp Sensor**	8577-8580	9577-9580
99	1	11	Relays/System Alarms (See table below)	8641-8674	9641-9674
99	1	12	NetGuardian Expansion 1 Alarms 1-48	6001-6064	7001-7064
99	1	13	NetGuardian Expansion 1 Relays 1-8	6065-6072	7065-7072
99	1	14	NetGuardian Expansion 2 Alarms 1-48	6129-6177	7129-7177
99	1	15	NetGuardian Expansion 2 Relays 1-8	6193-6200	7193-7200
99	1	16	NetGuardian Expansion 3 Alarms 1-48	6257-6305	7257-7305
99	1	17	NetGuardian Expansion 3 Relays 1-8	6321-6328	7321-7328

Display descriptions and SNMP Trap numbers for the NetGuardian

* The TRAP number ranges shown correspond to the point range of each display. For example, the SNMP Trap "Set" number for alarm 1 (in Display 1) is 8001, "Set" for alarm 2 is 8002, "Set" for alarm 3 is 8003, etc.
** The TRAP number descriptions for the Analog channels (1-8) are in the following order: minor under, minor over, major under, and major over. For example, for Analog channel 1, the "Set" number for minor under is 8129, minor over is 8130, major under is 8131, and major over is 8132.

			SNMP Trap #s
Points	Description	Set	Clear
1	Relays	8641	9641
2	Relays	8642	9642
3	Relays	8643	9643
4	Relays	8644	9644
5	Relays	8645	9645
6	Relays	8646	9646
7	Relays	8647	9647
8	Relays	8648	9648
9	Undefined**	8649	9649
10	Undefined**	8650	9650
11	Undefined**	8651	9651
12	Undefined**	8652	9652
13	Undefined**	8653	9653
14	Undefined**	8654	9654
15	Undefined**	8655	9655
16	Undefined**	8656	9656
17	Timed Tick	8657	9657

Display 11 System Alarms point descriptions (continues on next page)

		SNMP Trap #s	
Points	Description	Set	Clear
18	Exp. Module Callout	8658	9658
19	Network Time Server	8659	9659
20	Accumulation Event	8660	9660
21	Duplicate IP Address	8661	9661
22	Undefined**	8662	9662
23	Undefined**	8663	9663
24	Undefined**	8664	9664
25	Undefined**	8665	9665
26	Undefined**	8666	9666
27	Undefined**	8667	9667
28	Undefined**	8668	9668
29	Undefined**	8669	9669
30	Undefined**	8670	9670
31	Undefined**	8671	9671
32	Undefined**	8672	9672
33	Unit Reset	8673	9673
34	Undefined**	8674	9674
35	Undefined**	8675	9675
36	Lost Provisioning	8676	9676
37	DCP Poller Inactive	8677	9677
38	NET1 not active	8678	9678
40	NET Link Down	8680	9680
41	Modem not	8681	9681
42	No dial-tone	8682	9682
43	SNMP Trap not Sent	8683	9683
44	Pager Que Overflow	8684	9684
45	Notification failed	8685	9685
46	Craft RcvQ full	8686	9686
47	Modem RcvQ full	8687	9687
48	Data 1 RcvQ full	8688	9688
49	Data 2 RcvQ full	8689	9689
50	Data 3 RcvQ full	8690	9690
51	Data 4 RcvQ full	8691	9691
52	Data 5 RcvQ full	8692	9692
53	Data 6 RcvQ full	8693	9693
54	Data 7 RcvQ full	9694	9694
55	Data 8 RcvQ full	8695	9695
56	NetGuardian DX 1 fail	8696	9696
57	NetGuardian DX 2 fail	8697	9697
58	NetGuardian DX 3 fail	8698	9698
59	GLD/BSU 1 Fail	8699	9699
60	GLD/BSU 2 Fail	8700	9700
61	GLD/BSU 3 Fail	8701	9701
62	CHAN timeout	8702	9702
63	Craft Timeout	8703	9703
64	Event Que Full	8704	9704

Display 11 System Alarms point descriptions (continued)

* Data Ports 2-5 are included on optional expansion card.

Note: See section: "System Alarms Display Map," for detailed descriptions of the NetGuardian's system alarms.

4.1.1 System Alarms Display Map

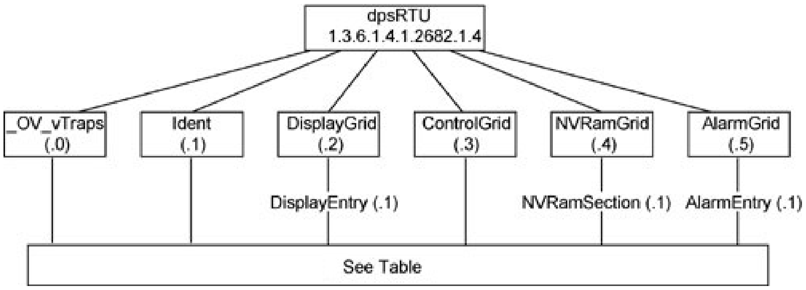
Display	Points	Alarm Point	Description	Solution
11	17	Timed Tick	Toggles state at constant rate as configured by the Timed Tick timer variable. Useful in testing integrity of SNMP trap alarm reporting.	To turn the feature off, set the Timed Tick timer to 0.
	19	Network Time Server	Communication with Network Time Server has failed.	Try pinging the Network Time Server's IP Address as it is configured. If the ping test is successful, then check the port setting and verify the port is not being blocked on your network.
	21	Duplicate IP Address	The unit has detected another node with the same IP Address.	Unplug the LAN cable and contact your network administrator. Your network and the unit will most likely behave incorrectly. After assigning a correct IP Address, reboot the unit to clear the System alarm.
	33	Power Up	The unit has just come-online. The set alarm condition is followed immediately by a clear alarm condition.	Seeing this alarm is normal if the unit is powering up.
	36	Lost Provisioning	The internal NVRAM may be damaged. The unit is using default configuration settings.	Use Web or latest version of NGEditG5 to configure unit. Power cycle to see if alarm goes away. May require RMA.
	37	DCP Poller Inactive	The unit has not seen a poll from the Master for the time specified by the DCP Timer setting.	If DCP responder is not being used, then set the DCP Unit ID to 0. Otherwise, try increasing the DCP timer setting under timers, or check how long it takes to cycle through the current polling chain on the Master system.
	38	Ethernet not active	The Net1 LAN port is down.	Check LAN cable. Ping to and from the unit. (If not using Net1 or Net2, set IP, Subnet and Gateway to 255's)
	40	LNK Alarm	No network connection detected	
	41	Modem not responding	An error has been detected during modem initialization. The modem did not respond to the initialization string.	Remove configured modem initialization string, then power cycle the unit. If alarm persists, try resetting the Modem port from the TTY interface, or contact DPS for possible RMA.
	43	SNMP Trap not Sent	SNMP trap address is not defined and an SNMP trap event occurred.	Define the IP Address where you would like to send SNMP trap events, or configure the event not to trap.
	44	Pager Queue Overflow	Over 250 events are currently queued in the pager queued and are still trying to report.	Check for failed notification events that may be filling up the pager queue. There may be a configuration or communication problem with the notification events.
	45	Notification failed	A notification event, like a page or email, was unsuccessful.	Use RPT filter debug to help diagnose notification problems.
	46	Craft RcvQ full	The Craft port received more data than it was able to process.	Disconnect whatever device is connected to the craft serial port. This alarm should not occur.
	47	Modem RcvQ full	The modem port received more data than it was able to process.	Check what is connecting to the NetGuardian. This alarm should not occur.
	48	Serial 1 RcvQ full	Serial port 1 (or appropriate serial port number) receiver filled with 8 K of data (4 K if BAC active).	Check proxy connection. The serial port data may not be getting collected as expected.
	49	Serial 2 RcvQ full		
	50	Serial 3 RcvQ full		
	51	Serial 4 RcvQ full		
	52	Serial 5 RcvQ full		
	53	Serial 6 RcvQ full		
	54	Serial 7 RcvQ full		
	55	Serial 8 RcvQ full		

System Alarms Descriptions

*Data Ports 2-5 are included on optional expansion card.

4.2 SNMP Manager Functions

The SNMP Manager allow s the user to view alarm status, set date/time, issue controls, and perform a resync. The display and tables below outline the MIB object identifiers. Table B.1 begins w ith dpsRTU; how ever, the MIB object identifier tree has several levels above it. The full English name is as follow s: root.iso.org.dod.internet.private.enterprises.dps-Inc.dpsAlarmControl.dpsRTU. Therefore, dpsRTU's full object identifier is 1.3.6.1.4.1.2682.1.2. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the Control Grid is 1.3.6.1.4.1.2682.1.2.3.3 because the object identifier of dpsRTU is 1.3.6.1.4.1.2682.1.2 + the Control Grid (.3) + the Display (.3).



Tbl. B1 (O.)_OV_Traps points
_OV_vTraps (1.3.6.1.4.1.2682.1.2.0)
PointSet (.20)
PointClr (.21)
SumPSet (.101)
SumPClr (.102)
ComFailed (.103)
ComRestored (.014)
P0001Set (.10001) through P0064Set (.10064)
P0001Clr (.20001) through P0064Clr (.20064)

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

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

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

Tbl. 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

The NetGuardian 216F OID has changed from 1.3.6.1.4.1.2682.1.4 to 1.3.6.1.4.1.2682.1.2 Updated MIB files are available on the Resource CD or upon request.

	Description	Port	Address	Point
Display 1	Discrete Alarms	99	1	1-32
	Undefined	99	1	33-64
Display 2	Ping Targets	99	1	1-32
	Undefined	99	1	33-64
Display 3	Analog 1	99	1	1-4
	Undefined	99	1	5-64
Display 4	Analog 2	99	1	1-4
	Undefined	99	1	5-64
Display 5	Analog 3	99	1	1-4
	Undefined	99	1	5-64
Display 6	Analog 4	99	1	1-4
	Undefined	99	1	5-64
Display 7	Analog 5	99	1	1-4
	Undefined	99	1	5-64
Display 8	Analog 6	99	1	1-4
	Undefined**	99	1	5-64
Display 9	Analog 7	99	1	1-4
	Undefined**	99	1	5-64
Display 10	Analog 8	99	1	1-4
	Undefined**	99	1	5-64
Display 11	Relays 1-8	99	1	1-8
	Undefined**	99	1	9-16
	Timed Tick	99	1	17
	Exp. Module Callout	99	1	18
	Network Time Server	99	1	19
	Accumulation Event	99	1	20
	Duplicate IP Address	99	1	21
	Undefined**	99	1	22-32
	Unit Reset	99	1	33
	Undefined**	99	1	34-35
	Lost Provisioning	99	1	36
	DCP poll inactive	99	1	37
	NET 1 not active	99	1	38
	NET 2 not active	99	1	39
	NET link down	99	1	40
	Modem not responding	99	1	41
	No dial-tone	99	1	42
	SNMP trap not sent	99	1	43
	Pager Queue Overflow	99	1	44
	Notification failed	99	1	45
	Craft RCVQ full	99	1	46
	Modem RCVQ	99	1	47
	Data 1-8 RCVQ	99	1	48-55
	NGDdx 1-3 fail	99	1	56-58
	GLD/BSU 1-3 fail	99	1	59-61
	CHAN timeout	99	1	62
	CRFT timeout	99	1	63
	Event Que Full	99	1	64

Alarm Point Descriptions

* "No data" indicates that the alarm point is defined but there is no description entered.

** "Undefined" indicates that the alarm point is not used.

^ Data Ports 2-5 are included on optional expansion card.

4.3 SNMP Granular Trap Packets

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

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

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

UDP Headers and descriptions

SNMP Header	Description
0	Version
Public	Request
Trap	Request
1.3.6.1.4.1.2682.1.2	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 216F v1.0B	Value
1.3.6.1.2.1.1.6.0	Object
1-800-622-3314	Value
1.3.6.1.4.1.2682.1.2.4.1.0	Object
01-02-1995 05:08:27.760	Value
1.3.6.1.4.1.2682.1.2.5.1.1.99.1.1.1	Object
99	Value
1.3.6.1.4.1.2682.1.2.5.1.4.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.3.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.2.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.5.99.1.1.1	Object
Rectifier Failure	Value
1.3.6.1.4.1.2682.1.2.5.1.6.99.1.1.1	Object
Alarm	Value

SNMP Headers and descriptions

4.4 ASCII Conversion

The information contained in the table below is a list of ASCII symbols and their meanings. Refer to the bulleted list below to interpret the ASCII data transmitted or received through the data port. Port transmit and receive activity can be viewed from the Web browser interface.

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

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

ASCII symbols

5 Frequently Asked Questions

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

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

5.1 General FAQs

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

Q. How do I connect my NetGuardian to the LAN?
A. To connect your NetGuardian 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 NetGuardian's IP configuration requires a reboot.

Q. When I connect to the NetGuardian through the craft port on the front panel it either doesn't work right or it doesn't work at all. What's going on?
A. Make sure your using the right COM port settings. 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.

Q. I can't change the craft port baud rate.
A. If you select a higher baud rate, you must set your terminal emulator program to the new baud rate and press Enter. If your terminal emulator is set to a slower baud rate than the craft port, normal keys can appear as a break key — and the craft port interprets a break key as an override that resets the baud rate to the standard 9600 baud.

Q. How do I use the NetGuardian to access TTY interfaces on remote site equipment?
A. If your remote site device supports RS-232, you can connect it to one of the eight data ports located on the NetGuardian back panel. To make the data port accessible via LAN, configure the port for TCP/IP operation. You now have a LAN-based proxy port connection that lets you access your device's TTY interface through a Telnet session.

Q. How do I telnet to the NetGuardian?
A. Configure your Telnet client with these options:

1. Connect using TCP/IP (**not** "Telnet," or any other port options)
2. Enter the IP address of the NetGuardian
3. Enter **Port 2002**

Example:
To connect using the Windows Telnet client, click Start, click Run, and type telnet 126.12.220.8 2002.

Telnet is connected through the 10BaseT switch. Make sure you're connected to one of the switch's 7 connectors.

Q. I just changed the port settings for one of my data ports, but the changes did not seem to take effect even after I wrote the NVRAM.

A. In order for data port and craft port changes (including changes to the baud rate and word format) to take effect, the NetGuardian must be rebooted. Whenever you make changes, remember to write them to the NetGuardian's NVRAM so they will be saved when the unit is rebooted.

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

Q. What do the terms "port," "address," "display" and "alarm point" mean?

A. These terms refer to numbers that designate the location of a network alarm, from the most general (a port to which several devices are connected) to the most specific (an individual alarm sensor).

Port: A number designating a serial port through which a monitoring device collects data.

Address: A number designating a device connected to a port.

Display: A number designating a logical group of 64 alarm points.

Alarm Point: A number designating a contact closure that is activated when an alarm condition occurs. For example, an alarm point might represent a low oil sensor in a generator or an open/close sensor in a door.

These terms originally referred only to physical things: actual ports, devices, and contact closures. For the sake of consistency, port-address-display-alarm point terminology has been extended to include purely logical elements: for example, the NetGuardian reports internal alarms on Port 99, Address 1.

Q. What characteristics of an alarm point can be configured through software? For instance, can point 4 be used to sense an active-low signal, or point 5 to sense a level or a edge?

A. The NetGuardian's standard configuration is for all alarm points to be level-sensed. You **cannot** use configuration software to convert alarm points to TTL (edge-sensed) operation. TTL alarm points are a hardware option that must be specified when you order your NetGuardian. Ordering TTL points for your NetGuardian does not add to the cost of the unit What you can do with the configuration software is change any alarm point from "Normal" to "Reversed" operation. Switching to Reversed operation has different effects, depending on the kind of input connected to the alarm point:

- **If the alarm input generates an active-high signal**, switching to Reversed operation means the NetGuardian will declare an alarm in the absence of the active-high signal, creating the practical equivalent of an active-low alarm.
- **If the alarm input generates an active-low signal**, switching to Reversed operation means the NetGuardian will declare an alarm in the absence of the active-low signal, creating the practical equivalent of an active-high alarm.
- **If the alarm input is normally open**, switching to Reversed operation converts it to a normally closed alarm point.
- **If the alarm input is normally closed**, switching to Reversed operation converts it to a normally open alarm point.

Q. Every time my NetGuardian starts up, I have to reenter the date and time. How can I get the NetGuardian to automatically maintain the date and time setting?

A. You have three options for keeping the correct time on your NetGuardian:

Real Time Clock Option: You can order your NetGuardian with the Real Time Clock hardware option. Once it's set, the Real Time Clock will keep the correct date and time, regardless of reboots.

Network Time Protocol Synchronization: If your NetGuardian has Firmware Version 2.9F or later, you can configure the unit to automatically synchronize to a Network Time Protocol (NTP) server.

- To get the latest NetGuardian firmware, sign in to MyDPS at www.dpstelecom.com/mydps.
- For instructions on configuring your NetGuardian to use NTP synchronization, see your Edit216F or NetGuardian Web Browser Interface user manual.

T/Mon RTU Time Sync Signal: You can configure your T/Mon NOC to send an RTU Time Sync signal at a regular interval, which you can set to any time period between 10 and 10,080 minutes. The Time Sync will automatically synchronize the NetGuardian's clock to the T/Mon's clock. And if you set your T/Mon to NTP synchronization, you'll make sure you have consistent, accurate time stamps throughout your monitoring network.

Q. How do I back up my NetGuardian configuration?
A. There are two ways to back up NetGuardian configuration files:

- **Use Edit216F:**
- NGEdit4 can read the configuration of a NetGuardian unit connected to your PC via LAN, modem or COM port. You can then use NGEdit4 to save a NetGuardian configuration file on your PC's hard disk or on a floppy disk. With Edit216F you can also make changes to the configuration file and write the changed configuration to the NetGuardian's NVRAM.
- **Use FTP:**
- You can use File Transfer Protocol (FTP) to read and write configuration files to the NetGuardian's NVRAM, but you can't use FTP to edit configuration files.

5.2 SNMP FAQs

Q. Which version of SNMP is supported by the SNMP agent on the NetGuardian?
A. SNMP v1 and v2.0c.

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

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

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

Q. How many traps are triggered when a single point is set or cleared? The MIB defines traps like "major alarm set/cleared," "RTU point set," and a lot of granular traps, which could imply that more than one trap is sent when a change of state occurs on one point.
A. Generally, a single change of state generates a single trap, but there are two exception to this rule. Exception 1: the first alarm in an "all clear" condition generates an additional "summary point set" trap. Exception 2: the final clear alarm that triggers an "all clear" condition generates an additional "summary point clear" trap.

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

Q. The NetGuardian manual talks about two control relay outputs. How do I control these from my SNMP manager?
A. The control relays are operated by issuing the appropriate set commands, which are contained in the DPS Telecom MIB. For more information about the set commands, see Reference Section, "Display Mapping," in any of the NetGuardian software configuration guides.

Q. How can I associate descriptive information with a point for the RTU granular traps?
A. The NetGuardian alarm point descriptions are individually defined using the Web Browser, TTY, or Edit216F configuration interfaces.

Q. My SNMP traps aren't getting through. What should I try?
A. Try these three steps:

1. Make sure that the Trap Address (IP address of the SNMP manager) is defined. (If you changed the Trap Address, make sure you saved the change to NVRAM and rebooted.)
2. Make sure all alarm points are configured to send SNMP traps.
3. Make sure the NetGuardian and the SNMP manager are both on the network. Use the NetGuardian's ping command to ping the SNMP manager.

6 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.*

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

The Protocol Alarm Monitoring Ezine

DPS Telecom

White Paper: 5 Steps to Intelligent SNMP-Legacy Integration

[illegible]

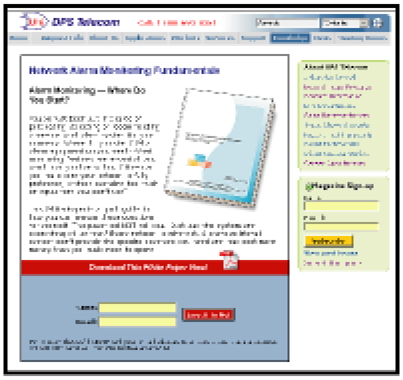
Turbocharge Your NetGuardian With SNMP v2c

[illegible]

Creative Solution: Convert Your LEDs to Contact Closures

[illegible]

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



DPS Telecom

Network Alarm Monitoring Fundamentals

Alarm Monitoring — Where Do You Start?

[illegible]

Download This White Paper Now!

Free Tech Support on the Web: MyDPS

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

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

DPS Telecom

"Your Partners in Network Alarm Monitoring"

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