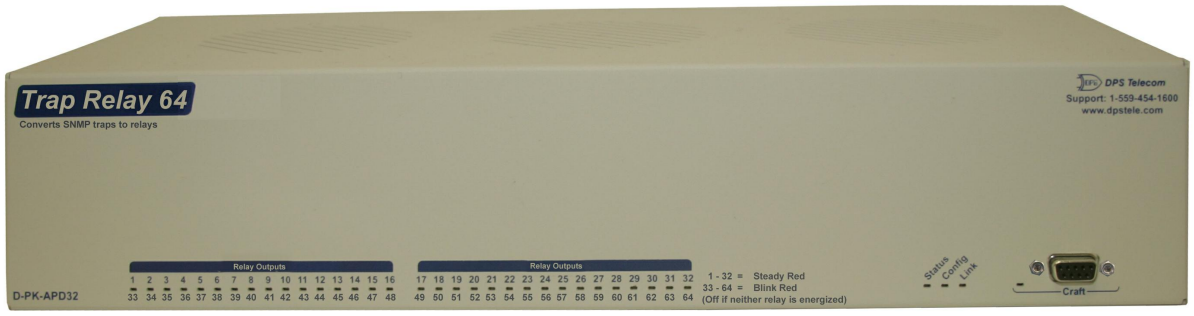
DPS Telecom

"Your Partners In Network Alarm Monitoring"

Trap Relay 32/64

USER MANUAL



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

November 25, 2020 **D-UM-APD32-TRP64** **Firmware Version 1.0A**

Revision History	
November 25, 2020	Shunting for normally open/closed relays
April 17, 2019	SNMP Set support v1 and v2
October 24, 2016	Added control sections
April 4, 2013	Added an additional variable binding
October 25, 2012	Added variable bindings
October 5, 2012	Updated to reflect support for both 32 and 64 versions
September 20, 2012	Added ping targets
May 21, 2012	Updated Configuring Granular Mode and Amphenol Pinout
May 8, 2012	Added control configuration with IP description
April 19, 2012	Added Amphenol pinout information
March 30, 2012	Initial release

Notice

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

Contents

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

1 Trap Relay 32/64 Overview **1**

2 Specifications **2**

3 Shipping List **3**

4 Installation **4**

4.1 Tools Needed 4

4.2 Mounting 5

5 Trap Relay 64 Back Panel **6**

5.1 Power Connection 6

5.2 LAN Connection 7

5.3 8-Pin Screw Lug Connectors 7

5.4 (Optional) 50-Pin Control Relay Connector 10

6 Trap Relay 64 Front Panel **11**

6.1 DB9 Craft Port 11

7 Quick Start: How to Connect to the Trap Relay 64 **11**

7.1 ...via DB9 Craft Port (using TTY Interface) 11

7.2 ...via LAN 12

8 TTY Interface **13**

9 Trap Relay 64 Web Browser **14**

9.1 Logging on to the Trap Relay 64 14

9.1.1 Changing the Default Password 14

10 Trap Relay 64 - Quick Turn Up **16**

10.1 How to Send Email Notifications 16

11 Edit Menu Field Descriptions **20**

11.1 System 20

11.2 Ethernet 21

11.3 Notifications 22

11.3.1 Notification Settings 23

11.3.2 Schedule 24

11.4 System Alarms 25

11.5 Variable Bindings 26

11.6 Controls 27

11.6.1 Configuring Granular and Cisco-VMS OIDs 29

11.6.2 Derived Controls 31

11.7 Ping Targets 32

11.8 Date and Time 33

11.9 Timers 34

11.10 Reboot 34
12 Monitoring via the Web Browser 35
12.1 Monitoring System Alarms 35
12.2 Monitoring Virtual Alarms 36
12.2.1 Editing Virtual Alarms 37
12.3 Controls 38
12.4 Ping Targets 39
13 Firmware Upgrade 40
14 Reference Section 41
14.1 Front and Back Panel LEDs 41
14.2 Display Mapping 43
14.3 SNMP Manager Functions 43
14.4 SNMP Granular Trap Packets 44
14.5 Shunting for Normally Open/Closed Relays 46
15 Frequently Asked Questions 47
15.1 General FAQs 48
15.2 SNMP FAQs 49
16 Technical Support 50
17 End User License Agreement 51

1 Trap Relay 32/64 Overview

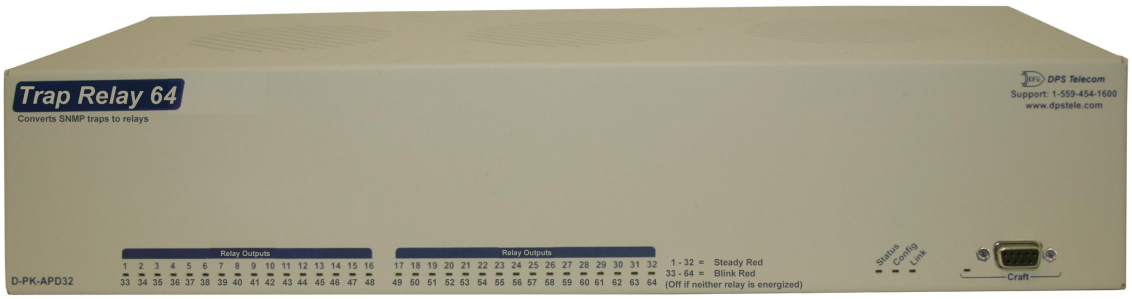


Fig. 1.1 *The easy-to-install Trap Relay 64 operates up to 64 relays*

Overview

The Trap Relay 32/64 is a device that operates up to 32 or 64 relays (depending on build option) using received SNMP trap information. Currently there are two supported trap processing modes of operation. Granular mode allows the user to configure each relay to operate or release based on the enterprise, generic-trap, and specific-trap information of a SNMP v1 trap or the trap OID of a SNMP v2c trap. In Cisco-VMS mode, the unit will ignore each relay's SNMP trap configuration and will momentarily operate relays when it receives either a mediaStreamDeviceUnreachable, mediaStreamConnectionLoss, or mediaStreamConfigFailure VMS 6.3 SNMP Trap. A relay in Cisco-VMS mode will only operate if its description matches the VMS trap's mediaStreamName value. This telco-grade remote is housed in a durable aluminum chassis that will require the use of two standard rack units for mounting.

Note: In this user manual, the Trap Relay 64 version is shown. All of the provisioning, configuring, and managing content is the same for both devices. The only difference is the number of control relays supported.

Multiple connectors can be used to securely terminate relay outputs

On the back panel of the Trap Relay 64 the 16 8-pin screw lug connectors securely terminate the relay outputs. An optional version of the Trap relay 64 uses four 50-pin amphenol connectors to terminate the 64 relay outputs.

- **32 or 64 Control Relay Outputs**
- **32 or 64 Ping Targets**

Visual alarm interface

The front panel LED indicators provide visual indication of relay point status. Two relays share one LED (ex. 1/33, 2/34 etc.). LEDs that are on indicate active relays. LEDs that are off indicate inactive relay points.

Web Browser Interface

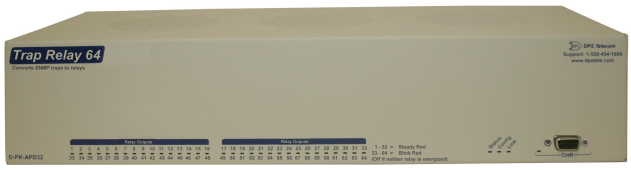
From the device's easy-to-use web interface, you do all of the configuration setup tasks like reversing the relay energize state on an individual basis. Additionally, from the web interface you are able to view the status of relay outputs.

2 Specifications

Control Relay Outputs:	32 or 64
Ping Targets:	32 or 64
Protocols:	HTTP, Telnet, ICMP, DCPX, SNMPv1, SNMPv2c
Dimensions:	3.47" H x 17.026 W x 7.336" D
	(8.81 cm x 43.25 cm x 18.63 cm)
Weight:	3.5 lbs. 3oz. (1.6 kg)
Mounting:	19" or 23" rack mount, 2 RU height
Power Input	
Voltage Options Include:	Dual Feed -48VDC (-36 to -72 VDC)
Current Draw:	250mA max for -48VDC (idle 50mA)
GMT Fuse:	3/4 Amp GMT Fuse
Interfaces:	1 RJ45 10BaseT half-duplex Ethernet port
	1 DB9 front-panel craft port
Visual Interface:	36 Front Panel LEDs
	5 Back Panel LEDs
Operating Temperature:	32° to 140° F (0° to 60° C)
Industrial Temperature Option:	-22° to 158° F (-30° to 70° C)
Operating Humidity:	0% to 95% non-condensing
MTBF:	60 years
Windows Compatibility:	Windows XP, Vista, 7 32/64 bit
RoHS:	5/6

3 Shipping List

Please make sure all of the following items are included with your Trap Relay 64. If parts are missing, or if you ever need to order new parts, please refer to the part numbers listed and call DPS Telecom at **1-800-622-3314**.



Trap Relay 64
D-PK-APD32

Trap Relay 64 User Manual
D-UM-APD32-TRP64

6 ft. DB9M-DB9F Download Cable
D-PR-045-10A-04

14 ft. Ethernet Cable
D-PR-923-10B-14

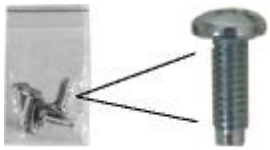
X2

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

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

x8

3/8" Ear Screws and Lock Washers
2-000-60375-05



x4

Rack Screws
1-000-12500-06

x4
Alternate Rack Screws
2-820-80750-03

Pads
2-015-00030-00

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

x 2
Lg. Power Connectors
(Main Power)
2-820-35102-00

x 16
Terminal Block, 8 Pt
2-821-10835-00 (Only included w/ pluggable version)

x 2
Grounding Lug Nuts
2-002-01420-00

4 Installation

4.1 Tools Needed

To install the Trap Relay 64, you'll need the following tools:

Phillips No. 2 Screwdriver

Small Standard No. 2 Screwdriver

PC with terminal emulator,
such as HyperTerminal

4.2 Mounting

Fig. 4.1 *The Trap Relay 64 can be flush or rear-mounted*

The compact Trap Relay 64 occupies two standard rack units. The Trap Relay 64 mounts in a 19" or 23" rack, and can be mounted on the right or left, in the flush-mount or rear mount locations, as shown in Fig. 4.1.

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

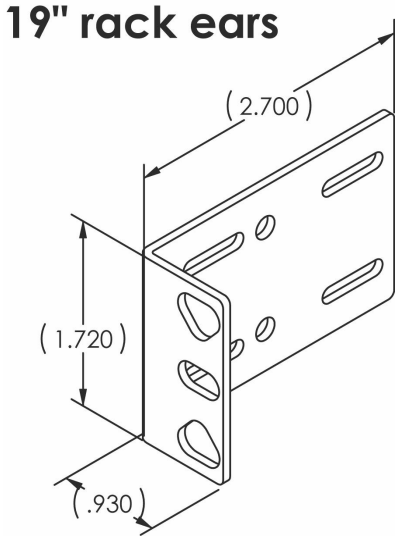


Fig. 4.2

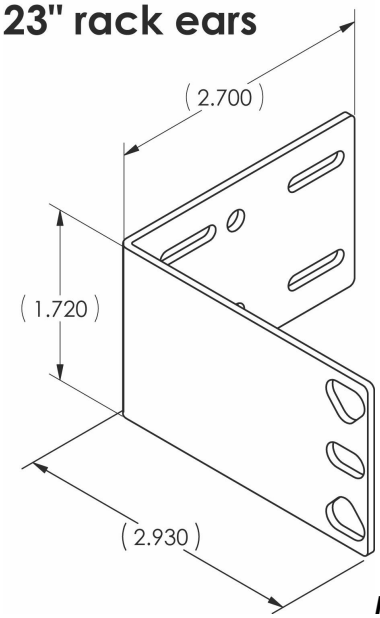


Fig. 4.3

5 Trap Relay 64 Back Panel

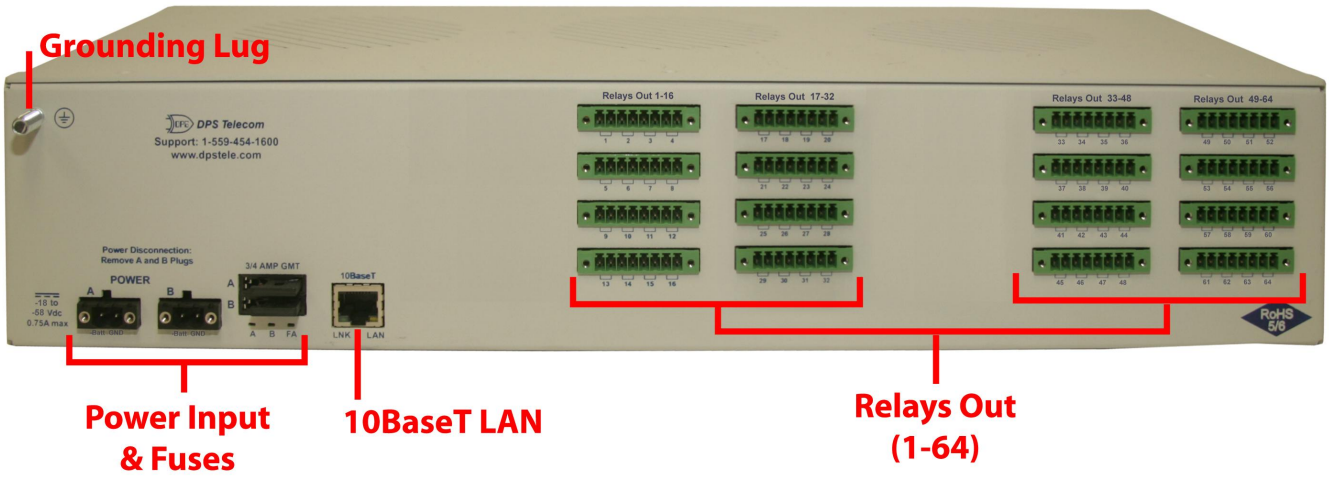


Fig 5.1 *Trap Relay 64 back panel connections*

5.1 Power Connection

The Trap Relay 64 is powered by two screw terminal barrier plug power connectors.

Fig. 5.2 *Screw terminal barrier plugs*

To connect the Trap Relay 64 to a power supply, follow these steps:

1. Always use safe power practices when making power connections. Be sure to remove fuses from the fuse distribution panel, as well as the back of the Trap Relay 64, before making your power connections.
2. Use the grounding lug to connect the unit to earth ground. The grounding lug is next to the symbol ⏚. Insert the eyelet of the earth ground cable between the two bolts on the grounding lug (Ground cable not included).
3. Insert a battery ground into the power connector plug's right terminal and tighten the screw; then insert a battery line to the plug's left terminal and tighten its screw.
4. Insert a fuse into the fuse distribution panel and measure voltage. The voltmeter should read between -18 and -58VDC (for the Wide Range build option), –36 and –72VDC (for -48VDC build option), +18 and +36VDC (+24VDC build option) or -18 and -36VDC (-24VDC build option).
5. The power plug can be inserted into the power connector only one way to ensure the correct polarity.

Note that the negative voltage terminal is on the left and the GND terminal is on the right.

6. Insert fuse into the Power A fuse slot. The power LED should be lit green. If the LED is off, the power connection may be reversed. To confirm that power is correctly connected, the front panel LEDs will flash RED and GREEN, indicating that the firmware is booting up.
7. Repeat steps 1 -6 for Power B connector.

5.2 LAN Connection

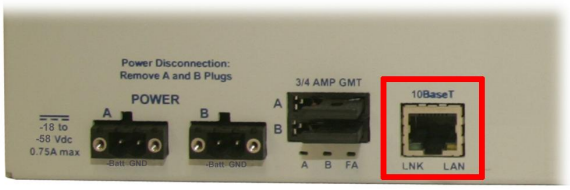


Fig. 5.3 *LAN Port*

To connect the Trap Relay 64 to the LAN, insert a standard RJ45 Ethernet cable into the 10BaseT Ethernet port on the back of the unit. If the LAN connection is OK, the LNK LED will illuminate **SOLID**.

5.3 8-Pin Screw Lug Connectors

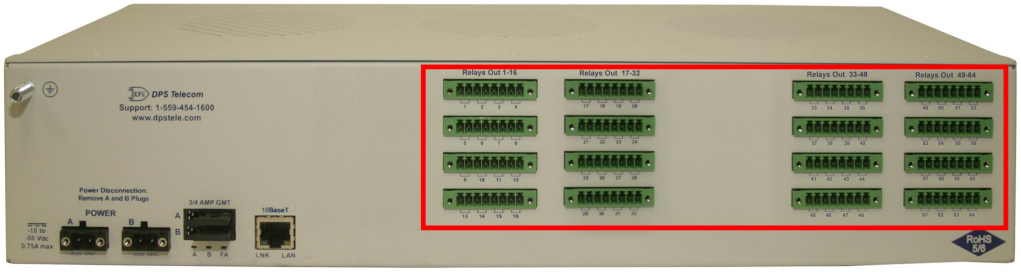


Fig 5.4 *Relay Screw Lug Connectors*

On the back panel of the Trap Relay 64 the sixteen 8-pin screw lug connectors securely terminate the relay outputs.

Fig 5.5 Inserting wire

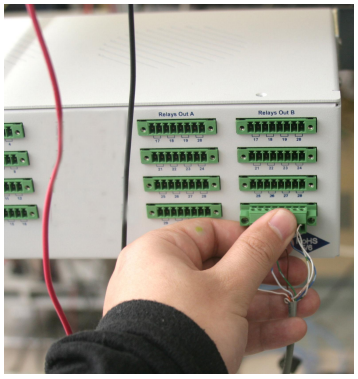


Fig 5.6 Inserting barrier plug

To insert wires into the terminal plugs, first completely loosen the tightening screw on the top of the terminal block. Then insert the wire into the open end of the connector

To connect the terminal plug in to the header, first verify the correct orientation of the connectors and insert the terminal plug into the header. To securely fasten the connectors tighten the locking screws on both sides of the terminal plug.

and tighten the screw until the wire is securely fastened.

Fig 5.7 Jumper configuration

Jumper NO/NC	Relays Out 1-32		Jumper NO/NC	Relays Out 33-64	
	Pluggable	Amphenol		Pluggable	Amphenol
1	1	32	33	33	64
2	2	31	34	34	63
3	3	30	35	35	62
4	4	29	36	36	61
5	5	28	37	37	60
6	6	27	38	38	59
7	7	26	39	39	58
8	8	25	40	40	57
9	9	24	41	41	56
10	10	23	42	42	55
11	11	22	43	43	54
12	12	21	44	44	53
13	13	20	45	45	52
14	14	19	46	46	51
15	15	18	47	47	50
16	16	17	48	48	49
17	17	16	49	49	48
18	18	15	50	50	47
19	19	14	51	51	46
20	20	13	52	52	45
21	21	12	53	53	44
22	22	11	54	54	43
23	23	10	55	55	42
24	24	9	56	56	41
25	25	8	57	57	40
26	26	7	58	58	39
27	27	6	59	59	38
28	28	5	60	60	37
29	29	4	61	61	36
30	30	3	62	62	35
31	31	2	63	63	34
32	32	1	64	64	33

Table 5.1 Relay and jumper configuration for 8-pin screw lug and 50-pin Amphenol connector options

Fig 5.8 Jumpers

The build option determines if jumpers are present. If they are not, the unit will be hand wired for either N/O if N/C on all relays. Check your product number description for your devices configuration.

5.4 (Optional) 50-Pin Control Relay Connector

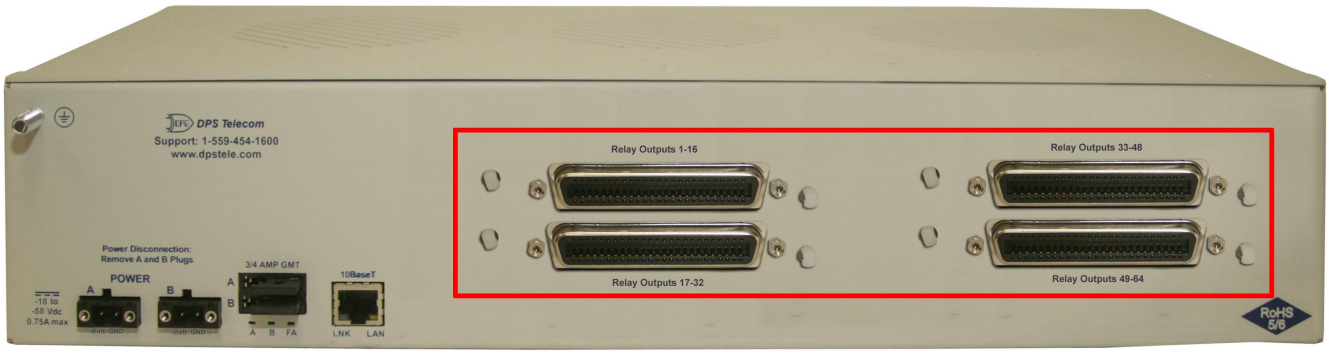


Fig 5.9 *50-pin Amphenol connectors*

An optional version of the Trap Relay 64 uses up to four 50-pin Amphenol connectors to securely terminate the relay outputs.

Control Relays 1-16 (33-48)			
Top	**Pin #**	**J1**	**Pin #**
CT 1 CO	1	CT 9 CO	9
CT 1 SW	26	CT 9 SW	34
CT 2 CO	2	CT 10 CO	10
CT 2 SW	27	CT 10 SW	35
CT 3 CO	3	CT 11 CO	11
CT 3 SW	28	CT 11 SW	36
CT 4 CO	4	CT 12 CO	12
CT 4 SW	29	CT 12 SW	37
CT 5 CO	5	CT 13 CO	13
CT 5 SW	30	CT 13 SW	38
CT 6 CO	6	CT 14 CO	14
CT 6 SW	31	CT 14 SW	39
CT 7 CO	7	CT 15 CO	15
CT 7 SW	32	CT 15 SW	40
CT 8 CO	8	CT 16 CO	16
CT 8 SW	33	CT 16 SW	41

Control Relays 17-32 (49-64)			
Bottom	**Pin #**	**J2**	**Pin #**
CT 17 CO	1	CT 25 CO	9
CT 17 SW	26	CT 25 SW	34
CT 18 CO	2	CT 26 CO	10
CT 18 SW	27	CT 26 SW	35
CT 19 CO	3	CT 27 CO	11
CT 19 SW	28	CT 27 SW	36
CT 20 CO	4	CT 28 CO	12
CT 20 SW	29	CT 28 SW	37
CT 21 CO	5	CT 29 CO	13
CT 21 SW	30	CT 29 SW	38
CT 22 CO	6	CT 30 CO	14
CT 22 SW	31	CT 30 SW	39
CT 23 CO	7	CT 31 CO	15
CT 23 SW	32	CT 31 SW	40
CT 24 CO	8	CT 32 CO	16
CT 24 SW	33	CT 32 SW	41

Control Relay connection pinout

Note: Relays 33-48 and 49-64 will follow the same pinout configuration as relays 1-32.

6 Trap Relay 64 Front Panel

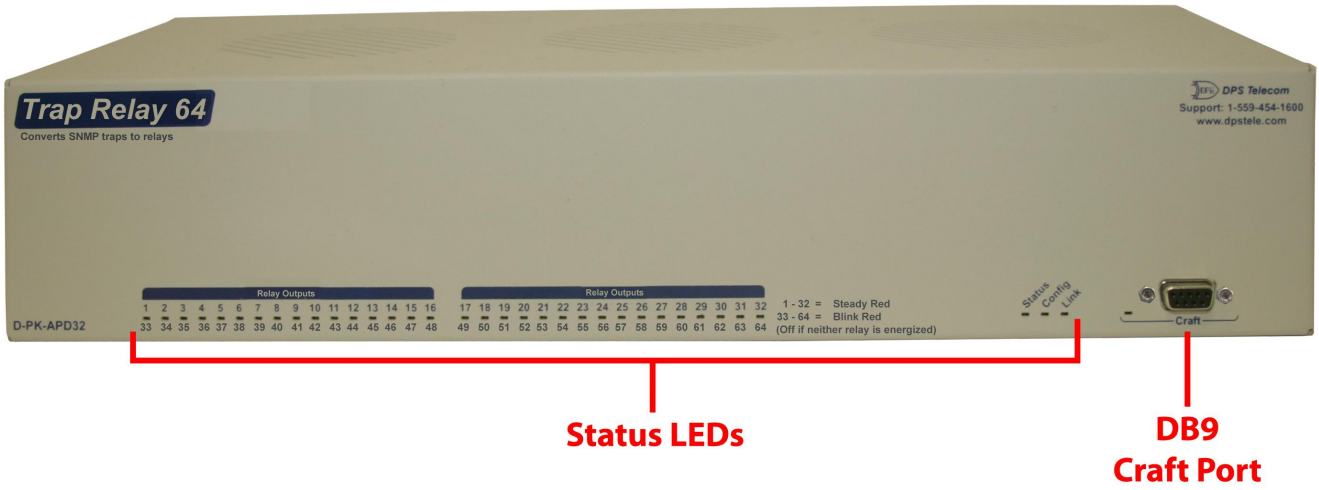


***Fig. 6.1**. Trap Relay 64 front panel*

6.1 DB9 Craft Port

Use the front-panel DB9 RS-232 craft port to connect the Trap Relay 64 to a PC for onsite unit configuration. To connect via the DB9 RS-232 craft port, use a standard DB9M-DB9Fcable.

***Fig 6.2** DB9 RS-232 Pinouts (**Craft Port Only**)*

7 Quick Start: How to Connect to the Trap Relay 64

Most Trap Relay 64 users find it easiest to give the unit an IP address, subnet and gateway through the front serial craft port (TTY interface) to start. Once these settings are saved and you reboot the unit, you can access it over LAN to do the rest of your databasing via the Web Browser interface.

Alternative option: You can skip the TTY interface by using a LAN crossover cable directly from your PC to the Trap Relay 64 and access its Web Browser. See the "...via LAN" section of this chapter.

7.1 ...via DB9 Craft Port (using TTY Interface)

***Fig. 7.1** Trap Relay 64 Craft Port*

The simplest way to connect to the Trap Relay 64 is over a physical cable connection between your PC's COM port and the Trap Relay 64's craft port.

Select the following COM port options:

- Bits per second: **9600**
- Data bits: **8**
- Parity: **None**
- Stop bits: **1**

- Flow control: **None**

When a connection is established (sometimes accompanied by receipt of a hex byte), press Enter to activate the configuration menu. The default password is 'dpstelecom'.

You can perform basic configuration via the craft port — but if you like, you can connect via the craft port just to configure the Trap Relay 64's Private LAN IP address, and then do the rest of your configuration via a LAN connection.

7.2 ...via LAN

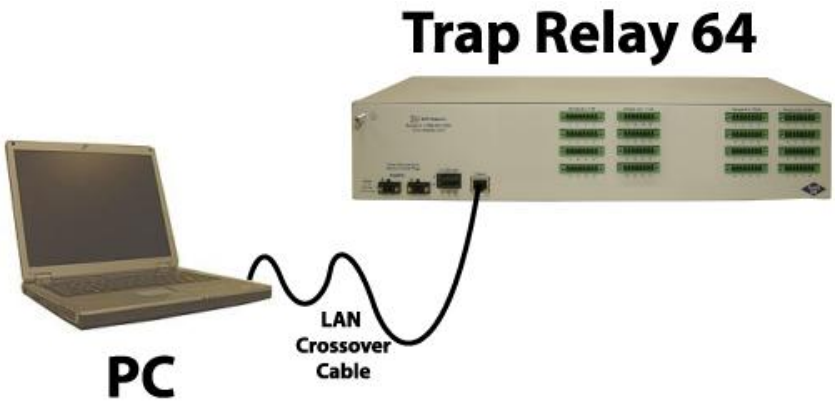


Fig 7.2 *Connection through Ethernet port*

To connect to the Trap Relay 64 via LAN, all you need is the unit's IP address (Default IP address is 192.168.1.100).

If you DON'T have LAN, but DO have physical access to the Trap Relay 64, connect using a LAN crossover cable. **NOTE:** Newer PCs should be able to use a standard straight-through LAN cable and handle the crossover for you. To do this, you will temporarily change your PC's IP address and subnet mask to match the Trap Relay 64's factory default IP settings. Follow these steps:

1. Get a LAN crossover cable and plug it directly into the Trap Relay 64's LAN port.
2. Look up your PC's current IP address and subnet mask, and write this information down.
3. Reset your PC's IP address to **192.168.1.200**. Contact your IT department if you are unsure how to do this.
4. Reset your PC's subnet mask to **255.255.0.0**. You may have to reboot your PC to apply your changes.
5. Once the IP address and subnet mask of your computer coincide with the unit, you can access the Trap Relay 64 via a Telnet session or via Web browser by using the unit's default IP address of **192.168.1.100**.
6. Provision the Trap Relay 64 with the appropriate information, then **change your computer's IP address and subnet mask back to their original settings.**

Now you're ready to do the rest of your configuration via LAN. Plug your Trap Relay 64 into your LAN and see the "Logging On to the Trap Relay 64" section to continue databasing using the Web Browser.

8 TTY Interface

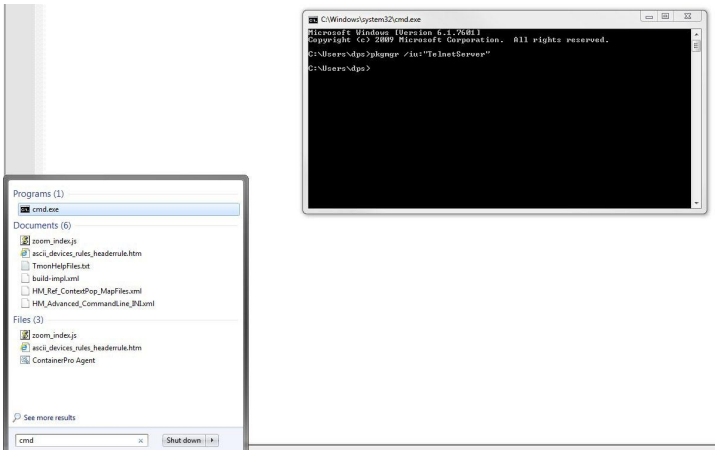
The TTY interface is the Trap Relay 64's built-in interface for basic configuration. From the TTY interface, you can:

- Edit the IPA, subnet, and gateway
- Debug and troubleshoot
- Set unit back to factory defaults
- Ping other devices on the network

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

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

If you're using Windows 7, then you'll need to install telnet before you can use the TTY interface. To install telnet, open up your command line (type "cmd" into the search bar in the **Start Menu**). Select **cmd.exe** to run the command line.

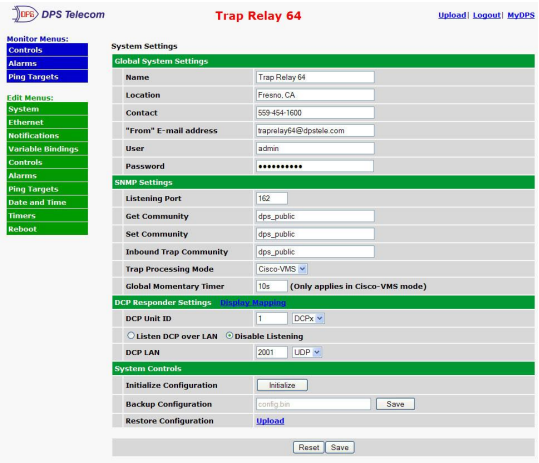


From the command line, type in "pkgmgr /iu:"TelnetServer" then press **enter**. When the command prompt appears again, the installation is complete.

Menu Shortcut Keys

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

9 Trap Relay 64 Web Browser



The Trap Relay 64 features a built-in Web Browser Interface that allows you to 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 using most commonly used browsers.

NOTE: Max # of users allowed to simultaneously access the Trap Relay 64 via the Web is 4.

9.1 Logging on to the Trap Relay 64

For Web Interface functionality, the unit must first be configured with some basic network addresses. If this has not been done yet, refer to the section "Quick Start: How to Connect to the Trap Relay 64" for instructions on initial configuration.

1. To connect to the Trap Relay 64 from your Web browser, enter its IP address in the address bar of your web browser. It may be helpful to bookmark the logon page to avoid entering this each time.

2. After connecting to the unit's IP address, enter your login information and click OK. **NOTE:** The factory default username is "***admin***" and the password is "***dpstelecom***".

Best Practice: DPS Telecom suggests that you change your password before configuring your unit as seen in section 9.1.1 Changing the Default Password.

3. In the left pane, you will see the **Monitor** menu (blue) and **Edit** menu (green) The Monitor menu links are used to view the current status of alarms. The Edit menu is used to change the unit's configuration settings. All the software configuration will occur in the **Edit** menu. The following sections provide detailed information regarding these functions.

Fig. 9.1 *Enter your password to enter the Trap Relay 64 Web Browser Interface*

9.1.1 Changing the Default Password

The password can be configured from the **Edit** > **System** screen. The minimum password length is four characters; however, DPS recommends setting the minimum password length to at least five characters.

Use the following steps to change the logon password:

1. From the **Edit** menu select **System**.
2. Enter the new user name in the **User** field.

3. Enter the new password in the **Password** field.
4. Click the **Save** button.

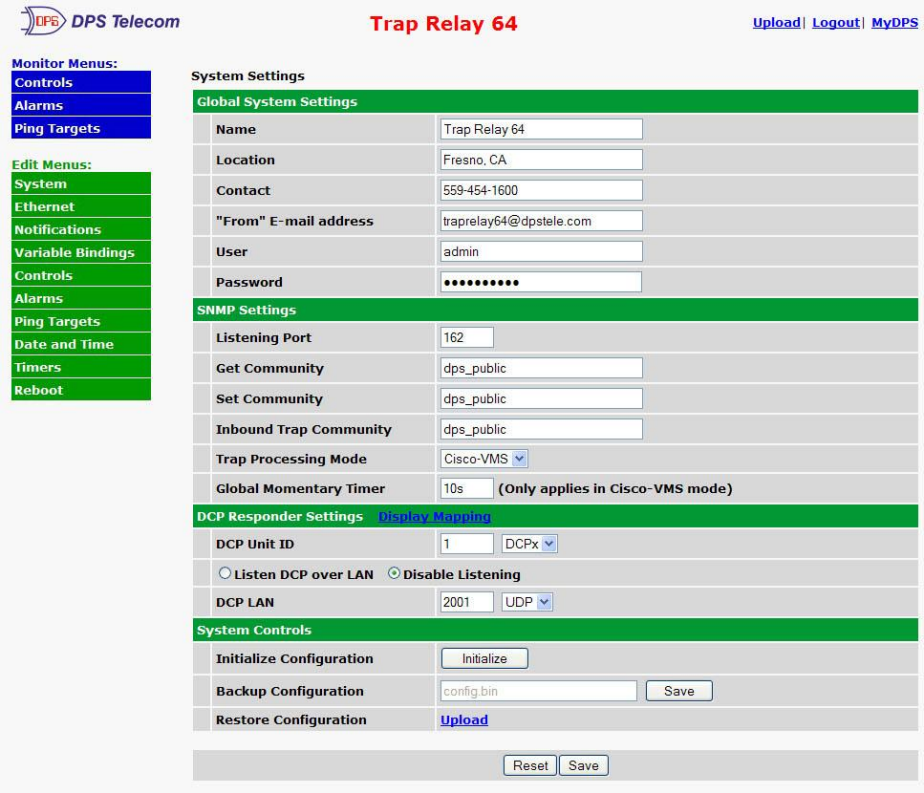


Fig. 9.2 *- Global System Settings section of the Edit > System menu*

NOTE: You will see the following popup when making changes to the Trap Relay 64 from the **Edit** menu. It will appear when confirming your changes to the database, either by clicking **Next** in the setup wizards or the **Save** button.

Fig. 9.3 *- Commit to NVRAM popup*

10 Trap Relay 64 - Quick Turn Up

The next section of this manual will walk you through some of the most common tasks for using the Trap Relay 64. You will learn how to send email notifications to your alarm master- all using the Web browser. For details on entering your settings into each Web browser menu, go to section 11 "Edit Menu Field Descriptions."

10.1 How to Send Email Notifications

1. Click on the **System** button in the **Edit** menu and enter a valid email address in the **"From" Email Address** field. (You may need to check with your IT department to have one created for the unit.) This is the address that will appear in your email as the sender.

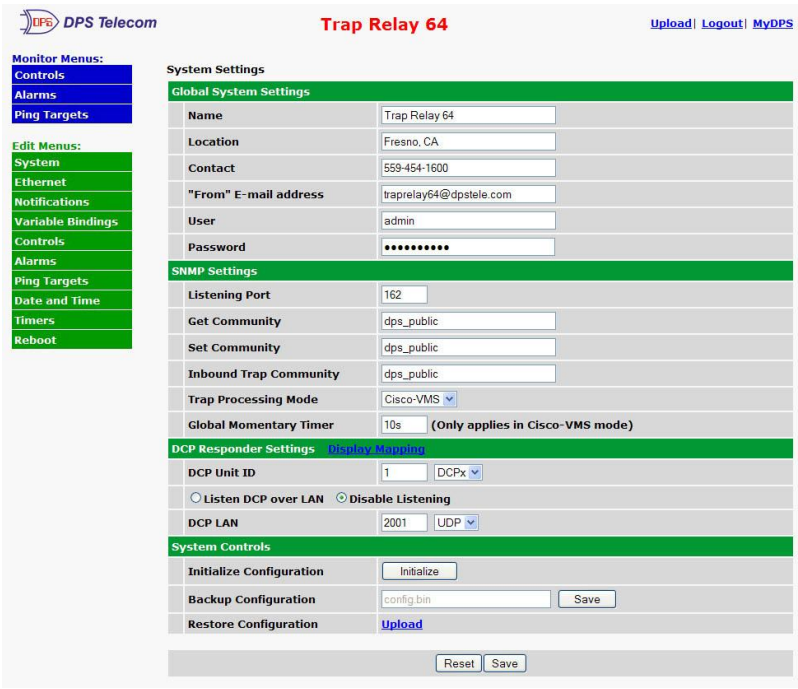


Fig. 10.1

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

Fig. 10.2

3. At the **Notification Setting** screen, use the drop-down menu to choose whether you want notifications for alarms, clears, or both. Now, select the **Send Email** button and click Next.

Fig. 10.3

4. At the **Email Notification** screen, you'll enter your email server settings. Enter the **IP address** or **Host Name** of your email server (If using **Host Name,** DNS servers must be configured under the ethernet settings). Enter the **Port Number** (usually 25) and the **"To" Email Address** of the technician that will receive these emails. The "From" E-mail address is set on the "Edit > System" menu, and cannot be modified from this menu. Click **Next**.

Fig. 10.4

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

Fig. 10.5

6. If you chose to test the email notification you've just setup, you will see a popup. Click **OK** to send a test email notification. Confirm all your settings by checking your email to see if you've received it.

NOTE: This test only means that your notification settings are correct, but you still need to assign the notification to an alarm point. See the next step.

Fig. 10.6

7. Now you will associate this notification to a control You have 8 notification devices available to use. In the image below, you might assign **Notification Device 1** to **Control 1**. This means that you would receive an email notification when "Relay 1" (Control 1) changes state. Remember that Notification #1 in the Notifications menu corresponds to the first "Notifications" column of check boxes. (Notification #2 is the second column, and so on until Notification #8)

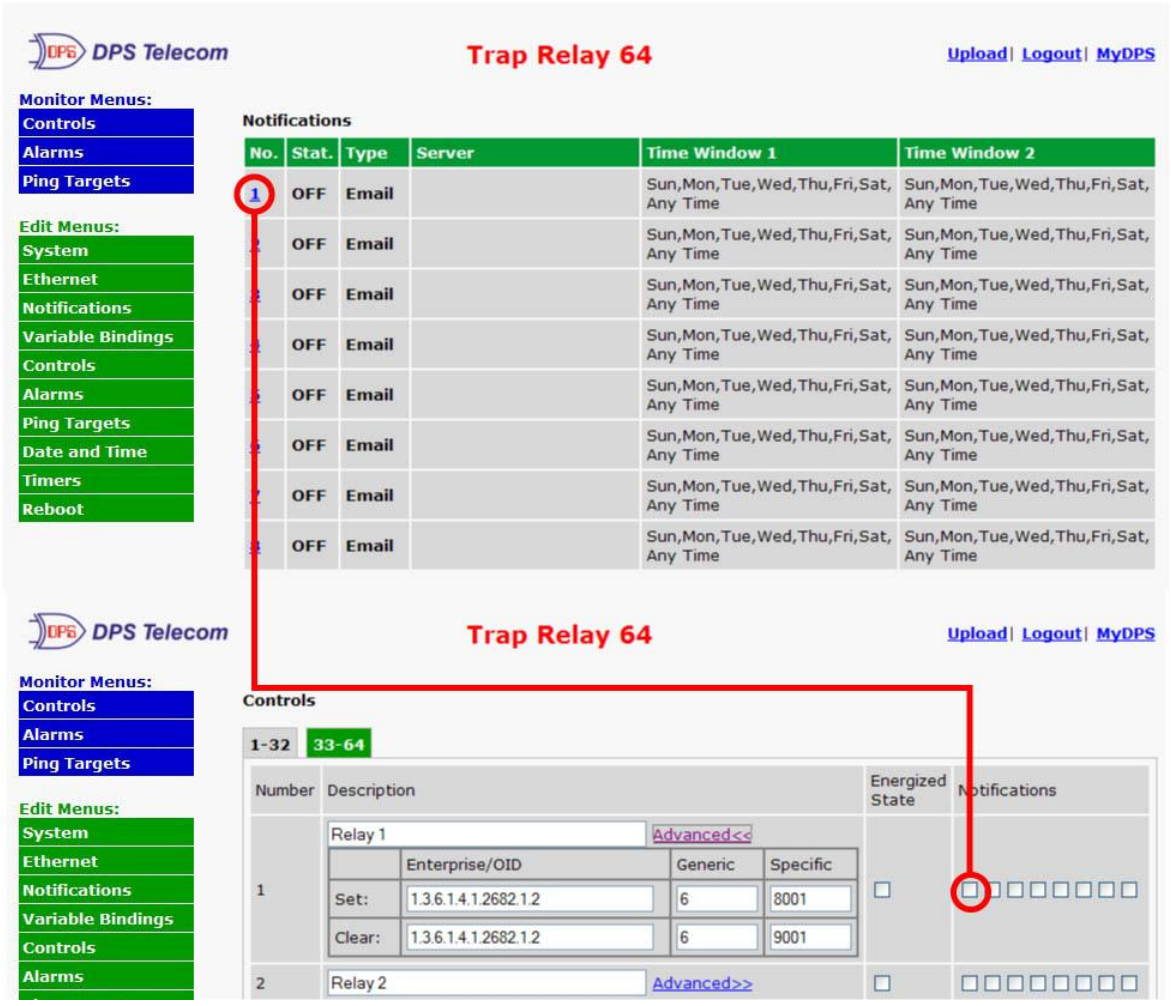


Fig. 10.7 *Associating Controls to the Notifications Table*

11 Edit Menu Field Descriptions

11.1 System

From the **Edit** > **System** menu, you will configure and edit the global system, T/Mon and control settings for the Trap Relay 64.

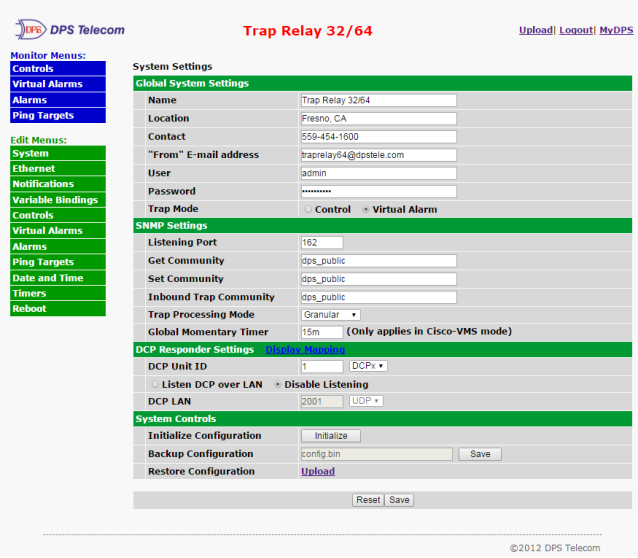


Fig. 11.1 *- The Edit > System menu*

Global System Settings	
Name	A name for this Trap Relay 64. (Optional field)
Location	The location of this Trap Relay 64. (Optional field)
Contact	Contact telephone number for the person responsible for this Trap Relay 64. (Optional field)
"From" Email Address	A valid email address used by the Trap Relay 64 for sending email alarm notifications.
User	Used to change the username for logging into the unit.
Password	Used to change the password for logging into the unit (case-sensitive).
Trap Mode	Control: Traps trigger relays directly.
	Virtual Alarm: Traps trigger virtual alarms. Relays are triggered through derived controls.
SNMP Settings	
Listening Port	Enter the port number which traps must be sent to.
Get Community	Community name for SNMP requests. (case-sensitive).
Set Community	Community name for SNMP SET requests. (case-sensitive).
Inbound Trap Community	Community name for SNMP TRAP requests. (case-sensitive).
Trap Processing Mode	Select one of the supported trap processing modes of operation.
Global Momentary Timer	Enter the amount of time a relay will be operated in the Cisco-VMS mode. **Note:** This will overwrite each individual relays momentary time.
DCP Responder Settings *(For use with T/Mon Master Station)*	
DCP Unit ID	User-definable ID number for this Trap Relay 64 (DCP Address).
Listen DCP	Choose to listen DCP over LAN. May also be disabled.
DCP LAN	Enter the DCP port for this Trap Relay 64 (UDP/TCP port).
System Controls	
Initialize Configuration	Used to restore all factory default settings to the Trap Relay 64. Do not initialize the non-volatile RAM (NVRAM) unless you want to re-enter all of your configuration settings again.
Backup Configuration	⚠ Save the Trap Relay 64's configuration as a .BIN file to your local PC.
Restore Configuration	Click the "Upload" link and select a .BIN configuration file that you saved previously to your local PC. This will restore the saved configuration.

⚠ **Best Practice**: Always make a copy of your Trap Relay 64's configurations

11.2 Ethernet

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

Fig. 11.2 *- The Edit > Ethernet menu*

Ethernet Settings	
MAC Address	Hardware address of the Trap Relay 64. (Not editable - For reference only.)
Host Name	Used only for local web browsing. Example: If you don't want to remember this Trap Relay 64's IP address, you can type in a name is this field, such as Trap Relay 64. Once you save and reboot the unit, you can now browse to it locally by simply typing in "Trap Relay 64" in the address bar. (no "http://" needed).
Enable DHCP	Used to turn on Dynamic Host Connection Protocol. NOT recommended, because the unit is assigned an IP address from your DHCP server. The IP you've already assigned to the unit becomes inactive. Using DHCP means the unit will NOT operate in a T/Mon environment.
Unit IP	IP address of the Trap Relay 64.
Subnet Mask	A road sign to the Trap Relay 64, telling it whether your packets should stay on your local network or be forwarded somewhere else on a wide-area network.
Gateway	An important parameter if you are connected to a wide-area network. It tells the Trap Relay 64 which machine is the gateway out of your local network. Set to 255.255.255.255 if not using. Contact your network administrator for this info.
DNS Server 1	Primary IP address of the domain name server. Set to 255.255.255.255 if not using.
DNS Server 2	Secondary IP address of the domain name server. Set to 255.255.255.255 is not using.

11.3 Notifications

From the initial **Edit** > **Notifications** menu, you may configure any of eight different notifications for your Trap Relay 64's alarms. Click on the number of the notification in the far left column under **No.** to begin configuring notifications.

Fig. 11.3 *- The Edit > Notifications menu*

After clicking on a notification, you will tell the Trap Relay 64 for what sorts of events you'd like to see notifications and what sort of notification to send.

1. In the drop-down box, choose whether you'd like to receive notification for alarms, clears, or both. You may also disable the notification by selecting the appropriate option.
2. Next, choose the sort of notification you would like sent when an event occurs. You may choose:
   - **Send Email** to have an email sent when events occur
   - **Send SNMP** to have a trap sent when events occur
3. Click **Next >** to continue configuring notifications.

Fig. 11.4 *- The Notification Setting menu*

11.3.1 Notification Settings

Email Notification Fields

Fig. 11.5 *- Editing Email Notification Settings*

4a. Enter the appropriate information for email notifications in the fields of the Email Notification screen. Click **Next >** to continue.

Email Notification	
SMTP Server IP or Host Name	The IP address of your email server.
Port Number	The port used by your email server to receive emails, usually set to 25.
"From" E-mail Address	Displays the email address (defined in the Edit menu > System) that the Trap Relay 64 will send email from. Not editable from this screen.
"To" E-mail Address	The email address of the person responsible for this Trap Relay 64, who will receive email alarm notifications.

SNMP Notification Fields

Fig. 11.6 *- Editing SNMP notification settings*

4b. Enter the appropriate information for SNMP Trap notifications in the fields of the SNMP Notification screen. Click **Next >** to continue.

SNMP Notification	
SNMP Trap Server IP	The SNMP trap manager's IP address.
Trap Port No.	The SNMP port (UDP port) set by the SNMP trap manager to receive traps, usually set to 162.
Trap Community	Community name for SNMP TRAP requests.

11.3.2 Schedule

Set a schedule for when you'd like the Trap Relay 64 to send the notification configured in the previous steps. All schedule settings default to full-time notification, 24 hours a day, 7 days a week.

Fig. 11.7 *- The Schedule creation screen*

Notification Scheduling	
Days of the week	From either Schedule 1 or 2, check which days you want to receive notifications.
Any Time	Select to tell the Trap Relay 64 you want to receive alarm notifications at any time for the day(s) you've selected.
Notification Time	Instead of "Any Time", use these fields to only send alarm notifications during certain hours on the day(s) you've selected.

When finished, click **Test** to test the notification or **Finish** to save the notification.

11.4 System Alarms

Fig. 11.8 *- The Edit > System Alarms menu*

Choose the "System" tab on the "Edit > Alarms" menu to via the system alarms. These are "software" alarms that are internally generated by the Trap Relay 64 to report various events and problems (ex. "Unit has reset" or "NTP server connection has failed").

Editing System Alarms	
(first column)	Alarm point number
Description	Non-editable description for this System (housekeeping) Alarm.
Rpt (Report)	Check this box to choose to report this alarm.Check the box in the green bar (top) to have all System Alarms reported. Leave unchecked to ignore.
Notification devices	Check which notification device(s), 1 through 8, you want to send alarm notifications for that alarm point. Check the box in the green bar (top) to have that notification device send a notification for all the System Alarms.

11.5 Variable Bindings

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

Fig. 11.9 *- The Edit > Variable Bindings menu*

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

11.6 Controls

A Trap Relay 64 relay can be configured in the **Edit** > **Controls** menu. You can enter your own description for this relay and designate it to a notification device(s). This section is only relevant when Trap Mode is configured to Control. When Trap Mode is configured to Virtual Alarm, refer to section **11.6.2 Derived Controls**.

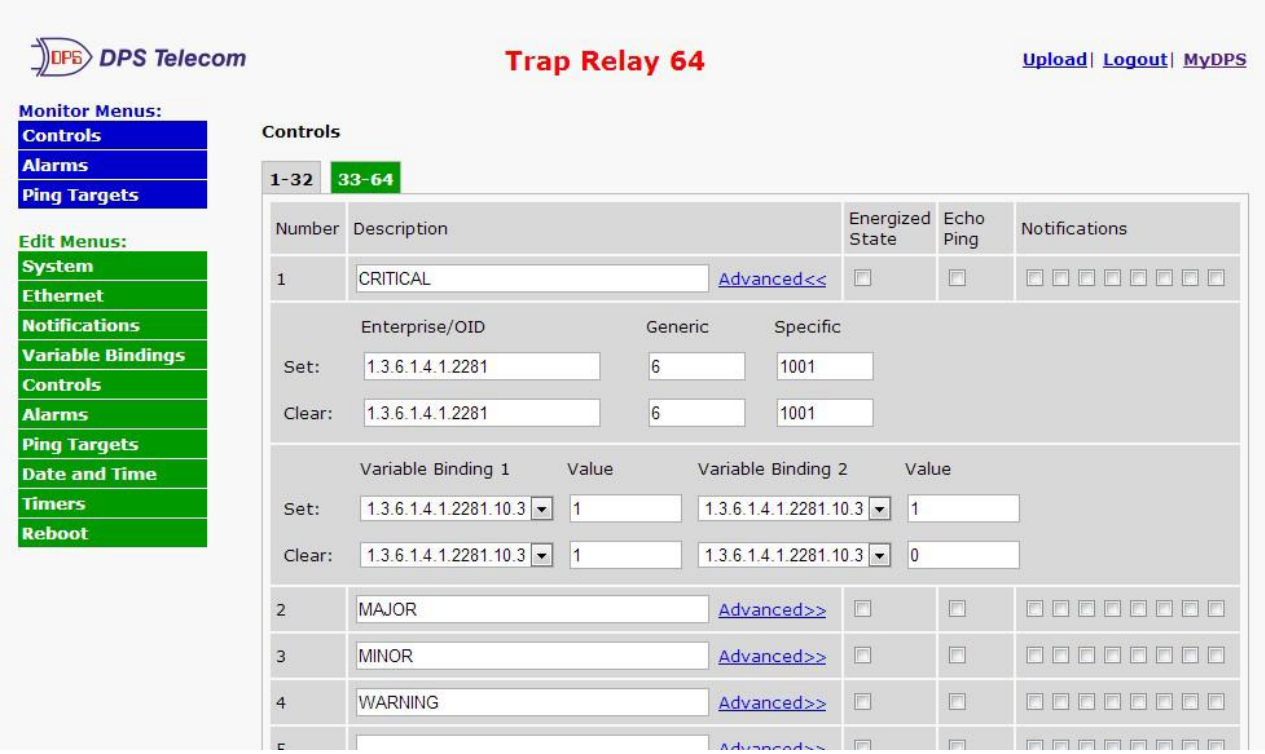


Fig. 11.10 *- The Edit > Controls menu*

Editing Control Relays	
Description	User-definable description for the Trap Relay 64's control.
Notifications	Check which notification device(s), 1 through 8, you want to send alarm notifications for the control.
Energized State	When the box in the Energize State column is not checked, the relay's normal electrical state is **De-energized**. Checking this box will set the relay's normal electrical state to **Energized**.
Echo Ping	Associates the control relay with the ping target of the same ID/Number. When a ping fails, the relay will latch. If the ping is successful, the relay will release. **Note**: Enabling Echo Ping will prevent the relay from being triggered by trap OIDs.
Momentary Time	The amount of time the relay is latched when "MOM" is clicked in the monitor interface.
Advanced	
Set	Enter the Enterprise/OID, Generic Type and Specific Type to operate a relay.
Clear	Enter the Enterprise/OID, Generic Type and Specific Type to release a relay.
Variable Binding	If defined, additional OID (from equipment connected to control relay) to uniquely identify the SNMP trap. **Note**: Variable Bindings set to 'None" will be ignored; trap must math all variable bindings to trigger an action.
Value	Value of the variable binding. Must be integer or string (when searching for a specific string, the string must be contained within the received trap variable binding value). **Note**: Using a ***** in this field is like a "wild card" - any value is accepted. **Note**: Variable Bindings 3 and 4 can only be integers 0 - 65535.
Chain to Next	Make the control part of a chain allowing up to 15 variable bindings. A chain is defined as a group of consecutive controls with this box checked, plus the control immediately following. Enabling this feature for controls 1,2,4,7 would make 3 chains: 1-3, 4-5, 7-8.

	Chains can be up to four controls long and have the following effect: When a trap comes is, the trap is evaluated against the chain as a whole. The trap is evaluated against the Enterprise, OID, Generic, and Specific of the first link in the chain and the variable bindings for every link in the chain. If the trap matches, the last control in the chain is latched or released. **Note**: in a chain of 4, the Variable Binding #4 of link #4 is ignored.

Note: The **Advanced** tab will only appear only when "Granular" Trap Processing Mode is selected in the **Edit > System** menu.
Note: If the **Description** is configured in the following manner: IP_xxx.xxx.xxx.xxx (where "xxx.xxx.xxx.xxx" is the desired IP address), the relay will only respond to traps received from the configured IP in the description.

11.6.1 Configuring Granular and Cisco-VMS OIDs

The Trap 64 has 2 modes for processing incoming SNMP traps:

1. Granular Mode (for any SNMP device):
Each Relay will operate or release based on the trap information of an SNMPv1 trap or the OID of an SNMPv2c trap. Granular Mode can be used with any SNMP device. Other modes are only used with specific SNMP device types to provide specialized functionality.

2. Cisco-VMS Mode:
This is a specialized mode designed only to be used with Cisco-VMS devices. The Trap Relay 64 will ignore each Relay's SNMP trap configuration and will momentarily operate relays when it receives a VMS 6.3 SNMP Trap. A Relay in Cisco-VMS mode will operate if its description matches the trap's mediaStreamName value.

Granular Mode

SNMP v1

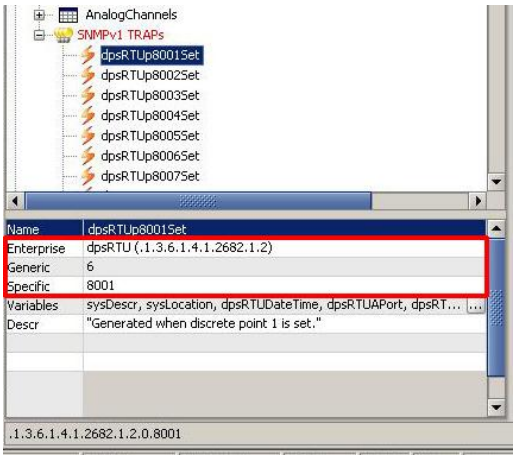


Fig. 11.11 *- Location of the OID, Generic Type and Specific Type information for SNMP v1*

In your MIB Browser (freeware MIB Browser software available for free trial) navigate to the SNMPv1 TRAPs to obtain the Enterprise, Generic Type and Specific Type as seen in the image above. This information is needed for the **Set** and **Clear** properties in the **Advanced** tab.

SNMP v2c

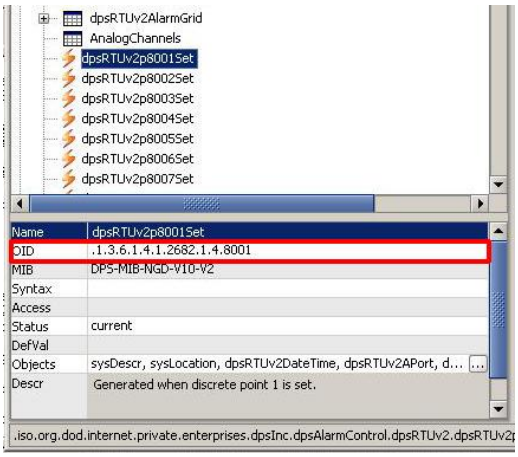


Fig. 11.12 *- Location of the OID information for SNMP v2c*

When using a SNMP v2c TRAP, you only need to configure the TRAP OID. The location of the OID in your MIB Browser can be seen in the image above.

In the image below **Control 1** "Relay 1" is configured using a SNMP v1 trap's Enterprise, Generic Type and Specific Type.

Fig. 11.13

NOTE: To use the IP filter feature for the Granular Mode, type "_IP: " in the description field followed by the IP of the source SNMP trap (example: 192.168.1.1) and only traps from the specified IP address will be processed.

Energized State

The 'Energized State' checkbox for each Relay may be used to "reverse the polarity" of that relay.

When the 'Energized State' checkbox IS NOT checked, the relay will be "normally open." On startup, the relay will be in a released state. When the specified "Set" SNMP trap is received, the relay will latch. When the specified "Clear" SNMP trap is received, the relay will release. This is the commonly used configuration for 'Energized State.'

When the 'Energized State' checkbox IS checked, the relay will be "normally closed." On startup, the relay will be in a latched state. When the specified "Set" SNMP trap is received, the relay will release. When the specified "Clear" SNMP trap is received, the relay will latch. This is not a common configuration, but it can be very useful in certain situations.

Energized State has no effect on Notification Devices. If you configure a Notification Device to trigger on "Set" events and associate it with a Relay, it will always trigger when the specified "Set" SNMP trap is received. The opposite is true for "Clear" Notification Devices when "Clear" SNMP traps are received. Even if you've reversed the latch/release operation of a Relay using Energized State, associated Notification Devices respond to "Set" and "Clear" SNMP traps in the same way. Of course, this distinction is irrelevant for Notification Devices configured to trigger on "Both" event types, which trigger on both "Set" and "Clear".

Cisco-VMS Mode

In Cisco-VMS mode, the unit will only process the trap OID's and object OID's in the table below. A relay in Cisco-VMS mode will only operate if the VMS trap's mediaStreamName value matches the relay's description (case sensitive). The relay will stay active for the time specified in the Global Momentary Timer setting.

Cisco-VMS Mode	
Trap	**OID**
mediaStreamDeviceUnreachable	1.3.6.1.4.1.28196.2.0.2
mediaStreamDeviceConnectionLoss	1.3.6.1.4.1.28196.2.0.3
mediaStreamConfigFailure	1.3.6.1.4.1.28196.2.0.5
Object	**OID**
mediaStreamName	1.3.6.1.4.1.28196.2.1.1

11.6.2 Derived Controls

1. When Trap Mode is set to Virtual Alarms, traps trigger virtual alarms instead of relays and derived controls are enabled. To setup a derived control, enter a formula in the description and click "Parse" to verify the formula is valid. Invalid formulas will always leave the relay released.

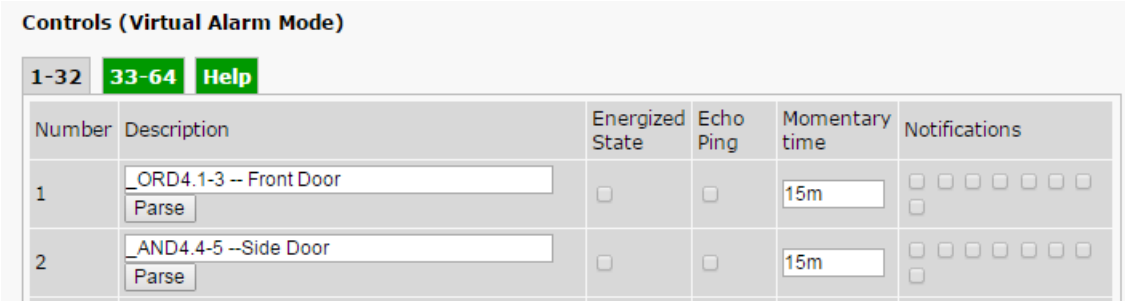


Fig. 11.14 *With Virtual Alarms Enabled.*

2. Add the operator "--" to add a comment after the formula. Anything after the operator is ignored by the parser (Example: _OR D4.1-3 -- Front Door)

Derived controls 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.
-- Add a comment that will be ignored by parser.

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.

_OR D1.3-5 is logically equivalent to (1.3 || 1.4 || 1.5)

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

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

_AN D1.3-5D2.6_OR.7D3.10.12 is logically equivalent to ((1.3 && 1.4 && 1.5 && 2.6) || 2.7 || 3.10 || 3.12))

_OR D4.1-3 -- Front Door is logically equivalent to (4.1 || 4.2 || 4.3)

11.7 Ping Targets

Configuration for the 64 ping targets can be done from the **Edit** > **Ping Targets** window.

Fig. 11.15 *The Edit > Ping Targets interface*

Editing Ping Targets	
ID	Point number.
Description	User-definable description for the ping target.
IP Address	IP address of the device (the ping target).
Notifications	Check which notification device(s), 1 through 8, you want to send alarm notifications for that ping target.

11.8 Date and Time

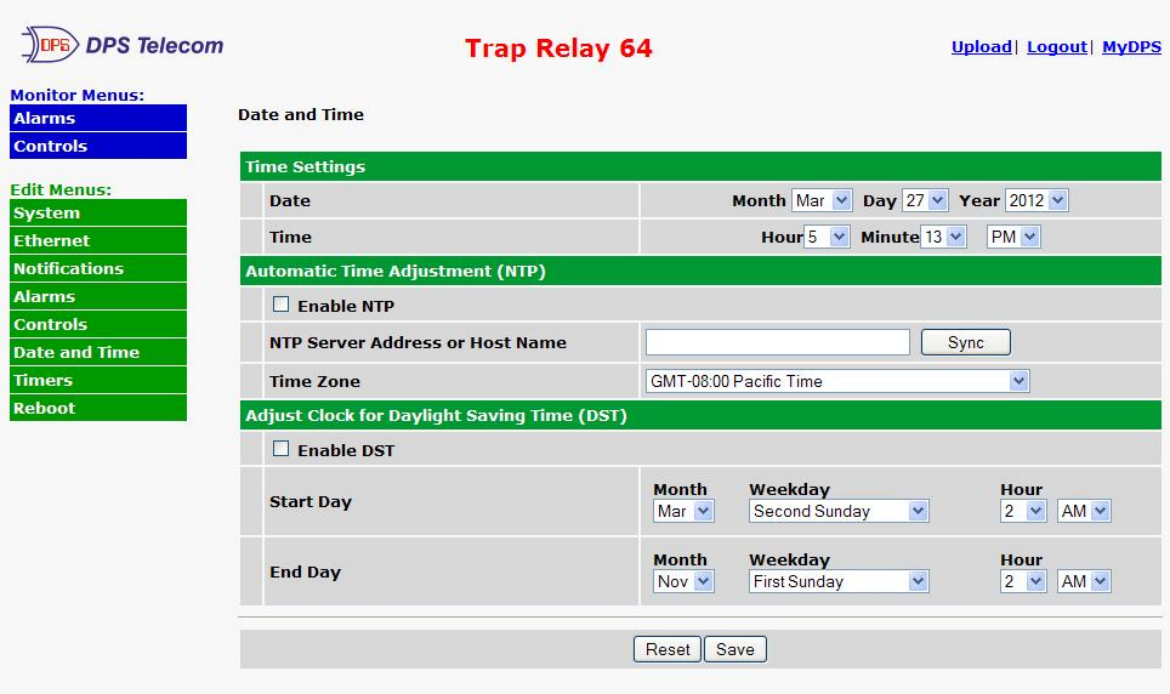


Fig. 11.16 *- The Edit > Date and Time menu*

Time Settings	
Date	Select the current month, day, and year from the drop-down menus.
Time	Select the current hour, minutes, and time of day fro the drop-down menus.
Automatic Time Adjustment (NTP)	
Enable NTP	Check this box to enable Network Time Protocol.
NTP Server Address or Host Name	Enter the NTP server's IP address or host name, then click Sync. Example: north-america.pool.ntp.org
Time Zone	Select your time zone from the drop-down menu.
Adjust Clock for Daylight Savings Time (DST)	
Enable DST	Check this box to have the Trap Relay 64 observe Daylight Savings.
Start Day	Select the month, weekday, and time when Daylight Savings will begin.
End Day	Select the month, weekday, and time when Daylight Savings will end.

11.9 Timers

The Timers Menu allows configuration of various intervals, such as delays between pings, audible alarm tone length, and web refresh delay. Each timer is fully explained within the Timers Menu, as shown below:

***Fig. 11.17**- The Edit > Timers menu*

11.10 Reboot

Click on the **Reboot** link from the **Edit** menu will reboot the Trap Relay 64 after writing all changes to NVRAM.

***Fig. 11.18**- The Edit > Reboot confirmation popup*

12 Monitoring via the Web Browser

12.1 Monitoring System Alarms

System alarms are non-editable, housekeeping alarms that are programmed into Trap Relay 64. The "System" tab of the **Monitor** > **Alarms** screen provides the status of the system alarms by indicating if an alarm has been triggered. Under the **State** column, the status will appear in red if an alarm has been activated, or green if it has not been activated. The status will be displayed in green when the alarm condition is not present.

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

Fig 12.1 *View the status of System Alarms from the Monitor > Alarms menu.*

12.2 Monitoring Virtual Alarms

Virtual Alarms are enabled by setting "Trap Mode" to "Virtual Alarms" in the system provisioning page. When enabled, traps trigger Virtual Alarms instead of relays. Virtual Alarms have no physical effect, they are used to trigger derived controls.

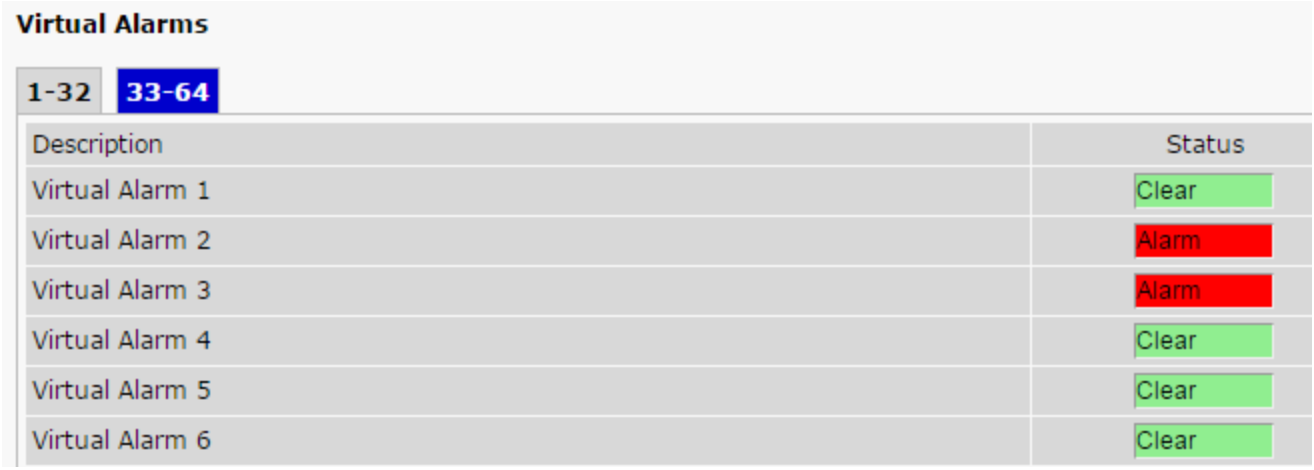


Fig 12.2 *View the status of Virtual Alarms from the Monitor > Virtual Alarms.*

12.2.1 Editing Virtual Alarms

Virtual Alarms are enabled by setting "Trap Mode" to "Virtual Alarms" in the system provisioning page. When enabled, traps trigger Virtual Alarms instead of relays. Virtual Alarms have no physical effect, they are used to trigger derived controls.

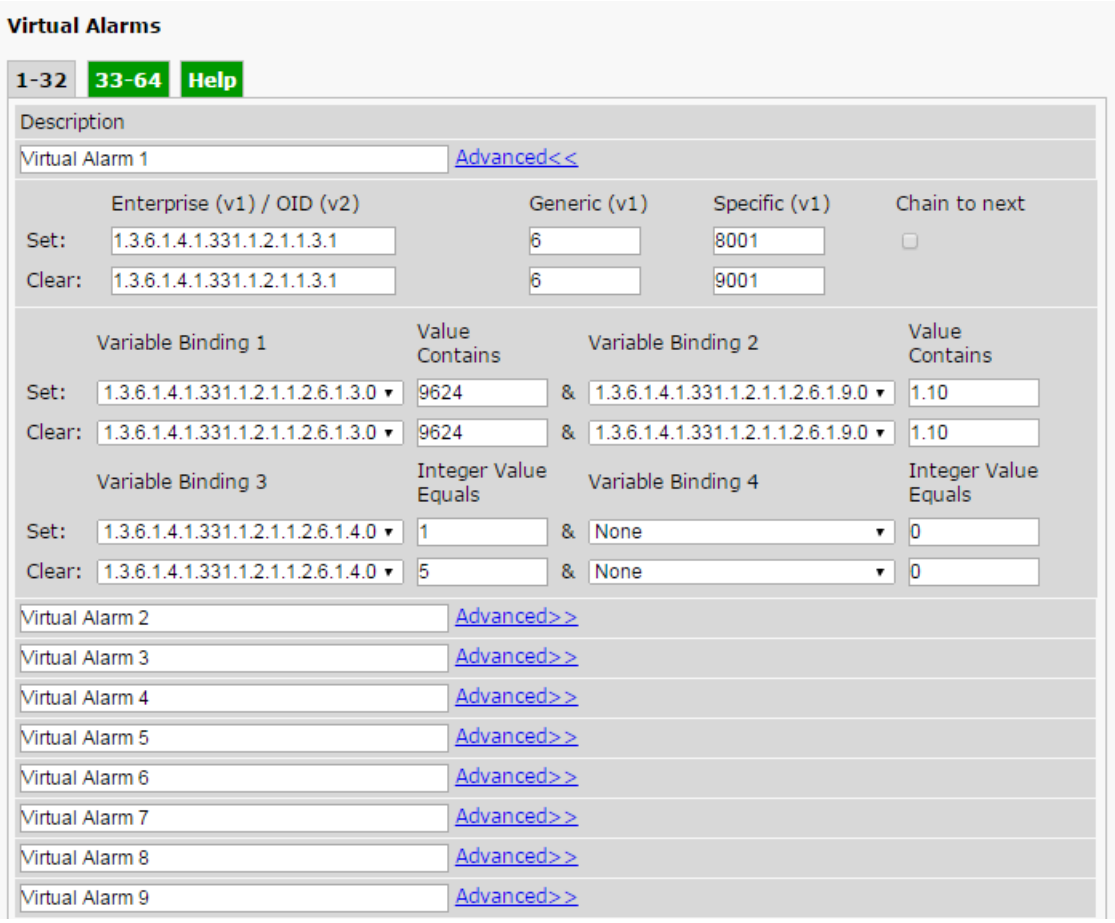


Fig 12.3 *- The Edit > Virtual Alarms menu*

Editing Virtual Alarms	
Set	Enter the Enterprise/OID, Generic Type and Specific Type to operate a relay.
Clear	Enter the Enterprise/OID, Generic Type and Specific Type to release a relay.
Variable Binding	If defined, additional OID to uniquely identify the SNMP trap. **Note**: Variable Bindings set to 'None" will be ignored; trap must math all variable bindings to trigger an action.
Value	Value of the variable binding. Must be integer or string (when searching for a specific string, the string must be contained within the received trap variable binding value). **Note**: Using a ***** in this field is like a "wild card" - any value is accepted. **Note**: Variable Bindings 3 and 4 can only be integers 0 - 65535.
Chain to Next	Make the virtual alarm of a chain allowing up to 15 variable bindings. A chain is defined as a group of consecutive virtual alarms with this box checked, plus the virtual alarm immediately following. Enabling this feature for virtual alarms 1,2,4,7 would make 3 chains: 1-3, 4-5, 7-8. Chains can be up to four virtual alarms long and have the following effect: When a trap comes is, the trap is evaluated against the chain as a whole. The trap is evaluated against the Enterprise, OID, Generic, and Specific of the first link in the chain and the variable bindings for every link in the chain. If the trap matches, the last virtual alarm in the chain is latched or released. **Note**: in a chain of 4, the Variable Binding #4 of link #4 is ignored.

12.3 Controls

Use the following rules to operate the Trap Relay 64's control:

1. Select **Controls** from the **Monitor** menu.
2. Under the **State** field, you can see the current condition of the control.

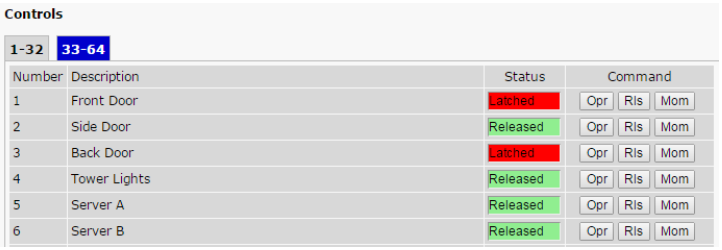


Fig 12.4 *View the state of the control relays in the Monitor > Controls menu*

In the "Command" field "Opr" will latch the relay, "Rls" will release the relay, and "Mom" will latch the relay for the time configured in the provisioning page.

12.4 Ping Targets

The Trap Relay 64 can support up to 64 ping targets. You can view each the configured ping targets by browsing to the **Monitor** > **Ping Targets** window.

Fig 12.5 *The Monitor > Ping Targets interface*

13 Firmware Upgrade

Before upgrading the firmware, DPS Telecom suggests that you go to **System Settings >> Backup Configuration** and save your configuration settings. To access the **Firmware Load** screen, click on the upload link at the top right of the browser.

To be notified every time a new firmware is released for your device, login to your My DPS account and navigate to the **Notifications** page. At this page check the box that corresponds to the device that you want firmware notifications for.

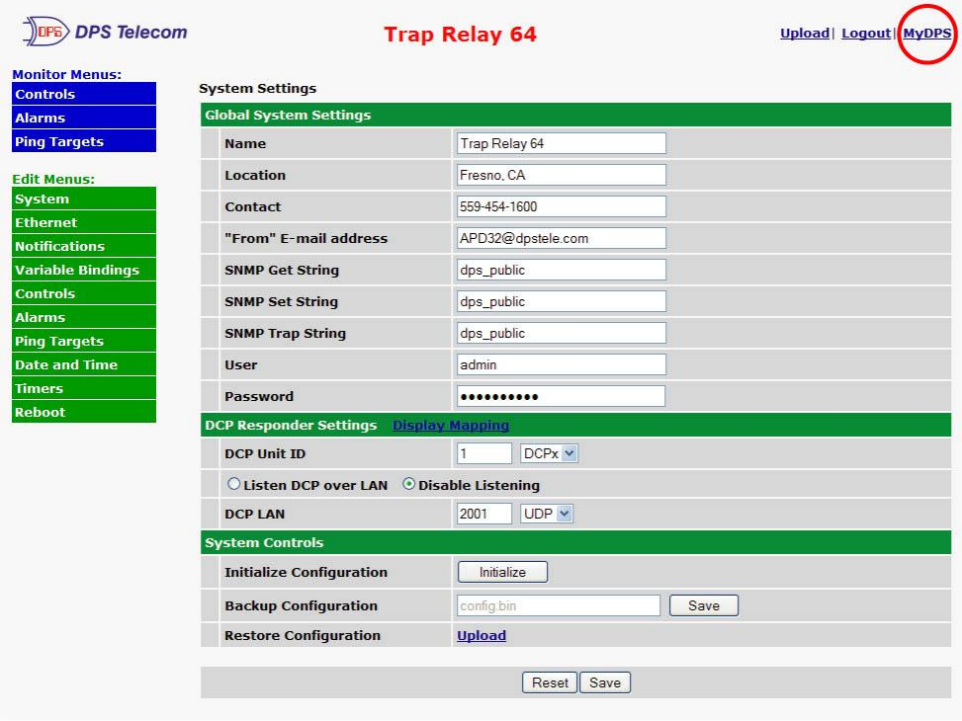


Fig. 13.1 *The clickable link to upgrade firmware from the Edit > System menu*

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

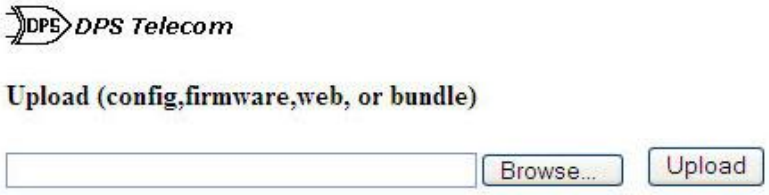


Fig. 13.2 *Browse for downloaded firmware upgrade*

14 Reference Section

14.1 Front and Back Panel LEDs

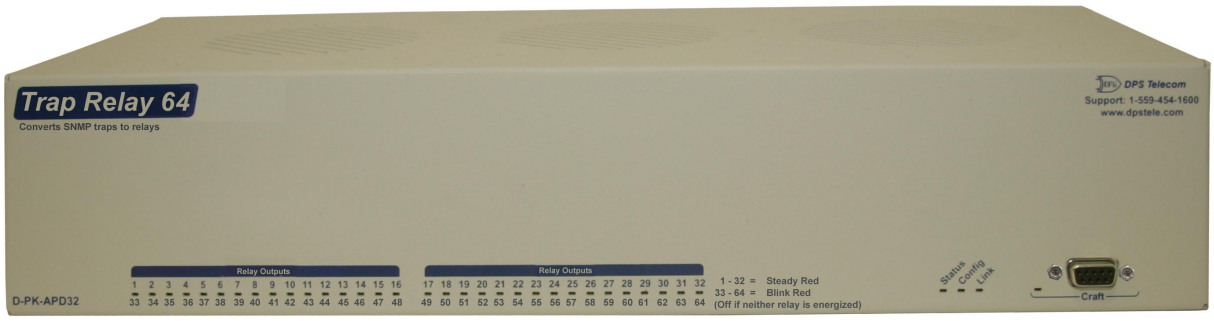


Fig. 14.1 *Front panel LEDs*

LED	Status	Description
Config	Solid Red	The unit has been configured and needs to be rebooted
Status	Flashing Green	Trap Relay 64 application running
	Flashing Red	Boot Loader is running
Link	Solid Green	LAN connected
	Solid Red	LAN not detected
Relay Outputs	Solid Red	Relay is active on relay labeled 1-32
	Flashing Red	Relay is active on relay labeled 33-64
	Alternating Solid Red and Flashing Red	Relays are active on points labeled 1/33, 2/34 etc.
Craft	Flashing Green	Trap Relay 64 data transmitted over craft port
	Flashing Red	Trap Relay 64 data received over craft port

Table 14.1 *Front Panel LED Descriptions*

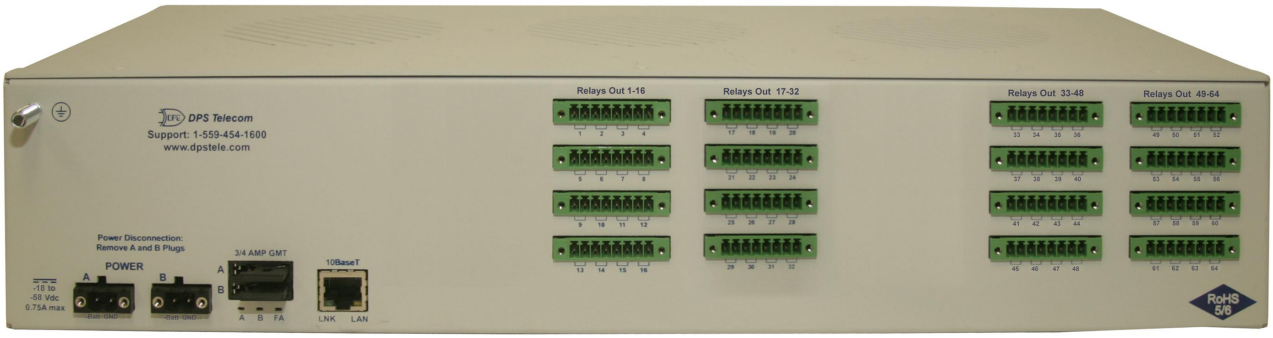


Fig. 14.2 *Back panel LEDs*

LED	Status	Description
A	Solid Green	Power supply A OK
	Off	No voltage, low voltage or incorrect polarity on Power supply A
B	Solid Green	Power supply B OK
	Off	No voltage, low voltage or incorrect polarity on Power supply B
FA	Solid Red	Blown Fuse
LNK	Solid Green	LAN connected
LAN	Flashing Yellow	LAN Activity

Table 14.2 *Back Panel LED Descriptions*

14.2 Display Mapping

	Description	Port	Address	Point
Display 1	Default configuration	99	1	33
	MAC address not set	99	1	35
	IP address not set	99	1	36
	LAN hardw are error	99	1	37
	SNMP processing error	99	1	38
	SNMP community error	99	1	39
	LAN TX packet drop	99	1	40
	Notification 1 failed	99	1	41
	Notification 2 failed	99	1	42
	Notification 3 failed	99	1	43
	Notification 4 failed	99	1	44
	Notification 5 failed	99	1	45
	Notification 6 failed	99	1	46
	Notification 7 failed	99	1	47
	Notification 8 failed	99	1	48
	NTP failed	99	1	49
	Timed Tick	99	1	50
	Dynamic memory full	99	1	52
	Unit Reset	99	1	53
Display 2	Controls 1 - 64	99	1	1-64
Display 3	Ping Targets 1 - 64	99	1	1-64
Display 4	Virtual Alarms 1 - 64	99	1	1-64

Table 14.3 *Display Mapping*

14.3 SNMP Manager Functions

The SNMP Manager allows the user to view alarm status, set date/time, issue controls, and perform a resync. The display and tables below outline the MIB object identifiers. Table 14.4 begins with dpsRTU; however, the MIB object identifier tree has several levels above it. The full English name is as follows: root.iso.org.dod.internet.private.enterprises.dps-Inc.dpsAlarmControl.dpsRTU. Therefore, dpsRTU's full object identifier is 1.3.6.1.4.1.2682.1.2. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the Control Grid is 1.3.6.1.4.1.2682.1.2.3.3 because the object identifier of dpsRTU is 1.3.6.1.4.1.2682.1.2 + the Control Grid (.3) + the Display (.3).

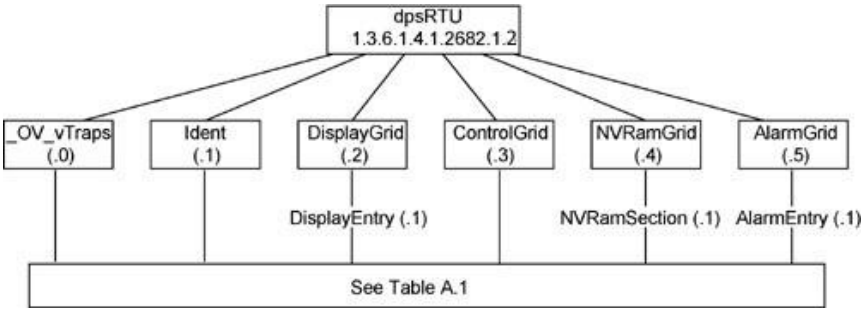


Table 14.4

Tbl. B1 (O.)_OV_Traps points	Tbl. B2 (.1) Identity points	Tbl. B3 (.2) DisplayGrid points
_OV_vTraps (1.3.6.1.4.1.2682.1.2.0)	**Ident (1.3.6.1.4.1.2682.1.2.1)**	**DisplayEntry (1.3.6.1.4.1.2682.1.2.2.1)**
PointSet (.20)	Manufacturer (.1)	Port (.1)
PointClr (.21)	Model (.2)	Address (.2)
SumPSet (.101)	Firmware Version (.3)	Display (.3)
SumPClr (.102)	DateTime (.4)	DispDesc (.4)*

ComFailed (.103)
ComRestored (.014)
P0001Set (.10001) through P0064Set (.10064)
P0001Clr (.20001) through P0064Clr (.20064)

ResyncReq (.5)*
* Must be set to "1" to perform the resync request which will resend TRAPs for any standing alarm.

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 (1.3.6.1.4.1.2682.1.21.5.1)
Aport (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)
APntDesc (.5)*
AState (.6)
* For specific alarm points, see Table B6

Table 14.5

MIB files are available on the Resource CD or upon request.

14.4 SNMP Granular Trap Packets

Tables 14.5 and 14.6 provide a list of the information contained in the SNMP Trap packets sent by the Trap Relay 64

SNMP Trap managers can use one of two methods to get alarm information:

1. Granular traps (not necessary to define point descriptions for the Trap Relay 64) **OR**
2. The SNMP manager reads the description from the Trap.

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

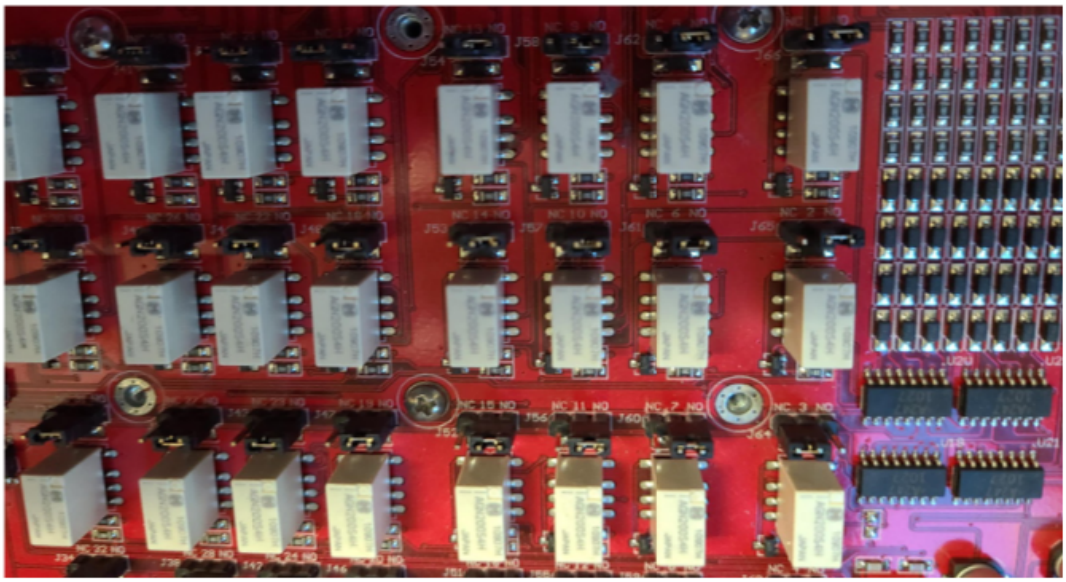
Table 14.6 *UDP Headers and descriptions*

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 v1.0K	Value
1.3.6.1.2.1.1.6.0	Object
1-800-622-3314	Value
1.3.6.1.4.1.2682.1.2.4.1.0	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
1.3.6.1.4.1.2682.1.2.5.1.2.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.3.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.4.99.1.1.1	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

Table 14.7 *SNMP Headers and descriptions*

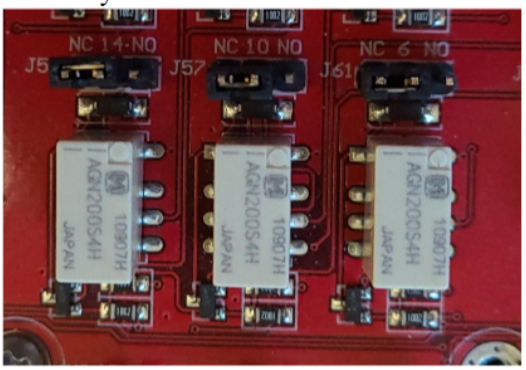
14.5 Shunting for Normally Open/Closed Relays

You can modify the behavior of your relays to act as normally opened or normally closed by switching the position of the current shunts located next to each relay within the unit. There are three pins located in front of each relay with the labels of: NO (normally open), the relay number, and NC (normally closed). The shunts by default are connecting the unit number pins to the normally open pins. These relays will not have continuity unless energized in firmware. This is recommended configuration for the relays, as the relays' statuses will match their status in the web interface.

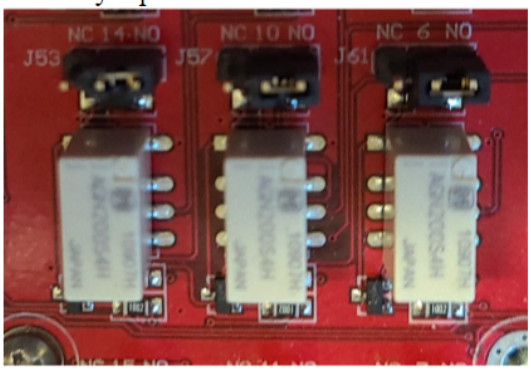


If the shunts are switched over by opening the unit and manually repositioning the shunts to be connecting the unit number and normally closed pins, the relays will be closed by default. The relay will maintain continuity unless energized in firmware. This configuration is only recommended for those who need their relays to maintain continuity even in the event of a power failure.

Normally Closed



Normally Open



15 Frequently Asked Questions

Here are answers to some common questions from Trap Relay 64 users. The latest FAQs can be found on the Trap Relay 64 support web page, **http://www.dpstele.com.**

If you have a question about the Trap Relay 64, please call us at **(559) 454-1600** or e-mail us at **support@dpstele.com**

15.1 General FAQs

Q. How do I telnet to the Trap Relay 64?

A. You must use **Port 2002** to connect to the Trap Relay 64. 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 Trap Relay 64 and Port 2002. For example, to connect to the Trap Relay 64 using the standard Windows Telnet client, click Start, click Run, and type "telnet <Trap Relay 64 IP address> 2002."

Q. How do I connect my Trap Relay 64 to the LAN?

A. To connect your Trap Relay 64 to your LAN, you need to configure the unit IP address, the subnet mask and the default gateway. A sample configuration could look like this:
Unit Address: 192.168.1.100
subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1
Save your changes by writing to NVRAM and reboot. Any change to the unit's IP configuration requires a reboot.

Q. When I connect to the Trap Relay 64 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 Trap Relay 64.

Q. The LAN link LED is green on my Trap Relay 64, 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. I'm unsure if the voltage of my power supply is within the specified range. How do I test the voltage?

A. Connect the black common lead of a voltmeter to the ground terminal of the battery. Connect the red lead of the voltmeter to the batter's VCD terminal. The voltmeter should read between -36 and -72VDC for -48VDC build.

15.2 SNMP FAQs

Q. Which version of SNMP is supported by the SNMP agent on the Trap Relay 64?
A. SNMP v1 and SNMPv2c.

Q. How do I configure the Trap Relay 64 to send traps to an SNMP manager? Is there a separate MIB for the Trap Relay 64? 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 Trap Relay 64 begins sending traps as soon as the SNMP managers are defined. The Trap Relay 64 MIB is included on the Trap Relay 64 Resource CD. The MIB should be compiled on your SNMP manager. (**Note:** MIB versions may change in the future.) The unit supports 2 SNMP managers, which are configured by entering its IP address in the Trap Address field of Ethernet Port Setup. To configure the community strings, choose SNMP from the Edit menu, and enter appropriate values in the Get, Set, and Trap fields.

Q. Does the Trap Relay 64 support MIB-2 and/or any other standard MIBs?
A. The Trap Relay 64 supports the bulk of MIB-2.

Q. Does the Trap Relay 64 SNMP agent support both Trap Relay 64 and T/MonXM variables?
A. The Trap Relay 64 SNMP agent manages an embedded MIB that supports only the Trap Relay 64's RTU variables. The T/MonXM variables are included in the distributed MIB only to provide SNMP managers with a single MIB for all DPS Telecom products.

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

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

Q. The Trap Relay 64 manual talks about control relay outputs. How do I control these from my SNMP manager?
A. The control relays are operated by issuing the appropriate set commands, which are contained in the DPS Telecom MIB.

Q. How can I associate descriptive information with a point for the RTU granular traps?
A. The Trap Relay 64 control point descriptions are individually defined using the Web Browser.

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

1. Make sure that the Trap Address (IP address of the SNMP manager) is defined. (If you changed the Trap Address, make sure you saved the change to NVRAM and rebooted.)
2. Make sure all alarm points are configured to send SNMP traps.
3. Make sure the Trap Relay 64 and the SNMP manager are both on the network. Use the unit's ping command to ping the SNMP manager.

16 Technical Support

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

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

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

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

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

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

17 End User License Agreement

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

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

DPS Telecom's warranty and limitation on its liability for the Software is as described in the warranty information provided to End User in the Product Manual.

End User shall indemnify DPS Telecom and hold it harmless for and against any and all claims, damages, losses, costs, expenses, obligations, liabilities, fees and costs and all amounts paid in settlement of any claim, action or suit which may be asserted against DPS Telecom which arise out of or are related to the non-fulfillment of any covenant or obligation of End User in connection with this Agreement.

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

Warranty

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

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

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

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

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

Technical Support

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

Free Tech Support is Only a Click Away

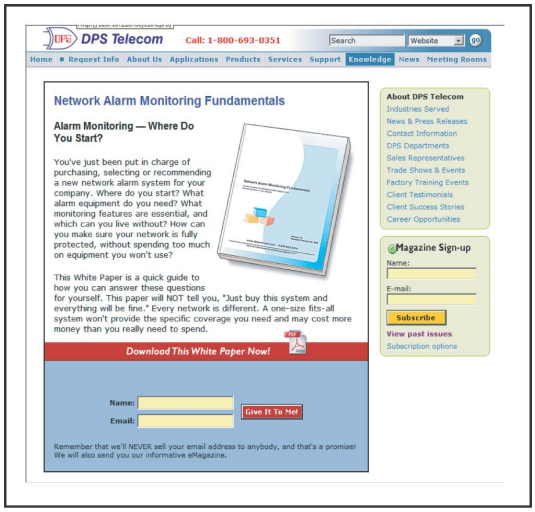
Need help with your alarm monitoring? DPS Information Services are ready to serve you … in your email or over the Web!

www.DpsTele.com

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

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

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



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

Free Tech Support on the Web: MyDPS

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

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

DPS Telecom
"Your Partners in Network Alarm Monitoring"

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

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