Sentry

Remote Power Manager

Operations Manual

Third Edition, January 2001.

Table of Contents

Introduction and Initial Connection 1
Starting a Session 1
Logging In 2
Default Usernames 3
Command Prompt 4
Command Syntax Rules 4
General Commands 5
OFF 5
ON 5
REBOOT 6
STATUS 6
SHOW 6
CONNECT 7
LOGIN 8
RESYNC 8
VERS 8
QUIT 8
SET Commands 9
SET CONNECT 9
SET LOCATION 9
SET MODEM 10
SET NETAUTH 11
SET PANEL 12
SET PASSWORD 12
SET CNFG (*Power Tower Specific*) 12
SET SHOW 13
SET SCREEN 13
SET TEMPH 14
SET TEMPL 14
SET LOADH 15
SET LOADL 15
SET ILOADH 15
SET ILOADL 16
SET ENABLET 16
SET DISABLET 17
SET TRAPTIME 17
LIST TRAPS 18
Username/Password and Serial Port Name Administration Commands 19
ADD USER 19
ADD PORT 19
ADD SNAME 19
DEL USER 21
DEL PORT 21
DEL SNAME 21
LIST USERS 22
LIST USER 22
LIST PORTS 22
LIST PORT 22
LIST SNAME 22

Power Control Screen..25
Screen Item Descriptions..26
Location: 26
Input Load:..26
Port Name: 26
Control Status:..26
Module Status: 27
Device Load:...27
Minimum-On Time: 27
Minimum-Off Time:..27
Shutdown Delay:...27
Wake-Up State:..28
Group: 28
Access: 28
Page:..28
Temperature:...28
Ending a Session 29
Resetting to Factory Defaults...30
Network Access Device Configuration 31
Network Access Device TCP/IP Configuration...31
Starting a Session through the Network Access Device: 33
Modifying the Network Access Device Telnet Port...33
Disabling the Network Access Device Inactivity Timeout...33
Encrypted Telnet Support 34
Network Access Device SNMP Configuration...35
Network Access Device TACACS+ Configuration...37
Network Access Device SecurID Support 39
Network Access Device Out-Of-Band Authentication Support...40
Network Access Device Authentication Fallback Support 40
Additional Network Access Device Security Options 41
Passwords and Password Requirements...41
IP Security Table..42
Resetting the Network Access Device to Factory Defaults...43
Sentry SNMP Support...44
Temperature Limit Exceeded Trap...45
Sentry Start Up Trap...46
Control Status Change Trap 46
Module Status Error Trap..46
Device Load Error Trap..47
Input Load Error Trap 47
Sentry Shutdown and Windows NT UPS Service Configuration 48
Support and Warranty 51
Support 51
Warranty...51
Appendix A -- Sentry MIB...52
Appendix B -- Sentry OID Tree..62

Introduction and Initial Connection

The Server Technology Inc. Sentry family of products provides easy, practical, and secure solutions for power management of remote internetworking equipment. Although the various Sentry hardware products are tailored for a wide range of applications, the software operation of these various products is designed to be consistent throughout the product line. This manual describes the software operation of the Sentry products. Because the different products in the Sentry product line offer different features, not all of the commands and operations described in this manual may be applicable to your specific Sentry product.

Starting a Session

Once you have installed and configured your Sentry product, it is necessary to establish a connection to the Sentry. You may use any terminal or terminal emulation program that you chose to connect to the Sentry. The terminal or terminal application must be configured to support ANSI or VT100.

Sending two carriage returns to the Sentry starts a session.

For Modem access, the user first uses any communication software that supports ANSI or VT100 terminal emulation to dial the phone number of the external modem attached to the Sentry. When the modems connect, the user then presses the Enter key twice to send two carriage returns.

Note: When setting up the Sentry for the first time, the first modem call made to the Sentry should be made with the dialing modem set to 9600 bits per second (BPS), which is the factory default modem data rate for the Sentry. This should guarantee that the first connection will succeed, after which the Sentry’s modem initialization data rate can be increased with the “SET MODEM RATE” command and the dialing modem’s data rate can be increased in the communication software.

For direct RS-232C access, the user starts any serial communication software that supports ANSI or VT100 terminal emulation. The program must configure the serial port to one of the supported data rates (38400, 19200, 9600, 4800, 2400, 1200, and 300 BPS), along with no parity, 8 data bits, and one stop bit, and must assert the Device Ready output signal (DTR or DSR). The user then presses the Enter key twice to send two carriage returns.

For Ethernet Network Connections, the user connects to the Sentry by using a TELNET program and connecting to Port 2001 at the TCP/IP address configured for the ServerTech MSS installed in the Sentry. Please refer to the Network Access Device Configuration section of this manual for information on configuring the MSS.

The Sentry will automatically detect the data rate of the carriage return and send a username login prompt back to the user, starting a session.

Logging In

After the carriage returns, the user will receive a banner that consists of the word “Sentry” followed by the current Sentry version string, a blank line, and then a “Username:” prompt. (Note the X.Xx in the following illustration is replaced by the current Sentry version.

```
Sentry Version X.Xx

Username: _
```

The Sentry banner will only be displayed after the initial connection or after the LOGIN command. In response to the “Username:” prompt, the user enters a valid username string. The username is a character string up to 16 characters long followed by a carriage return. Usernames may not contain either spaces or the colon ‘:’ character. Usernames are not case sensitive. The user has up to 60 seconds to enter a username string. If data is not entered within the time limit, the session is ended with the following message: "Your time is up. Try again later!".

After the user responds to the “Username:” prompt, the user will be prompted for an associated password with the “Password:” prompt.

```
Password: _
```

The Sentry will not echo characters typed in response to the password prompt. Passwords are up to 16 characters and are case sensitive. Alphanumeric and other typeable characters (ASCII 32 to 126 decimal) may be used. The Sentry will validate the username/password strings against the internal table of usernames/passwords that have been previously defined. If the user enters an invalid username string or password, the Sentry will send an error message as follows: “Username/Password entered is NOT valid!”. The user will then receive the “Username:” prompt again. The user will have three chances to enter a correct username/password. If a valid username/password is not specified on the third attempt, the following message will be sent: “Check your Username/Password and try again later!”. The current user session will then be ended. As with the username, the user has up to 60 seconds to enter a password string. If data is not entered within the time limit, the session is ended with the following message: “Your time is up. Try again later!”.

The Sentry supports a three-level username/password scheme, with up to 120 total users. There is one built-in administrative system-level username (ADMN), two built-in general-user system-level usernames (GEN1 and GEN2), and up to 117 general-users port-level usernames can be added.

Only a user logged in with the built-in administrative system-level username (ADMN) can make configuration changes. The administrative user can also view the status of all power outputs, and control power to all power outputs. A user logged in with a built-in general-user system-level username (GEN1 or GEN2) can view the status of all power outputs, and initially can control power to all power outputs, but may be restricted by the administrator to only controlling power to specific power outputs. A user logged in with an added general-user port-level username can only view the status of, and control power to, specific power outputs that have been assigned by the administrator.

Default Usernames

There are three built-in system-level usernames and passwords. The built-in usernames and passwords are:

Username: **ADMN**	Password: **admn**
Username: **GEN1**	Password: **gen1**
Username: **GEN2**	Password: **gen2**

These usernames cannot be deleted. By default, all three built-in usernames have access to all individually controllable power outputs, which are also called Intelligent Power Modules (IPMs) throughout this manual.

The “ADMN” username is the administrative username. These default usernames are able to view the status of all IPMs in the Sentry chain even if they do not have access to the IPMs for turning power on and off. Newly added usernames can only view the status of IPMs to which they have power on and off access. This means that a user logged in with any of the three default usernames can determine the number of IPMs in a Sentry by issuing the STATUS command (described later in this manual) because the status of all IPMs will be reported. A user logged in with a non-default username will only be able to view the status of IPMs to which the username has been assigned access.

When logging in for the first time, the system administrator should use the default administrative username. This will allow the system administrator to configure all the options, as well as to change the default passwords. Changing the passwords is done using the “SET PASSWORD” command at the command prompt. This command, as well as the other administrative commands, are described in the next section.

Command Prompt

The command prompt interface is used for power control and configuration of some options, including adding/deleting usernames, changing passwords, and changing the modem initialization data rate. From the command prompt, power control actions can be applied to individual IPMs or to a group of IPMs.

All configuration changes made at the command prompt are effective immediately and are saved to non-volatile RAM when the session is ended.

Once a valid username and password has been entered, the Sentry displays a command prompt:

```
Sentry: _
```

To get a display of available commands, press enter at the Sentry prompt, which will show:

```
Sentry commands are:

   CONNECT LOGIN OFF ON QUIT REBOOT RESYNC SET ADD DEL LIST SHOW
   STATUS  VERS
```

Note: The RESYNC, SET, ADD, DEL, and LIST commands will only be available when logged in with the administrative-level username (ADMN). In addition the SHOW command will only be available if the administrator grants SHOW privileges to the username. By default the GEN1 and GEN2 usernames have SHOW privileges. Added usernames do not have SHOW privileges unless specifically granted by the administrator via the SET SHOW command described later in this manual.

Command Syntax Rules

`CAPS` Keywords that are entered exactly as shown appear in all uppercase letters. Upper or lowercase can be used when the command is entered.

`Words` Parameters that are replaced with data appear in words that are a combination of uppercase and lowercase letters. The word indicates the type of parameter required. Upper or lowercase can be used when the command is entered.

`{ }` Required parameters appear within curly brackets. Do not include the brackets when the command is entered.

`[ ]` Optional parameters appear within square brackets. Do not include the brackets when the command is entered.

| A broken vertical bar indicates the OR function. Enter only one of the options or parameters shown. Do not include the broken vertical bar when the command is entered.

* An asterisk indicates that an entry may be repeated as many times as needed. The entry that may be repeated appears within the preceding curly or square brackets. Do not include the asterisk when the command is entered.

General Commands

Note: The port name and group parameters in the following OFF, ON, REBOOT, and STATUS commands are the administrator-defined names from the Power Control Screens (See the following Power Control Screen section for descriptions of these fields). Multiple IPMs or groups can be specified, each separated by a space, up to 50 characters. In addition port names may be specified as absolute port names. An absolute port name is specified by a period (".") followed by the Sentry Board letter (i.e. "A" for the first board, "B" for the second board, etc.) and the port number ("1", "2", "3", or "4") on the specific board. For example, the third port on the third Sentry Board in the chain of boards would have an absolute port name of ".C3". If the chain of Sentry Boards is altered for any reason, the absolute port names change. For example, if the second board in the chain is removed, such that the third board changes to becomes the second board, then the absolute port names change from "C1, C2, C3, C4" to "B1, B2, B3, B4". An absolute port name always refers to a single port on a specific Sentry board.

OFF {Port Name|Group|ALL} [{Port Name|Group}*]

Turns off an individual IPM, a predefined group of IPMs, or all IPMs for which the user has access.

Example: `OFF Device`

The OFF command returns information in the form:

```
n port(s) turned off
m port(s) locked
```

n indicates the number of referenced IPMs that turned off.
m indicates the number of referenced IPMs that are locked in their current state.

ON {Port Name|Group|ALL} [{Port Name|Group}*]

Turns on an individual IPM, a predefined group of IPMs, or all IPMs for which the user has access.

Example: `ON Device`

The ON command returns information in the form:

```
n port(s) turned on
m port(s) locked
```

n indicates the number of referenced IPMs that turned on.
m indicates the number of referenced IPMs that are locked in their current state.

REBOOT {Port Name|Group|ALL} [{Port Name|Group}*]

Turns off, delays, and turns back on, an individual IPM, a predefined group of IPMs, or all IPMs for which the user has access. The delay before turning back on is either 15 seconds or the Minimum-Off Time from the Power Control Screen, whichever is greater.

Example: `REBOOT Device`

The REBOOT command returns information in the form:

```
   n port(s) rebooted
   m port(s) locked
```

n indicates the number of referenced IPMs that were rebooted.
m indicates the number of referenced IPMs that are locked in their current state.

STATUS [Port Name|Group|ALL] [{Port Name|Group}*]

Returns the status of an individual IPM, a predefined group of IPMs, or all IPMs. For the three default usernames (i.e. admn, gen1, and gen2), this command can report the status for an IPM for which power control access is not allowed. For all other usernames this command can report status only for IPMs for which the username has power control access.

Example: `STATUS Device`

The STATUS command returns information in the form:

```
 n port(s) on
 m port(s) off
```

n indicates the number of referenced IPMs that are on.
m indicates the number of referenced IPMs that are off.

SHOW [Page|MODEM|NETAUTH|CONNECT {SWITCH|MODEM|LINK|CONSOLE|NETWORK}]

With no parameter or with a page name, this command puts the Sentry into the screen oriented interface mode. With no parameter specified, display starts at the Power Control Screen of the first four power modules. If a page name is specified, display starts at the Power Control Screen with that page name. See the Power Control Screen section that follows for setting the name of each page.

With the MODEM parameter, a page is displayed that shows the current modem data rate and the current status of the modem initialization strings.

With the CONNECT parameter, one of the five serial port names listed above must be specified. The SHOW CONNECT command displays the current setting of DSR and CTS checking for the specified serial port name.

With the NETAUTH parameter the current settings of the Sentry out-of-band network authentication feature for the CONSOLE and MODEM ports is displayed. The following is an example of the display that is shown in response to the SHOW NETAUTH command:

```
NetAuth settings:

  Modem:     Off
  Console:   Off
```

For more information on network authentication, please refer to the Sentry SET NETAUTH command and to the Network Access Device Configuration descriptions later in this document.

Note: The SHOW command is always available to the default usernames (i.e. ADMN, GEN1 and GEN2). By default, added usernames are not allowed to use the SHOW command. The administrator (i.e. ADMN username) may add and delete SHOW command privileges to other usernames using the SET SHOW command described later in this manual.

CONNECT {1-32|Serial Port Name|IPM Name|CONSOLE|MODEM|LINK|NETWORK}

This command attempts to make a connection to a serial device attached to one of the four standard serial ports (CONSOLE, MODEM, LINK or the internal NETWORK), or to any blue Pass-through Port.

There are two types of blue Pass-through ports: Side-Switch ports, and End-of-Chain ports.

In most cases, when the blue Pass-through Ports are built into the same enclosure as the IPM Ports, the blue Pass-through Ports are known as Side-Switch ports. Side-Switch ports are automatically associated with IPM ports and are addressed by using the same names that are assigned to the Sentry Power Modules or IPM Ports as a parameter to the CONNECT command. For example – with a unit that contains Side-Switch Pass-through Ports – the name that is assigned to outlet #1 may also be used to establish a Pass-through connection out the first Pass-though Port. That is, the Port Name of the first IPM identifies not only that IPM’s outlet, but the name of the first side-switch port as well. The same goes for all remaining IPM ports that have side-switch ports associated with them.

The CONNECT command can also be used to address End-of-Chain (EOC) Pass-through Ports that exist in-series at the end of a Sentry product or a chain of Sentry products. With End-of-Chain Pass-through Ports, the CONNECT command is entered with a single parameter, 1 to 32, to establish the connection out the EOC Pass-through Port. EOC Pass-through ports are identified by all blue ports being contained within their own separate enclosure, with a cable that connects from the LINK port of the final Sentry in a chain, to the LINK input port on the EOC Pass-through enclosure. Alternatively, the EOC Pass-through Ports may be contained within the same enclosure as a Sentry controller; if this is the case, the Pass-through ports can be identified as EOC ports by the Sentry unit NOT having a LINK port present

NOTE: Sentry Power Tower Administrator units only support End-of-Chain (EOC) pass through connections, either within the unit itself, or by being linked to a separate EOC Pass-through unit; Power Tower Administrator units do not support side-switch type pass-through ports.

To ease the use of the CONNECT command, the administrator can configure names for any of the possible blue serial Pass-through ports that are available. The CONNECT command can then be used with the assigned name (i.e. the Serial Port Name parameter) to connect to the port associated with the Serial Port Name. When the CONNECT command is used with a Serial Port Name, or with a number from 1 to 32 as a parameter, the IPM access restrictions do not apply. All users can use the CONNECT command to connect to any serial port that has a Serial Port Name or is accessed with a number from 1 to 32.

If the CONNECT command is entered with no parameters, a list of possible names is displayed on the screen. The user can then use the CONNECT command with one of the names displayed to attempt a serial port connection. The administrator can use the ADD, DEL, and LIST commands to set up the Serial Port Name configuration. These commands are described later in this manual.

For most CONNECT commands, the Sentry defaults to requiring that the attached device assert a device-ready indicator in the form of both Data Set Ready (DSR) and Clear To Send (CTS), in order to successfully connect. These requirements can be individually enabled and disabled with the “SET CONNECT” command. When a connection is successful, the message “Connection complete” will be displayed, at which point communication to the attached device will be transparent through the Sentry.

When finished communicating to the serial device, type “!*login<CR>”. The keyword “login” is not case sensitive. This disconnection character sequence returns the user to the login username prompt at which point the user may login normally to the Sentry.

A disconnection will also automatically occur when CD or DSR goes inactive on the device that started the session (as caused by hanging up a modem or exiting a communications program) or when a Telnet session is disconnected.

LOGIN

Brings up the “Username:” prompt to allow a user to re-login under a different username. No parameters.

RESYNC

Ends the session and resynchronizes the chain of Sentry boards. This command should be issued after adding or removing a Sentry board from the chain if all of the chain is not accessible. This is an administrative-level command.

VERS

Displays the firmware version of the first Sentry in the chain. No parameters.

QUIT

Ends the session. No parameters.

SET Commands

Note: Set commands are only available when logged in with the administrative username (i.e. admn).

To get a display of available SET commands, just enter “SET” at the Sentry prompt, which will show:

```
SET commands are:

   CONNECT LOCATION MODEM NETAUTH PANEL PASSWORD SHOW SCREEN TEMPH
   TEMPL LOADL LOADH ILOADL ILOADH ENABLET DISABLET TRAPTIME
```

SET CONNECT {CONSOLE|MODEM|LINK|NETWORK|SWITCH} {DSRCHECK|NODSRCHECK|CTSCHECK|NOCTSCHECK}

Turns on or off active signal checking when connecting to a pass-through port when using the CONNECT command. There are two required parameters with the command, a serial port name and a signal check state.

Of the possible serial port names, CONSOLE, MODEM, LINK, and NETWORK all refer to a specific single serial port. The SWITCH serial port name, however, applies to **all** side-switch pass-through port connections. It is not possible to set individual side-switch ports to different signal checking states.

When dealing with multiple End-of-Chain (EOC) blue Pass-through connections, the serial port name LINK is used to enable or disable DSRCHECK and/or CTSCHECK for all of the EOC ports. Like side-switch ports, it is not possible to set individual EOC ‘Link’ Pass-through connections to different signal checking states.

DSRCHECK requires that DSR be active from the attached device to connect. NODSRCHECK ignores that state of DSR. CTSCHECK requires that CTS be active from the attached device to connect. NOCTSCHECK ignores that state of CTS. When both DSR and CTS checking are disabled, Pass-through connections will always be made, regardless of whether or not a device is ready or not, or even connected. Both DSR checking and CTS checking will need to be disabled in order to allow connections to serial devices that only support Transmit Data, Receive Data, and a Signal Ground. The defaults are as follows for each of the five ports:

	DSR	CTS
Console	On	Off
Modem	On	On
Link	On	On
Network	Off	On
Switch	On	Off

SET LOCATION {Location}

Sets the location description field of the Power Control Screen for the entire Sentry chain. The location field is displayed as part of a “Welcome to...” message when a session is started. Up to 16 characters, including spaces, can be entered. Extra characters will be truncated from the location field.

SET MODEM {RATE {NONE|300|1200|2400|4800|9600|19200|38400}}
SET MODEM {INIT1|INIT2|INIT3|ATTENTION|HANGUP} {DEFAULT|NONE}

SET MODEM RATE sets the initialization data rate for the modem attached to the Sentry. The data rate can be set to any of the listed speeds (300, 1200, 2400, 4800, 9600, 19200, or 38400 Bits Per Second). The NONE parameter is used to disable all modem initialization string support. The default is 9600 BPS. The initialization takes place at the administrator-selectable data rate, with no parity, 8 data bits, and one stop bit.

SET MODEM INIT1, INIT2, INIT3, ATTENTION, or HANGUP, allows an individual modem initialization string to be enabled (DEFAULT) or disabled (NONE). The default setting is enabled (DEFAULT).

The Sentry initializes the modem when the Sentry is first turned on, whenever the modem is turned on or connected, and after every user session (via modem) with the Sentry. During initialization, the Sentry sends each of the following five-fixed modem initialization strings that is enabled to the modem in the following order:

Attention String:	**@@@**
Hang-up String:	**ATH**<CR>
Initialization String 1:	**AT**<CR>
Initialization String 2:	**AT E0 Q1 S0=3 S2=64 S12=50 &C1 &D2**<CR>
Initialization String 3:	**AT S0=1**<CR>

The Attention String is sent to switch from online mode to command mode if a modem is connected. The “S2=64” in Initialization String 2 sets the modem’s escape character to “@” to match the “@@@” Attention String used by the Sentry.

The Hang-up String is sent to cause the modem to hang up if there is an active connection.

Initialization String 1 is sent to alter the modem’s DTE data rate to the rate of the initialization string, and to allow the modem time to prepare for the next command.

Initialization String 2 is sent to initialize the modem to defaults required by the Sentry. The “E0” turns off the echoing of data, the “Q1” turns off result codes and the "S0=3" sets the modem to answer on the 3rd ring.

Initialization String 3 is sent to set the modem to answer on the 1st ring.

The modem initialization features allow a choice for the modem to answer on either ring number 1 or ring number 3. Initialization String 3 is “AT S0=1<CR>”. Like the other initialization strings, Initialization String 3 defaults to being enabled, and is sent in sequence after Initialization String 2. When this happens, the modem answers on ring number 1. To have the modem instead answer on ring number 3, disable Initialization String 3 with the command “SET MODEM INIT3 NONE”.

For most modems, Initialization String 1 or 2 being sent by the Sentry to the modem at one of the supported data rates is all that is needed for the modem to work with the Sentry. This is because most modems will communicate to the attached serial device (in this case, the Sentry) at the data rate of the last

AT command that was sent to it. A modem that operates in this manner is operating in *fixed data rate mode*. Since the Sentry sends the last AT command at one of its supported data rates, the modem will talk back to the Sentry at that same data rate when it is on-line with another modem.

Some high-speed modems, however, can be configured to operate in *variable data rate mode*. With a modem set to operate in *variable data rate mode*, when the modems connect, the modem may change from the speed of the last AT command to a different data rate, automatically adjusting to a data rate that is best for the actual modem-to-modem connect speed. If the data rate changes to one of the supported data rates, then the Sentry will be able to communicate because the Sentry will automatically detect the data rate. But, if the data rate changes to a non-supported data rate, such as 14400, 28800, or faster than 38400 BPS, the Sentry will not be able to communicate. Thus, it is best that the modem be configured to operate in *fixed data rate mode*, NOT *variable data rate mode*.

Configuring the modem to operate in *fixed data rate mode* is not addressed by the modem initialization built into the Sentry because the command that sets the modem to use *fixed data rate mode* varies significantly with different modem manufacturers.

If the modems are able to connect with each other, but there is not communication with the Sentry the modem attached to the Sentry is probably in *variable data rate mode* and has switched to an unsupported speed. In this case, in the modem’s manual, lookup the appropriate AT command(s) for the modem to operate in *fixed data rate mode*. Then attach the modem to a PC with a terminal program, send the command(s) to the modem, followed by an &W to write the new setting to the modem’s memory and make it the default, and then re-attach the modem to the Sentry.

SET NETAUTH {MODEM|CONSOLE} {ON|OFF}

The Sentry supports both TACACS and SecurID authentication protocols. By default, these protocols only apply to incoming Telnet sessions (in-band) as described in the Network Access Device Configuration section later in this manual. The SET NETAUTH command allows users to specify the use of these protocols for connections that use the modem and/or the console ports (out-of-band). When network authentication is enabled on these ports, the carriage returns that normally start a session will cause a connection to the Sentry Network Access Device, which will prompt the user for the network authentication username and password/passcode, and perform the authentication with the appropriate network server. If successful, the user is allowed to log into the Sentry with a Sentry username and password. If not successful, the user is disconnected.

The SET NETAUTH command is used to enable or disable out-of-band network authentication on the Modem and Console ports. The first parameter specifies which port (MODEM or CONSOLE) is to be the object of the command, and the second parameter specifies whether network authentication is to be enabled (i.e. ON) or disabled (i.e. OFF). The default is off (disabled), for both the Modem and Console ports.

The current settings can be displayed with the SHOW NETAUTH command as described earlier in this document.

For network authentication to work on any port, you must first enable TACACS and/or SecurID in the Sentry Network Access Device as described in the Network Access Device Configuration Section of this manual.

SET PANEL {NONE|DEFAULT}

Changes the operational behavior of the front panel pushbuttons, if present. NONE disables the pushbuttons. DEFAULT sets the front-panel pushbuttons to cycle through 2-states (ON and OFF) for non-Shutdown ports, and three states (ON, Shutdown, and OFF) for Shutdown ports. This is the default-operating mode from the factory.

The “DEFAULT” option supports locking a port in the on or off state by pressing and holding the port’s pushbutton for two seconds, at which point the LED above will flicker rapidly. If the port is on, this action will lock the port on. If the port is off, this action will lock the port off. To unlock a port, again press and hold the port’s pushbutton for two seconds – the port will stay in the same on or off state, it will just be unlocked again.

When a port is locked, a user cannot change the power state of the port remotely. A user logged in with the “admn” username, however, can lock or unlock a port remotely from the Power Control Screen by positioning the cursor in the column of the target port, and then pressing “L” to lock or “U” to unlock the port.

SET PASSWORD [Username]

SET PASSWORD command is used to change the password of any username. The administrator may specify the username for which the password is to be changed as a parameter to the SET PASSWORD command or the SET PASSWORD command may be entered with no parameters. When the SET PASSWORD command is entered without specifying a username, the system will prompt the for a username with the following prompt: “Username:”. If a valid username is not specified either as a parameter on the SET PASSWORD command or in response to the “Username:” prompt, the following message is displayed: “Name you have entered is NOT valid!”, and the SET PASSWORD command is terminated. If the administrator enters a valid username, the system prompts for the new password and also for a verification of the new password. The current password must be specified in order to change the password for the administrator username (i.e. “admn”). For all other usernames the password is changed without having to first specify the existing password. The password cannot contain more than 16 characters or the command is aborted with the following message: “Password is NOT valid!”. The following message is displayed when the password is changed: “All pages changed password”.

The Sentry will echo the ‘*’ character for all characters entered by the administrator for passwords when using the SET PASSWORD command. This includes the new password, the verification of the new password, and the verification of the existing password in the case of changing the ADMN password.

SET CNFG {Board|ALL} {IPMWAKEON|IPMWAKEOFF} (*Power Tower Specific*)

This command is used to change the wake up state of an external Power Tower attached to the Sentry. This causes a message to be transmitted to the Power Tower attached to the Sentry board which sets the default wake up state of the Power Tower according to the specified parameter (i.e. IPMWAKEON or IPMWAKEOFF). The specified setting is stored in non-volatile RAM in the Power Tower.

The **ALL** parameter can be used to change all Power Towers attached to all Sentry boards in a chain at once. *If a specific board is specified via an absolute board address (i.e. a period followed by a letter), then only the external Power Tower attached to the specified board will be changed. The administrator must know the correct board based on the existing Sentry configuration.*

The default setting for a Power Tower is IPMWAKEON. With IPMWAKEON, when input power is applied to the Power Tower, all of the outlets immediately turn on (without sequencing), regardless of the Power Tower being connected to the Sentry control unit or not. This allows the Power Tower (and devices powered by the Power Tower outlets) to be installed into a rack prior to installation of the Sentry control unit. After immediately turning on the outlets, if the Power Tower is (or when it gets) connected to the Sentry control unit, the Sentry control unit takes over control of the outlets, and will set the power state of the outlets to the current Control Status state in the Sentry control unit.

With IPMWAKEOFF, when input power is applied to the Power Tower, all of the outlets remain off. The outlets remain off until the connected Sentry control unit instructs the outlets to turn on. This allows the Sentry control unit to perform power up sequencing of the devices attached to the Power Tower outlets, which avoids an in-rush current condition. With IPMWAKEOFF, the Sentry will turn on each outlet individually in sequence, with a delay between each outlet:

- When the Power Tower and Sentry power up together (recovery from a site outage), the sequence delay time between outlets is two seconds. Each outlet that is configured in the Sentry with a “Wake-Up State” of “On” will be turned on at its sequence time.

- When the Power Tower powers up while the Sentry is already on (recovery from a single circuit outage), the sequence delay time between outlets is about 1/5 second, with an additional two seconds between each set of four outlets. Each outlet with a current “Control Status” of “On” will be turned on at its sequence time.

Note: If the Sentry loses and regains power without the Power Tower having lost power, the power outlets do NOT change states. Instead, the Sentry gets the status of each outlet from the Power Tower and updates its current “Control Status” to match.

SET SHOW [Username [ON|OFF]]

The SET SHOW command is used to enable or disable SHOW command access for a username. The SET SHOW command can be entered with no parameters, with a single parameter (which is the username) or with two parameters (which are the username followed by “on” or “off” to indicate the SHOW command is to be enabled or disabled). If a parameter is not specified, the administrator is prompted for the user name with the “Username:” message, followed by a prompt for the “on” or “off” specification with the “Specify ON or OFF:” message. If the administrator does not specify a valid username in response to the “Username:” prompt, the command aborts with the following message: “Name entered is NOT valid!”. If the administrator enters a valid single parameter, only the “Specify ON or OFF:” prompt occurs. If the administrator specifies both the username and “on”/“off” parameters, then there is no prompting. The appropriate error message is issued and the command aborted if the username is invalid, regardless if the “on”/“off” value is specified as a parameter on the command line or is entered in response to a prompt. If the command completes successfully, the following message is displayed: “Show command enabled/disabled for USERNAME”. In this message, USERNAME is replaced by the specified username and either enabled or disabled is displayed depending on the action taken.

SET SCREEN {CONFIRM|NOCONFIRM}

The SET SCREEN command is used to enable or disable a confirmation question when using the Sentry full-screen interface. When the CONFIRM option is set, the user is prompted with “Are your sure? (Y/N)” when making power changes via the SHOW screen. When the NOCONFIRM option is set, changes are made immediately. The default value is NOCONFIRM. This setting applies to all users.

Note: The following SET commands are used to set parameters pertaining to SNMP traps that can be generated by Sentry products. Please refer to the SNMP trap section of this manual for a description of the SNMP traps that are supported by the Sentry. Not all Sentry hardware supports all SNMP traps. Please refer to the hardware manuals for your specific Sentry product for information on the capabilities of your product. Some of these commands use Board Name as a parameter. The Board Name is the name specified in the Page field of the SHOW command full screen interface (described later in this manual). In addition to specifying the mnemonic name from the SHOW command page field, the administrator may specify an absolute Board Name by preceding the Board Name with a period ("."). Appending the Sentry Board letter (i.e. "A" for the first board, "B" for the second board, etc.) to the leading period creates the absolute Board Names. For example, the third Sentry Board in the chain of boards would have an absolute Board Name of ".C". If the chain of Sentry Boards is altered for any reason, the absolute Board Names change. For example, if the second board in the chain is removed, and what used to be the third board is now connected to the first board (it is now the second board in the chain), then the absolute Board Name on the new board changes from ".C" to ".B". An absolute Board Name always refers to a single board in a Sentry chain.

SET TEMPH [{Board Name|ALL} [Value]]

This command is used to set the SNMP temperature trap high limit. The SET TEMPH command takes two optional parameters. The first is the Board Name. If the Board Name parameter is not specified on the command line, the Sentry prompts for the Board Name with the "Board:" prompt. The administrator may specify an absolute Board Name, a mnemonic Board Name from the SHOW command page field, or the keyword ALL to cause all boards in the chain to be modified by the command.

The second parameter is the temperature limit value to be set. The value is in degrees Celsius and may be any value from 1 to 125. If the value is not specified on the command line, the Sentry prompts for the value with the "Temperature:" prompt. If the value specified is not within the proper range, the following error message is displayed: "Invalid Temperature, Valid range 1 to 125".

When the command completes successfully, the following message is displayed: "Limit Value Set Successfully on X board(s)/port(s,) Command Completed Successfully!". The "X" in the message indicates the number of Sentry boards modified by the command.

SET TEMPL [{Board Name|ALL} [Value]]

This command is used to set the SNMP temperature trap low limit. The SET TEMPL command takes two optional parameters. The first is the Board Name. If the Board Name parameter is not specified on the command line, the Sentry prompts for the Board Name with the "Board:" prompt. The administrator may specify an absolute Board Name, a mnemonic Board Name from the SHOW command page field, or the keyword ALL to cause all boards in the chain to be modified by the command.

The second parameter is the temperature limit value to be set. The value is in degrees Celsius and may be any value from 1 to 125. If the value is not specified on the command line, the Sentry prompts for the value with the "Temperature:" prompt. If the value specified is not within the proper range, the following error message is displayed: "Invalid Temperature, Valid range 1 to 125".

When the command completes successfully, the following message is displayed" Limit Value Set Successfully on X board(s)/port(s), Command Completed Successfully!". The "X" in the message indicates the number of Sentry boards modified by the command.

SET LOADH [{`Port Name|Group|ALL`} [Value]]

This command is used to set the SNMP output load-sense trap high limit. The SET LOADH command takes two optional parameters. The first is the Port Name. If the Port Name parameter is not specified on the command line, the Sentry prompts for the Port Name with the "Port Name:" prompt.

The second parameter is the amps limit value to be set. The amps value may be any value from 0 to 250. If the value specified is not within the proper range, the following error message is displayed: "Invalid Amps Value, Valid range 0 to 250". When the value is set to 0 (zero), a trap is generated when the 0 value occurs, since the amp value cannot go below 0. For all other values, the trap is generated when the value exceeds the limit.

When the command completes, the following message is displayed: "Limit Value Set Successfully on X board(s)/port(s), Command Completed Successfully!". The "X" in the message indicates the number of Sentry ports modified by the command.

SET LOADL [{Port Name|Group|ALL} [Value]]

This command is used to set the SNMP output load-sense trap low limit. The SET LOADL command takes two optional parameters. The first is the Port Name. If the Port Name parameter is not specified on the command line, the Sentry prompts for the Port Name with the "Port Name:" prompt.

The second parameter is the amps limit value to be set. The amps value may be any value from 0 to 250. If the value specified is not within the proper range, the following error message is displayed: "Invalid Amps Value, Valid range 0 to 250". When the value is set to 0 (zero), a trap is generated when the 0 value occurs, since the amp value cannot go below 0. For all other values, the trap is generated when the value exceeds the limit.

When the command completes, the following message is displayed: "Limit Value Set Successfully on X board(s)/port(s), Command Completed Successfully!". The "X" in the message indicates the number of Sentry ports modified by the command.

SET ILOADH [{Board|ALL} [Value]] (*Power Tower Specific*)

This command is used to set the SNMP input load-sense trap high limit. The SET ILOADH command takes two optional parameters. The first is the Board name parameter. If the Board name parameter is not specified on the command line, the Sentry prompts for the Board name with the "Board:" prompt.

The second parameter is the amps limit value to be set. The amps value may be any value from 0 to 250. If the value specified is not within the proper range, the following error message is displayed: "Invalid Amps Value, Valid range 0 to 250". When the value is set to 0 (zero), a trap is generated when the 0 value occurs, since the amp value cannot go below 0. For all other values, the trap is generated when the value exceeds the limit.

When the command completes, the following message is displayed: "Limit Value Set Successfully on X board(s)/port(s), Command Completed Successfully!". The "X" in the message indicates the number of Sentry boards modified by the command.

SET ILOADL [{Board|ALL} [Value]] (*Power Tower Specific*)

This command is used to set the SNMP input load-sense trap low limit. The SET ILOADL command takes two optional parameters. The first is the Board name parameter. If the Board name parameter is not specified on the command line, the Sentry prompts for the Board Name with the “Board:” prompt.

The second parameter is the amps limit value to be set. The amps value may be any value from 0 to 250. If the value specified is not within the proper range, the following error message is displayed: “Invalid Amps Value, Valid range 0 to 250”. When the value is set to 0 (zero), a trap is generated when the 0 value occurs, since the amp value cannot go below 0. For all other values, the trap is generated when the value exceeds the limit.

When the command completes, the following message is displayed: “Limit Value Set Successfully on X board(s)/port(s), Command Completed Successfully!”. The “X” in the message indicates the number of Sentry boards modified by the command.

SET ENABLET {STRT|TEMP|ILOAD} [Board|ALL]
SET ENABLET {MSTA|CSTA|LOAD} [Port|Group|ALL]

This command is used to enable an SNMP trap. The SET ENABLET command takes two parameters. The first is the type of trap to be enabled. There are six types of traps that are supported by the Sentry. They are:

STRT – trap generated when the Sentry is started or resynchronized.
TEMP – trap generated when the Sentry temperature probe senses a temperature out of limits.
MSTA – trap generated when an IPM indicates an error (Module STAus error).
CSTA – trap generated when a power change occurs (Control STAus change).
LOAD – trap generated when the output load on an IPM is out of limits.
ILOAD – trap generated when the input load on a Power Tower is out of limits.

If the first parameter is not specified, the command does not complete. A list of the possible trap types is displayed.

The second parameter is the Board Name for board-specific traps (i.e. STRT, ILOAD and TEMP) and is the Port Name for IPM-specific traps (i.e. MSTA, CSTA and LOAD). If the Board Name parameter is not specified on the command line, the Sentry prompts for the Board Name with the “Board:” prompt. If the Port Name parameter is not specified on the command line, the Sentry prompts for the Port Name with the “Port Name:” prompt.

When the command completes, the following message is displayed: “Trap Enabled/Disabled or Trap Time value set on X board(s)/port(s), Command Completed Successfully!”. The “X” in the message indicates the number of Sentry boards or ports for which the specified trap is enabled by the command.

SET DISABLET {STRT|TEMP|ILOAD} [Board|ALL]
SET DISABLET {MSTA|CSTA|LOAD} [Port|Group|ALL]

This command is used to disable an SNMP trap. There are six types of traps that are supported by the Sentry. They are:

STRT – trap generated when the Sentry is started or resynchronized.
TEMP – trap generated when the Sentry temperature probe senses a temperature out of limits.
MSTA – trap generated when an IPM indicates an error (Module STAus error).
CSTA – trap generated when a power change occurs (Control STAus change).
LOAD – trap generated when the output load on an IPM is out of limits.
ILOAD – trap generated when the input load on a Power Tower is out of limits.

The SET DISABLET command takes two parameters. The first is the type of trap to be disabled. If the first parameter is not specified, the command does not complete, and a list of the possible trap types is displayed.

The second parameter is the Board Name for board-specific traps (i.e. STRT, ILOAD and TEMP) and is the Port Name for IPM-specific traps (i.e. MSTA, CSTA and LOAD). If the Board Name parameter is not specified on the command line, the Sentry prompts for the Board Name with the “Board:” prompt. If the Port Name parameter is not specified on the command line, the Sentry prompts for the Port Name with the “Port Name:” prompt.

When the command completes, the following message is displayed: “Trap Enabled/Disabled or Trap Time value set on X board(s)/port(s), Command Completed Successfully!”. The “X” in the message indicates the number of Sentry boards or ports for which the specified trap is disabled by the command.

SET TRAPTIME [1-254]

This command is used to set the time delay that occurs between SNMP traps that are in a steady state condition. A steady state condition occurs when a trap value (for example a temperature value) is currently in a range that will cause a trap to be generated. When the value is in this range, SNMP traps are not constantly generated (this would preclude other operations), but rather SNMP traps are generated on a timed interval as set by the SET TRAPTIME command. The default value is 1 minute. The value specified as a parameter after TRAPTIME is the value of the time interval in minutes.

When the command completes, the following message is displayed: “Trap Enabled/Disabled or Trap Time value set on X board(s)/port(s), Command Completed Successfully!”. The “X” in the message indicates the number of Sentry boards or ports for which the specified trap is enabled or disabled by the command.

LIST TRAPS [Board Name|ALL]

The LIST TRAP command is used to list the current SNMP trap settings on one or more boards in a chain of Sentry boards

The LIST TRAP command takes a single parameter that is the name of the board to be listed. If this parameter is omitted, the Sentry prompts for the board name with the “Board:” prompt. If the administrator specifies an absolute board name (i.e. a period “.” followed by a letter), information on that specific board will be displayed. If a mnemonic name is entered, the command will display information on all boards with that board name with a “Press: N)ext, Q)uit:” prompt between board displays. The following is an example of the display that is returned by the LIST TRAP command:

```
TRAP INFORMATION FOR UNIT: .A

Sentry Start Up Trap: [X]    Temperature Error Trap: [X]        Input Load Trap: [X]

Temperature High Limit: 50 Deg C    Temperature Low Limit: 1 Deg C

Input Load High Limit: 250 Amp(s)     Input Load Low Limit: 1 Amp(s)

                         .A1     .A2     .A3     .A4
Control Status Trap      [X]     [X]     [X]     [X]
Module Status Trap       [X]     [  ]    [ ]     [ ]
Device Load Trap         [X]     [  ]    [ ]     [ ]
Load High Limit          4       4       4       4
Load Low  Limit          1       1       1       1

Trap Time Value (in minutes) is 1

Press: N)ext, Q)uit: n
```

The display begins with a line that prints the absolute board name for the board being displayed. Then a line is displayed that indicates whether the Start Up trap (STRT), the Temperature trap (TEMP), and the Input Load trap (ILOAD) are active on this board. An “X” between the brackets means the trap is active. Even if the Start Up trap is active on more than one board, start up traps are only generated on the first board in the chain of boards.

The next line shows the current Temperature trap limits for this board. The next line shows the current Input Load trap limits for this board. Following the input load limits is a four-column matrix that shows which traps are enabled for which ports on this board. An “X” between the brackets corresponding to the trap and the port indicates the trap is active. Only the absolute port names are displayed. Following the enabled/disabled display for the traps is a display of the current device load high and low limits for each of the four ports on this board. Next the current setting of the steady state trap time value is displayed. Finally, a prompt to continue with the next board or quit is displayed. When the command is complete a “Port List Complete” message is printed.

Username/Password and Serial Port Name Administration Commands

Note: The username/password and Serial Port Name administration commands are only available when logged in with the administrative username (i.e. admn). These commands are used to add/delete users, to allow/disallow access to Sentry IPMs for usernames, and to view the current usernames and their associated IPM access. They are also used to assign names to the various serial ports that can be accessed via the CONNECT command. The maximum number of usernames that can be assigned is 120. The maximum number of serial port names that can be assigned is 32.

ADD USER [Username]
ADD PORT [Username [Port Name|ALL]]
ADD SNAME [Serial Port Name [Serial Port Id]]

The ADD command is used to add usernames to the system, to add Serial Port Names, and to add port access to a username. The ADD command takes one required parameter and up to two optional parameters.

The first parameter is required and indicates whether a username is to be added (ADD USER), whether port access is to be granted to a user (ADD PORT), or whether a Serial Port Name is to be added (ADD SNAME).

The ADD USER command is used to add a new username to the system. The command can be entered with a single parameter (which is the new username) or with no parameters. If a parameter is not specified, the administrator is prompted for the username with the following prompt: “Username:”. A non-blank username that contains no more than 16 characters must be entered at this prompt or the command is aborted with the following message: “Name must be between 1 and 16 characters; spaces not allowed”. The username is not case sensitive.

Once the username is specified, the administrator is prompted for a password via the “Password:” message. The administrator is prompted for a verification of the newly entered password after entering the password. The verification password must match the first password entered or the command is aborted with the following message: “Password is NOT valid!”. The ‘*’ character is echoed in response to the characters typed for the password and the password verification strings. The password value entered at this prompt, and successfully verified, is stored as the password for this username and is used to validate this username during the normal Sentry logon processing. The password cannot contain more than 16 characters or the command is aborted with the following message: “Password is NOT valid!”. The password is case sensitive.

Once the information has been entered, the administrator receives the following message: “Command completed successfully!”. Note that only a value in the Username is required in this command. Blank or empty responses to the password prompt and the password verification prompt are accepted as valid.

By default, a new user does not have access to any resources on the Sentry Board, and cannot use the SHOW command. To allow a user to access a power module or a communications connection, the ADD PORT command must be used. To allow a user to use the SHOW command, the SET SHOW command must be used.

The ADD PORT command is used to allow a username to access a port in the Sentry Board chain. The specified port name gives access to both the power module and the side-switch communications pass-through port (if present) referenced by the port name. The command can be entered with no parameters, with a single parameter (which is the username,) or with two parameters (which are the username followed by the port name). If a parameter is not specified, the administrator is prompted first for the user name with the "Username:" message, followed by a prompt for the port name with the following prompt: "Port Name:". If the administrator does not specify a valid username in response to the "Username:" prompt, the command aborts with the following message: "Name entered is NOT valid!". A non-blank port name must be entered after the "Port Name:" prompt, or the command is aborted with the following message: "Port name is NOT valid!". If the Sentry does not recognize the port name, the command terminates with the following message:

```
        "0 port(s) added"
    "Command Completed Successfully"
```

This indicates that no port(s) were assigned to the specified user.

If the administrator enters only a single parameter, only the port name prompt occurs. If the administrator specifies both the username and port name parameters, there is no prompting. The administrator may specify "ALL" as a valid Port Name, which causes access to be added for all ports for the specified username. The appropriate error messages are issued and the command aborted if either the username or port name is invalid, regardless if the value is specified as a parameter on the command line or is entered in response to a prompt.

If the command completes successfully, the following message is displayed:

```
        "X port(s) added"
    "Command Completed Successfully"
```

Where "X" indicates the number of port(s) successfully added to the specified user.

The PORTNAME specified in this command can be an absolute port name, an administrator assigned port name, a group port name, or the keyword "ALL" to indicate all ports should be processed.

The ADD SNAME command is used to add a new name to a serial port in a Sentry chain. A maximum of 32 names can be added to the Sentry serial port name table. The command can be entered with no parameters, with a single parameter (which is the serial port name), or with two parameters (which are the serial port name followed by the serial port ID). If a parameter is not specified, the administrator is prompted first for the serial port name with the "Name:" message, followed by a prompt for the serial port ID with the "Serial Port ID:" message. If the administrator does not specify a valid serial port name in response to the "Name:" prompt, the command aborts with the following message: "Name must be between 1 and 16 characters; spaces not allowed". Valid serial port names are from 1 to 16 characters, with blanks not allowed. The serial port name is verified to ensure the name is not already used in the serial port name table. If the name is already used, it must first be deleted using the DEL command and then added. It is possible to have several entries that assign different names to the same Serial Port ID, but it is not possible to have the same name assigned to more than one Serial Port ID.

In response to the "Serial Port ID:" prompt, the administrator may enter either a number from 1 to 32 (to specify one of the 32 possible ports connected at the end of the chain), or a three-character absolute pass through port identifier that begins with a period ('.'), followed by a letter from A to Z , followed by a number from 1 to 4. The parameter is verified to ensure the serial port exists. If the serial port does not exist, the following message is displayed: “Port ID is NOT valid!” and the command ends with no further action.

DEL USER [Username]
DEL PORT [Username [Port Name|ALL]]
DEL SNAME [Serial Port Name [Serial Port Id]]

The DEL command is used to delete usernames from the system, to delete Serial Port Names, and to delete access to ports for a specific username. The DEL command takes one required parameter and up to two optional parameters.

The first parameter is required and indicates whether a username is to be deleted (DEL USER), whether port access is to be removed from a user (DEL PORT), or whether a Serial Port Name is to be deleted (DEL SNAME).

The DEL USER command is used to remove a username from the system. The command can be entered with a single parameter (which is the username to remove), or with no parameters. If a parameter is not specified, the administrator is prompted for the username with the following prompt: “Username:”. A valid system username must be entered at this prompt or the command is aborted with the following message: “Name entered is NOT valid!”. This command cannot be used to remove any of the three default usernames (i.e. ADMN, GEN1, or GEN2).

If the command completes successfully, the following message is displayed:

“X port(s) deleted”
“Command Completed Successfully”

Where “X” indicates the number of port(s) successfully deleted from the specified user that was deleted.

The DEL PORT command is used to remove access for a username to a port in the Sentry Board chain. The command can be entered with no parameters, with a single parameter (which is the username), or with two parameters (which are the username followed by the port name). If a parameter is not specified, the administrator is prompted first for the user name with the “Username:” message, followed by a prompt for the port name with the following prompt: “Port Name:”. If the administrator does not specify a valid username in response to the “Username:” prompt, the command aborts with the following message: “Name entered is NOT valid!”. A valid port name must be entered after the “Port Name:” or the command is aborted with the following message:

“0 port(s) deleted”
“Command Completed Successfully”

This indicates that no port(s) were deleted for the specified user.

(Note: see the discussion on port names in the ADD PORT command description for valid port names.)

The administrator may enter the keyword “ALL” in response to the “Port Name:” prompt, in which case access to all ports for this username is removed. If the administrator enters only a single parameter, only the port name prompt occurs. If the administrator specifies both the username and port name parameters, there is no prompting. The appropriate error messages are issued and the command aborted if either the username or port name is invalid, regardless if the value is specified as a parameter on the command line or is entered in response to a prompt. If the command completes successfully, the following message is displayed:

```
        "X port(s) deleted"
    "Command Completed Successfully"
```

Where "X" indicates the number of port(s) successfully deleted from the specified user

Note that access for the administrator cannot be removed.

The DEL SNAME command is used to remove a serial port name. The command can be entered with no parameters, or with a single parameter (which is the serial port name). If a parameter is not specified, the administrator is prompted first for the serial port name with the "Serial Port Name:" message. If the administrator does not specify a valid serial port name in response to the "Name:" prompt, the command aborts with the following message: "Name entered is NOT valid!".

LIST USERS
LIST USER [Username]
LIST PORTS
LIST PORT [Port Name]
LIST SNAME

The LIST command is used to list the current usernames active in the Sentry system with their current SHOW command access and the ports to which a username has access, to list the current users allowed access to the system ports, and to list the currently defined Serial Port Names.

The LIST command can be used to list all users in the system (LIST USERS), to list a single user and all ports to which the specified user has access (LIST USER), to list all ports in the Sentry chain and all users with access to all ports (LIST PORTS), and to list a single port and all users with access to that port (LIST PORT).

The LIST USER command is used to display information about a single user. This information includes a list of all ports on the system to which the user has access and whether the SHOW command is enabled or disabled for the user. The command can be entered with a single parameter (which is the username to list) or with no parameters. If a parameter is not specified, the administrator is prompted for the username with the following prompt: "Username:". A valid system username must be entered at this prompt or the command is aborted with the following message: "Name entered is NOT valid!".

If a valid username is specified, the following message is displayed:

```
Active Port List for Username XXXXXX   Show command enabled/disabled.
```

In the above message, XXXXXX is replaced by the username and either enabled or disabled is displayed depending on the status of the SHOW command for this username.

After the header message is displayed, a list of all ports to which the username has access is displayed. The absolute port name is displayed, followed by the administrator assigned port name (if there is one), followed by the group name (if there is one). If the list of ports fills a screen, the administrator is prompted to press N for additional names, or Q to end the list. The following is an example of the screen display:

```
.A1            PortA1         GroupA1
.A2            PortA2         GroupA1
.Z4            PortZ4         GroupA1

Press: N)ext, Q)uit
```

All ports will have at least the absolute port name displayed; however, the administrator assigned port name and the group name may or may not be present based on the configuration of the port.

The LIST USERS command is used to display a list of all the valid users on the system along with a display of whether the SHOW command is enabled or disabled for the user. If the username list fills the screen, the administrator is prompted to press N for additional names, or Q to end the list. The following is an example of the LIST USERS display:

```
        admn                          Show command enabled
        gen1                          Show command enabled
        gen2                          Show command enabled
        sentry1                       Show command disabled

Press: N)ext, Q)uit
```

When all users have been listed, the following message is displayed: “List Complete”.

The LIST PORT command is used to display a list of all users with access to a specific port on the system. The command can be entered with a single parameter (which is the port name to list) or with no parameters. If a parameter is not specified, the administrator is prompted for the port name with the following prompt: “Port Name:”

After a port name is specified, a list of usernames with access to the port is displayed on the screen. The port name being listed is displayed followed by a list of usernames. The port name is displayed as the absolute port name, followed by the user created port name (if there is one), followed by the group port name (if there is one). The following example illustrates the first group of a specific port name display:

```
.C4            USERPORT1              GROUPPORT1
usernames:
        admn                  gen1                        gen2
        sentry1               sentry2                     sentry3
        sentry4               sentry5                     sentry6
        sentry7               sentry8                     sentry9
        sentry10              sentry11                    sentry12
        sentry13              sentry14                    sentry15
        sentry16              sentry17                    sentry18
        sentry19              sentry20                    sentry21
        sentry22              sentry23                    sentry24
        sentry25              sentry26                    sentry27

Press: N)ext, Q)uit
```

When all users for a specific port have been displayed, the following message is displayed: “Username List for .XX Complete”, where .XX is the absolute Port identifier (i.e. **.C4**).

The LIST PORTS command is used to display a list of all ports on the system, with all users with access to each port on the system. The display is the same as for a single port name list as illustrated in the LIST PORT command above, except the N)ext, Q)uit prompt is displayed after the “Username List for PORT1 Complete” message is displayed, rather than returning to the Sentry prompt. Ports are displayed in port order starting with absolute port .A1 and ending with the forth port on the last Sentry board in the chain (unless the administrator specifies “Q” before the last port is listed).

When all users for all ports have been listed, the following message is displayed: “List Complete”.

The LIST SNAME command is used to display the current serial port names and the port associated with the serial port name. The command takes no parameters. The output of the LIST SNAME command is a display of the current serial port names. Each serial port name is followed by the Sentry’s physical port name. The names are displayed in groups of 20 ports. After each group of 20 ports is displayed the administrator is prompted to press N for additional names, or Q to end the list. The following is an example of the screen with three serial port names displayed.

```
TERMINALPORT          .A1
NTSYSTEM              .B4
LINKPORT              12
```

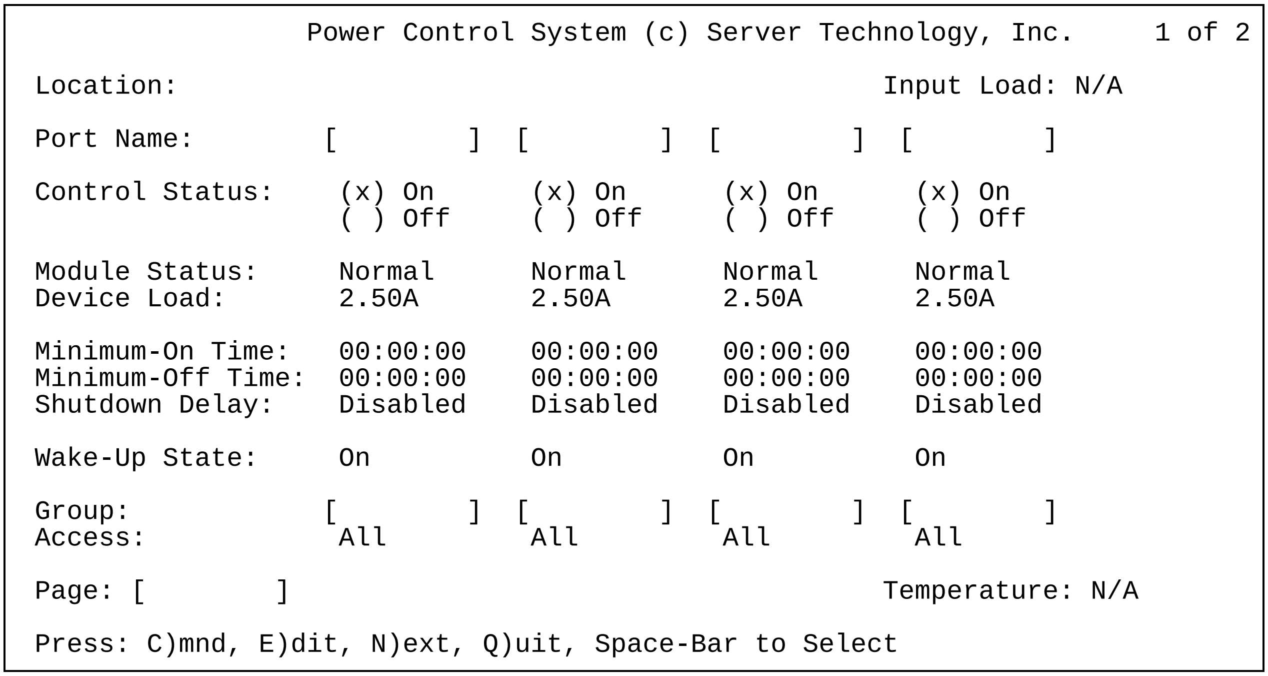
Power Control Screen

From the Power Control Screen, a user can control power and configure the Sentry by simply moving around the screen using the arrow keys and pressing an action key. All configuration changes made in the Power Control Screen are saved to non-volatile RAM and are effective immediately. Not all of the Sentry hardware supports all of the functions illustrated in the following descriptions. If a capability is not supported, the user will see an "N/A" displayed in the field on the screen.

The Power Control Screen is accessed by the SHOW command from the command prompt:

```
Sentry: SHOW
```

The SHOW command displays an ANSI power control screen (80 characters wide by 24 lines):



```
                 Power Control System (c) Server Technology, Inc.     1 of 2

Location:                                            Input Load: N/A

Port Name:        [        ]  [        ]  [        ]  [        ]

Control Status:    (x) On      (x) On      (x) On      (x) On
                   ( ) Off     ( ) Off     ( ) Off     ( ) Off

Module Status:     Normal      Normal      Normal      Normal
Device Load:       2.50A       2.50A       2.50A       2.50A

Minimum-On Time:   00:00:00    00:00:00    00:00:00    00:00:00
Minimum-Off Time:  00:00:00    00:00:00    00:00:00    00:00:00
Shutdown Delay:    Disabled    Disabled    Disabled    Disabled

Wake-Up State:     On          On          On          On

Group:            [        ]  [        ]  [        ]  [        ]
Access:            All         All         All         All

Page: [        ]                                     Temperature: N/A

Press: C)mnd, E)dit, N)ext, Q)uit, Space-Bar to Select
```

Sentry products can support up to 26 boards in a chain of boards. Each board has its own set of 4 Intelligent Power Modules (IPMs). The Sentry has a Power Control Screen for each of the boards in the Sentry chain. Some units have only one board and therefore only a single Power Control Screen. Others have multiple boards and therefore multiple Power Control Screens (one for each board). Each Power Control Screen is considered a different page and each Power Control Screen controls 4 IPMs. The page currently being viewed is displayed in the upper right corner of the screen, as is the total number of pages. The page currently being viewed is also indicated by the name in the Page field in the lower left of the screen.

The Help line at the bottom of the screen indicates what key presses are available for specific functions:

`C)mnd` puts the Sentry back into Command Prompt mode at the “Sentry:” prompt.
`E)dit` is used to edit fields enclosed by square brackets. When “E” is pressed, the cursor moves to the end of the current entry. The backspace key erases one character. Press Enter or Tab when done editing the field.
`N)ext` displays the next Power Control Screen page.
`P)revious` displays the previous Power Control Screen page.
`Q)uit` ends the current session.
`S)pace-Bar to Select` indicates that the space bar is used on non-editable fields to toggle between the predetermined settings. The space bar is also used on the status line to change the power state of a port to the state of the current cursor location (either On or Off). *Note:* The plus and minus keys can also be used to toggle forward or backward through the predetermined settings.

Screen Item Descriptions

Location:

This is a 16-character description field for the location of the Sentry. It has no purpose other than descriptive. The location field is displayed as part of a “Welcome to...” message when a session is started. The value of the Location is set using the SET LOCATION command described earlier.

Input Load:

This is an informational field that displays the current input load (in amps) on an external Power Tower product that is controlled by the associated board. If an external Power Tower is not attached, this field displays “N/A”.

Port Name:

This is an eight character descriptive field for the device plugged into the IPM. This field is used both as a description and as a parameter to the ON, OFF, REBOOT, and STATUS commands.

Control Status:

The current status of the IPM is shown by a character in the On or Off field. An “x” is displayed if the port is accessible remotely. An asterisk is displayed if the IPM is locked by the administrator, a front panel button press, or if the IPM is not accessible by the current password level.

To change the power state of an IPM, move the cursor to the desired state (On or Off), and press the space bar. The “x” will move to the new state, indicating the power changed to that state.

Press “R” when in the On or Off field to reboot the port. If the port is already off, it will turn on immediately. If it is on, it will turn off, delay, and then turn back on. The delay before turning back on is either 15 seconds, or the Minimum-Off Time, whichever is greater. During the reboot delay, an “r” is displayed in the Off field, indicating the port is going to reboot.

When in the On or Off field, tbe administrator can lock or unlock a port by pressing “L” to lock, or “U” to unlock. A locked port will display an asterisk in the On or Off field, and cannot be controlled by a general or added user – it can only be unlocked by the administrator.

Module Status:

This is an informational field that displays the current status of the associated IPM, as reported to the Sentry. This field is only significant if the Sentry product is equipped with the Server Technology “ON SENSE” IPMs that are capable of signaling the Sentry the on and off state of the IPM. If the Sentry product is not equipped with these “ON SENSE” IPMs, this field has no meaning. If the IPM is working correctly, this field will display “Normal”. If the Sentry is unable to communicate with the associated IPM, this field will display “No Rspns”. If the IPM is set to “On” and the Sentry detects the associated IPM is not on, this field will display “OnS Fail” (for On Sense Failure). If the IPM is set to “Off” and the Sentry detects the associated IPM is on, this field will display “Off Fail”. Sentry products equipped with “ON SENSE” IPMs can be configured to generate SNMP traps when On Sense errors are detected.

Device Load:

This is an informational field that displays the amount of current in Amps that is flowing through the associated IPM. This field is only significant if the Sentry product is equipped with the Server Technology “LOAD SENSE” IPMs that are capable of sensing the load going through the IPM and relaying this information to the Sentry. If the Sentry product is not equipped with these “LOAD SENSE” IPMs, this field has no meaning and “N/A” is displayed. This field will display the current in Amps when current is flowing. If the associated IPM is set to off with a module status of Normal, and no current is flowing this field will display “Not On”. Sentry products equipped with “LOAD SENSE” IPMs can be configured to generate SNMP traps when load sense values fall outside an administrator configurable range.

Minimum-On Time:

This is the minimum amount of time that an IPM will stay on before it can be turned off by actions at the Sentry command prompt. Manual actions in the Power Control Screen On or Off fields, however, are always immediate, ignoring this value. The default is 0.

Minimum-Off Time:

This is the minimum amount of time that an IPM will stay off before it can be turned on by actions at the Sentry command prompt. Manual actions in the Power Control Screen On or Off fields, however, are always immediate, ignoring this value, except in the case of a reboot. This field determines the off delay time of a reboot, if greater than 15 seconds. The default is 0.

Shutdown Delay:

This is the amount of time the Sentry will delay when a Power Off command is issued for an IPM before the IPM is actually set to the Power Off state. This delay is designed to allow a ShutDown signal to be sent to an operating system on a machine that is attached to the IPM. Pressing the space bar when positioned to this field changes this value. The value can be set from “Disabled” (i.e. no delay) to a series of choices ranging up to an eight minute delay. Please refer to the Sentry Shutdown and Windows NT UPS Service Configuration section of this manual for information on configuring automatic operating system shutdown.

Wake-Up State:

This is the state that the IPM will be in when controller power is turned on or when controller power is restored after a power outage. The options are ON and OFF. The default is ON.

Group:

The Group field takes an eight-character group identifier. All IPMs with the same group name can be acted upon simultaneously by command line actions (ON, OFF, and REBOOT). The group field can be left blank so that an IPM is not part of a group.

Access:

The Access field allows changing the access to the associated IPM for the three default usernames (ADMN, GEN1, GEN2). Access for additional users must be set via the username/password administration commands described earlier in this manual. With this field access can be granted to all three default usernames by setting the "ALL" value. To limit access to only the ADMN username, the field is set to "Admn". To limit access to the ADMNand GEN1 usernames, the field is set to "Gen1". To limit access to the ADMN and GEN2 usernames, the field is set to "Gen2". This field can only be modified when logged in with the ADMN username. The ADMN username always has access to all IPMs. The default is All.

Page:

The Page field is an eight character identifier to describe the current screen page, as a more descriptive alternative to the page numbering in the upper-right-hand corner of the screen. This entry is used as a parameter to the SHOW command to display the Power Control Screen of a specific set of four IPMs. If page names are entered, each page MUST have a unique page name.

Temperature:

This field displays the current temperature in degrees Celsius as detected by the temperature probe on the Sentry board, if the board is equipped with a temperature probe. If the Sentry is not equipped with a temperature probe, this field has no meaning and "N/A" is displayed. Sentry products equipped with temperature probes can be configured to generate SNMP traps when temperature values fall outside an administrator configurable range.

Ending a Session

Ending a session can be done from either the command prompt or the Power Control Screen:

From the command prompt, type QUIT and press Enter.
From the Power Control Screen, press “Q”.

A session will automatically be terminated after 5 minutes of inactivity.

A session will also automatically end when CD or DSR go inactive into the Modem or Console port, which occurs when the modem is hung-up or the communication software is exited. With a modem connection, the modem will automatically be hung-up by the Sentry lowering DTR to the modem, as well as sending the attention and Hang-up strings to the modem, if they have not been disabled.

By Telnet (if the option Network Access Device is installed – see next section), a session will also automatically end when the Telnet session is ended. The Telnet session will also automatically end when the Sentry session is ended.

When a session is ended, the user is notified with the message:

```
Session ended
```

There is then a period of about 15 seconds after a session is ended before another session can be started. This is due to the Sentry reinitializing the modem after a session is ended. If a modem is not used and the modem initialization strings are turned off, the time between sessions is only about 7 seconds.

Additionally, with the optional Network Access Device (see next section) and SNMP traps enabled, if the Sentry has pending SNMP traps to send, the time between sessions may be longer because pending SNMP traps are sent whenever a session ends. If the Sentry is busy during a subsequent attempt to start a session, the user is notified with the message: “The Sentry is busy, Try again later”.

Resetting to Factory Defaults

The non-volatile RAM that stores all configurable Sentry options, including the passwords, can be reset to factory defaults. This clears all the administrator-editable fields on the Power Control Screens and resets all the command-line configurable options to defaults, including the passwords.

Resetting to factory defaults can be done in two ways – by an administrative-level command at the Sentry prompt, or by a Reset button press during power up. This second method is necessary if the passwords are forgotten.

An administrative-level command reset is performed with the command:

```
SET CNFG ALL FACTORY
```

This command updates the current working configuration of the Sentry with the master configuration that was set at the factory. All Sentry boards in the chain are reset.

A power-up button-press reset is performed as follows:

Important Note: The power-up button-press reset procedure below resets both the Sentry boards and the Network Access Device (see next section) to factory defaults.

The power up button press reset must be done on the first Sentry at the beginning of a chain. The reset is performed by pressing and holding down the Reset button while turning on power with the On/Off toggle switch. Continue to hold down the Reset button for ten (10) seconds after turning on the power, and then let go.

Note: In the case of Sentry products that do not have a separate reset button, the A1 button on the button panel has a secondary function as a Reset button.

This will only reset the first power controller board in the Sentry at the beginning of a chain. The rest of the chain should then be reset by logging in with the administrator username (i.e. admn), and then issuing the administrative reset command shown above.

Network Access Device Configuration

The network option of the Sentry products is implemented by an OEM version of the MSS (Micro Serial Server) manufactured by Lantronix. This device is enclosed within the Sentry case and provides the Telnet-to-asynchronous functionality that allows the Sentry to be accessed over a TCP/IP Ethernet network.

NOTE: For purposes of this document, the MSS shall be considered part of the Sentry. References will be made to the Sentry as an Ethernet device, when, in actuality, it is the MSS inside the Sentry that provides the network functionality. The MSS will generally be referred to as the Sentry "network access device" or NAD.

Network Access Device TCP/IP Configuration

Before the Sentry can be accessed over a network, the network access device must first be configured with an IP Address, Subnet Mask, and Default Gateway. These instructions explain how to configure the network parameters through either a Modem or Console connection.

Start a session with the Sentry through either the Modem or Console port (follow the Operations Manual). Start this session with a data rate of 9600.

At the "Sentry:" prompt, issue the command "CONNECT NETWORK". This should connect the session to the internal network access device's serial port and display the message "Connection complete".

Press enter multiple times. A version message from the network access device inside the Sentry should be displayed, followed by a 'Login password>' prompt:

```
ServerTech MSSLite Version ST3.6/4(001020)

Login password>
```

Enter the following default `Login password`:

```
access  <Enter>
```

The password is case sensitive. A "`Local_1>`" prompt should appear:

At the "`Local_1>`" command prompt of the network access device, issue the command:

```
SET PRIVILEGED  <Enter>
```

This allows you to log in as a privileged user. A "`Password>`" prompt will be displayed, at which point you must enter the following default `privileged` password:

```
system  <Enter>
```

When the valid password is entered, the command prompt will change to ‘`Local_1>>`’ (two greater than signs), indicating you are in privileged user mode.

From the privileged command prompt, enter the command:

```
CHANGE IPADDRESS xxx.xxx.xxx.xxx  <Enter>
```

Where `xxx.xxx.xxx.xxx` is the IP address that you want to assign to the Sentry.

The CHANGE IPADDRESS command stores the new IP address in the non-volatile memory of the Sentry NAD.

Issue the command:

```
SHOW SERVER  <Enter>
```

On the screen displayed, verify the information entered in the above steps is correct. If the ‘`TCP/IP Gateway:`’ entry is ‘`(undefined)`’, or the ‘`Subnet Mask:`’ is incorrect for your network, you should also issue the following commands:

```
CHANGE GATEWAY xxx.xxx.xxx.xxx  <Enter>
CHANGE SUBNET MASK xxx.xxx.xxx.xxx  <Enter>
```

Where `xxx.xxx.xxx.xxx` are the appropriate IP addresses.

Once you have finished network configuration, to verify the information entered in the above commands, again issue the command:

```
SHOW SERVER <enter>
```

When finished, issue the command:

```
INIT DELAY 0 <enter>
```

This will re-initialize the network access device in the Sentry with the new settings. Wait one minute for the network access device to re-initialize.

Break the connection to the network access device by typing the string sequence “!*LOGIN” followed by Enter. Log back into the Sentry and QUIT. Additionally, the connection will break when the modem is hung up, or the cable is disconnected from the Modem or Console port, or power is cycled to the Sentry.

For other methods of configuring the Network Access Device TCP/IP parameters, refer to the Lantronix web site at www.lantronix.com.

Starting a Session through the Network Access Device:

To start a Sentry session via the TCP/IP network access device, the user must connect a Telnet session to the IP address of the Sentry using `Port 2001`. This is done with the command:

```
telnet xxx.xxx.xxx.xxx 2001  <Enter>
```

Where `xxx.xxx.xxx.xxx` is the IP address that was assigned to the Sentry.

Once the telnet connection is established, the user will be presented with the standard Sentry Login prompt as described earlier in this manual. If the "Username:" prompt is not presented, press the Enter key for one second and then release. This sends a series of carriage returns that will start the Sentry session. From this point forward, the Sentry will respond as described earlier in this manual.

Modifying the Network Access Device Telnet Port

It is possible to change the Telnet port used to connect to the Sentry product via the Network Access Device. By default, a Telnet connection to the default Telnet port (23) connects users to the Network Access Device console. This allows users to enter commands to configure and view the settings of the Network Access Device. To connect to the Sentry product, users connect to Telnet port 2001 as described above. It is possible to change the Telnet port to cause the default Telnet port of 23 to connect to the Sentry product rather than to the Network Access Device console. To change the connection for the default Telnet port (23), you must connect to the Network Access Device console (i.e. Telnet port 23) and use the CHANGE TELNETDEST command. The command is restricted to privileged users (see the previous section for details on logging on and getting into privileged mode). Details of the command follow.

CHANGE TELNETDEST { Console | Serial }

Parameters – specify either Console or Serial where:

"Console" causes Telnet Port 23 connections to connect to the Network Access Device console.

"Serial" causes Telnet Port 23 connections to connect directly to the serial port (which internally connects to the Sentry, just as described above for connecting to Telnet Port 2001).

If the CHANGE TELNETDEST command is used to change the default Telnet connection to the serial port, and then you wish to change the default back to the Network Access Device console, you must connect to Telnet Port 7000. This connection results in a '#' prompt from the Network Access Device. Respond to this prompt with the default login password (i.e. access) to begin a session with the Network Access Device console. You can then use the CHANGE TELNETDEST command to change the Telnet default port (23) back to the console.

Disabling the Network Access Device Inactivity Timeout

When connecting to a Sentry and then using a serial pass through port to connect to another device, the normal Sentry inactivity timeout is not enforced. However, the Network Access Device inactivity timeout remains in effect. If users wish to disable or modify the Network Access Device inactivity timeout, there are two Network Access Device console commands available for this purpose. The first is the CHANGE INACTIVE LOGOUT command. This command is used to enable or disable the inactivity timeout. This command requires privileged user status as described previously. The format of the command is as follows.

```
CHANGE INACTIVE LOGOUT {Enabled | Disabled }
```

Use the “Disabled” parameter to disable the inactive logout timer.

Use the “Enabled” parameter to enable the inactive logout timer.

To change the length of the inactive timer use the CHANGE INACTIVE TIMER command. This command requires privileged user status as described previously. The format of the command is as follows.

```
CHANGE INACTIVE TIMER { XXs | YYYm }
```

The parameter is specified either in seconds (5 to 60) or in minutes (1 to 120). For seconds add an ‘s’ after the number. For minutes add an ‘m’ after the number. The default value is 5 minutes.

Encrypted Telnet Support

Support for encrypted Telnet connections with the Network Access Device is available. Connections can be made from a Win32 PC to the Network Access Device. Win32 connections are established using a Server Technology supplied Telnet application, TCPSCRAM.EXE, available at:

ftp.servertech.com/pub/tcpscram/tcpscram.zip

This program allows a user on a Win32 platform to form an encrypted connection to a Sentry Network Access Device.

The target Network Access Device must be configured with the encryption password. Use the command:

```
CRYPT PASSWORD “xxxxxxx”
```

Note that the password can be up to 7 alphanumeric characters (56-bits) and is case sensitive. To preserve the case of the password it MUST be enclosed in quotes. If the password is not enclosed in quotes, it is automatically converted to all upper case. After entering the encryption password, theNAD unit must be rebooted with the command INIT DELAY 0.

To create a connection, run the program TCPSCRAM.EXE. In the fields provided, check the encryption box, specify the IP address of the Network Access Device, specify the Telnet port to be used for the connection, (i.e.2100 for the NAD console prompt or 2101 for a connection to the Sentry), and specify the encryption password. Note that the password specified in the application must match the password (case sensitive) configured on the Network Access Device itself.

The TCPSCRAM program will then form a connection to the Sentry and all data passed between the PC and the Sentry will be encrypted.

Encrypted connections support a key size of 56 bits.

For more information on the commands described in this section, and/or to view the complete MSS manual and support files see the Lantronix WWW page at http://www.lantronix.com.

Network Access Device SNMP Configuration

The Sentry (with the Network Access Device option) supports the Simple Network Management Protocol (SNMP). For a complete description of the Sentry SNMP support, please refer to the Sentry SNMP Support section of this manual. If SNMP support is required, the following section describes the commands that must be issued on the Network Access Device (i.e. the MSS -- all commands require privileged access).

Login to the MSS as described in the previous section, or by connecting via Telnet to port 23, rather than port 2001. Once connected, enter privileged mode as described in the previous section. The current settings can be viewed with the command: SHOW SENTRY.

The Sentry SNMP support must be enabled for access to Sentry2 MIB objects and for the generation of all Sentry2 traps. The Sentry SNMP support is enabled and disabled in the MSS with the command:

```
SENTRY SNMP { ENABLED | DISABLED }
```

The default is “DISABLED”. .

When the MSS receives a GET/SET SNMP request that requires communication to the Sentry controller board(s), the MSS opens a serial session with the Sentry, during which time other access paths (Modem, Console, Telnet) cannot establish a session with the Sentry. The timeout setting controls how long the MSS-to-Sentry SNMP serial session must be inactive (no longer needed for SNMP request fulfillment) before the session is automatically closed, thus again allowing other access paths.

The Sentry SNMP MSS-to-Sentry session timeout is configured with the command:

```
SENTRY SNMP TIMEOUT { 5 .. 55 }
```

Valid entries are between 5 and 55, which represents the session timeout in seconds.

The default is 15 seconds.

When the MSS receives a GET/SET SNMP request that requires communication to the Sentry controller board(s), the MSS opens a serial session with the Sentry. During that session, the SPEED controls the serial data rate that the Sentry uses for returning responses to query commands from the MSS.

The Sentry SNMP MSS-to-Sentry session speed is configured with the command:

```
SENTRY SNMP SPEED data_rate
```

Valid entries are 300, 1200, 2400, 4800, 9600, 19200, and 38400.

The default is 9600.

There are two commands that control the destination and community string of traps generated by the Sentry, defined below.

The Sentry trap destination is defined in the MSS with the command:

```
SENTRY SNMP TRAPDEST nnn.nnn.nnn.nnn
```

Where nnn.nnn.nnn.nnn is the IP Address of the SNMP management station that will receive all traps. An entry of 0.0.0.0 clears the address, setting it to “(undefined)”.

The default Sentry SNMP trap destination is “(undefined)”.

The trap destination must be configured for traps to be generated.

The Sentry trap community string is defined in the MSS with the command:

```
SENTRY SNMP TRAPCOMM “string”
```

Default = “sentry-trap”

The community string can be between 1 and 15 characters. By enclosing in double quotes, the case is preserved, otherwise it is converted to all uppercase. An entry of “” clears the string.

All traps are sent with this trap community string.

The trap community string must be configured for traps to be generated.

There are three SNMP community strings that provide different levels of access to specific subsets of the objects defined in the Sentry MIB. These community strings are defined below with the commands to configure them. Refer to descriptions in the Sentry MIB (Appendix A) and the Object ID Tree (Appendix B) for further clarification of the objects accessible by each community string.

Note: None of the Sentry community strings should be set to “public”. This is because “public” is the fixed GET community string for the MSS native SNMP support for MIB I, MIB II, and RS232 MIB objects.

The Sentry GET community string is defined in the MSS with the command:

```
SENTRY SNMP GETCOMM “string”
```

The community string can be between 1 and 15 characters. By enclosing in double quotes, the case is preserved, otherwise it is converted to all uppercase. An entry of “” clears the string.

GETCOMM is a string that will give access to the sentry2ChainGroup read-only MIB objects. The use of this string will start a session with the Sentry.

Default = “sentry”

The Sentry SET community string is defined in the MSS with the command:

SENTRY SNMP SETCOMM “string”

The community string can be between 1 and 15 characters. By enclosing in double quotes, the case is preserved, otherwise it is converted to all uppercase. An entry of “” clears the string.

SETCOMM is a string that will give access to the sentry2ChainGroup read-only MIB objects and the read-write sentry2PortPowerAction MIB object. The use of this string will start a session with the Sentry.

Default = “sentry-set”

The SETCOMM community string must be configured for power control operations to succeed.

The Sentry GET community string for extended Sentry error information is defined in the MSS with the command:

SENTRY SNMP ERRCOMM “string”

The community string can be between 1 and 15 characters. By enclosing in double quotes, the case is preserved, otherwise it is converted to all uppercase. An entry of “” clears the string.

ERRCOMM is a string that will give access to the sentry2ErrorGroup read-only MIB objects. The use of this string will NOT start a session with the Sentry.

Default = “sentry-error”

When finished, issue the command:

```
SHOW SENTRY <enter>
```

Verify the settings you have entered are correct, then issue the command:

```
INIT DELAY 0 <enter>
```

To logout and re-initialize the network access device in the Sentry with the new settings. Wait one minute for the network access device to re-initialize.

Network Access Device TACACS+ Configuration

If TACACS support is required, the following section describes the commands that must be issued on the Network Access Device (i.e. the MSS -- all commands require privileged access).

Login to the MSS as described in the previous section, or by connecting via Telnet to port 23, rather than port 2001. Once connected, enter privileged mode as described in the previous section. The current settings can be viewed with the command: SHOW SENTRY.

The Sentry TACACS support is enabled in the MSS by setting the TACACS IP address and defining the TACACS key.

Note: TACACS support is compatible with TACACS PLUS (TACACS+) servers only.

To set the TACACS Plus server IP address issue the following command:

```
SENTRY TACACS SERVER nnn.nnn.nnn.nnn
```

where nnn.nnn.nnn.nnn is the IP Address of the TACACS server that will authenticate telnet connections to the Sentry.

The Sentry TACACS key string is defined in the MSS with the command:

```
SENTRY TACACS KEY “string”
```

The key string should be enclosed in double quotes to ensure the case is preserved. Since the key does not echo, it is important to be sure the key is specified correctly with case being significant. The key must match the key specified on the TACACS server.

The TACACS key can be cleared by entering a null string in double quotes (i.e. “”).

PLEASE NOTE: Once you have enabled TACACS authentication and rebooted the MSS, you will not be able to telnet to the Sentry without successfully completing TACACS authentication. If you enter an invalid key, you will be unable to access the Sentry by Telnet without resetting the MSS. If your TACACS server is unavailable, you will not be able to access the Sentry via telnet (unless Authentication Fallback has been enabled – covered later in this section).

When TACACS is enabled, the standard MSS password protection is redundant, and you will probably want to turn it off. You can leave it on if you want, in which case you will first be prompted for the MSS login password, and then, after a successful entry, will be prompted for the TACACS username/password. To turn off the standard MSS password protection, use the privileged-level MSS commands:

```
CHANGE  INCOMING  NOPASSWORD
CHANGE  PASSWORD  PROTECT  DISABLED
```

When finished, issue the command:

```
SHOW SENTRY <enter>
```

Verify the settings you have entered are correct, then issue the command:

```
INIT DELAY 0 <enter>
```

This will re-initialize the network access device in the Sentry with the new settings. Wait one minute for the network access device to re-initialize.

Network Access Device SecurID Support

SecurID support is available with the Sentry Network Access Device.

SecurID is not enabled by default. It is enabled and configured by several privileged-level MSS commands.

Prior to enabling SecurID, the Sentry unit should be entirely configured and operational. You must also already be familiar with how to log into the MSS and how to set privileged-user mode.

These instructions also assume a thorough understanding of the ACE/Server configuration items and processes.

There are six configurable SecurID parameters: the primary ACE/Server IP address, the secondary (backup) ACE/Server IP address, the SecurID authentication request timeout, the maximum number of authentication request retries, the encryption method, and the SecurID port (TCP/IP socket number).

The current SecurID parameter settings can be displayed by the MSS privileged-level command:

```
SHOW  SENTRY
```

SecurID is enabled if either the primary or secondary ACE/Server IP Addresses is defined. This is done with the MSS privileged-level command:

```
SENTRY  SECURID  { PRIMARY | SECONDARY }  { ipaddress | NONE }
```

Where ipaddress is in decimal numerical form.

NONE removes the ipaddress definition.

Note: changing an ACE/Server IP Address clears the MSS Node Secret.

The other MSS SecurID commands are:

```
SENTRY  SECURID  TIMEOUT  n
```

Where n is the number of seconds between authentication requests retries. Default = 3.

```
SENTRY  SECURID  MAXTRETRY  n
```

Where n is the maximum number of authentication request retries. Default = 5.

```
SENTRY  SECURID  ENCRYPTION  { SID | DES }
```

Where SID or DES selects the encryption method. Default = DES. This must match the client configuration on the ACE/Server. Note: new ACE/Server versions renamed the SID encryption to SDI.

```
SENTRY  SECURID  PORT  nnnnn
```

Where nnnnn is the SecurID authentication socket number. Default = 5500. This must match the port configured on the ACE/Server.

```
SENTRY  SECURID  FACTORY
```

Resets all the SecurID configuration parameters to their factory defaults.

In the ACE/Server Database Administration, create and configure a Sentry client, selecting “Communication Server” as the Client Type. The MSS can perform multiple transactions and therefore can display the Next Tokencode and New PIN prompts.

When SecurID is enabled, the standard MSS password protection is redundant, and you will probably want to turn it off. You can leave it on if you want, in which case you will first be prompted for the MSS login password, and then, after a successful entry, will be prompted for the SecurID username/passcode. To turn off the standard MSS password protection, use the privileged-level MSS commands:

```
CHANGE  INCOMING  NOPASSWORD
CHANGE  PASSWORD  PROTECT  DISABLED
```

Network Access Device Out-Of-Band Authentication Support

The Sentry TACACS and SecurID network authentication support is available to users that connect to the Sentry via either the MODEM port or the CONSOLE port. When users connect to the Sentry via the Network Access Device, the network authentication support is referred to as In-Band authentication support. When TACACS and/or SecurID network authentication is required for users that connect to the Sentry via either the MODEM port or the CONSOLE port, the network authentication support is referred to as Out-Of-Band authentication support. If this feature is desired, it must be enabled on the Sentry. The command to enable this feature on the Sentry is the SET NETAUTH command that is described earlier in this document under the Sentry SET commands. When Out-Of-Band authentication support is enabled, the Sentry automatically makes a connection to the Network Access Device when a user begins a session on either the MODEM or CONSOLE port, and the authentication proceeds using the current authentication protocol.

Network Access Device Authentication Fallback Support

In normal operations with SecurID and TACACS authentication, the user is denied access if it is impossible to authenticate the user because the server is down or the network path to the server is down. To mitigate this situation, the Sentry supports an authentication fallback feature. When the authentication fallback feature is enabled, instead of disallowing access, the user is prompted for a local fallback password when SecurID or TACACS authentication cannot take place because the Network Access Device is unable to communicate with all defined authentication servers. The authentication fallback occurs after all retry attempts fail and all timeouts expire.

The Network Access Device command to enable or disable authentication fallback is:

```
SENTRY AUTHFALLBACK { ENABLED | DISABLED }
```

The default is disabled.

Authentication fallback is a global setting that applies to all access paths that have network authentication enabled.

The fallback password can be defined and changed by the Network Access Device command:

```
SENTRY FALLBACKPASS “fallbackpassword”
```

where “fallbackpassword” is a string from 0 to 16 7-bit characters. To preserve case, the password MUST be enclosed in double-quotes.

Note, when the fallback password is not set (blank; set to “”), and authentication fallback is enabled, if a fallback occurs, access will be allowed without prompting for the fallback password.

The Network Access Device command “SHOW SENTRY” displays the current authentication fallback setting, and whether or not a password has been set.

Additional Network Access Device Security Options

In addition to previously covered Encrypted Telnet, TACACS, and SecurID support, the Sentry network access device uses a two-level password scheme, and supports an IP Address security table.

Passwords and Password Requirements

The Sentry network access device supports two passwords – a Login password and a Privileged password.

The Login password allows a user to log into the NAD, but does not allow configuration changes. The command to change the Login password is:

```
CHANGE LOGINPASS “loginpass”
```

Default = “access”

Once logged in, the Privileged password is used to with the SET PRIV command to become the privileged user (administrator), which is required to change settings of the network access device.

```
CHANGE PRIVPASS “privpass”
```

Default = “system”

Both the Login and Privileged passwords can be made up of 1 to 6 case-insensitive alphanumeric characters. Changing either password requires privileged user status.

The network access device defaults to requiring the Login password when accessing the NAD Console by either Telnet (to Port 23) or serially through the Sentry using the CONNECT NETWORK command. The NAD defaults to not requiring the Login password when accessing the Sentry by Telnet (to port 2001).

These Login password requirements can be changed with the following commands:

To enable or disable the Login password requirement for a Telnet (Port 23) session to the NAD Console, use:

```
CHANGE INCOMING { PASSWORD | NOPASSWORD }
```

Default = “PASSWORD”

To enable or disable the Login password requirement for a serial session through the Sentry to the NAD Console using the CONNECT NETWORK command, use:

```
CHANGE PASSWORD PROTECT { ENABLED | DISABLED }
```

Default = “ENABLED”

To enable or disable the Login password requirement for a Telent (Port 2001) session to the Sentry, use:

```
CHANGE PASSWORD INCOMING { ENABLED | DISABLED }
```

Default = “DISABLED”

Additionally, access to the NAD Console by Telnet (to Port 23) can be enabled or disabled, and the number of password entry attempts for the Login password and Privileged password prompt can be changed.

To enable or disable the NAD Console access by Telnet to Port 23, use:

```
CHANGE INCOMING { NONE | TELNET }
```

Default = “TELNET”

To change the number of password attempts allowed at the Login password and Privileged password prompts, use:

```
CHANGE PASSWORD LIMIT  #
```

Default = 3

IP Security Table

The Sentry network access device also supports an IP Security Table option. IP security allows the system administrator to restrict (allowed or denied) incoming TCP/IP sessions to the NAD console or the Sentry based upon the source IP address.

IP security information can be added to the IP local host table using the CHANGE IPSECURITY command. Specify an address in standard numeric format. An address with 0 or 255 in any segment restricts all addresses in that range.

To add an entry, specify an IP address and whether to allow or deny connections. For example, the following command disables connections for all addresses between 192.0.1.1 and 192.0.1.254.

```
CHANGE IPSECURITY 192.0.1.255 DISABLED
```

The following example disables the address 192.0.220.77.

```
CHANGE IPSECURITY 192.0.220.77 DISABLED
```

The CHANGE IPSECURITY command requires privileged user status.

To view the host table entries, enter the SHOW IPSECURITY command. To remove an entry, use the DELETE IPSECURITY command followed by the IP address that you want to remove.

For more information on the commands described in this section, and/or to view the complete MSS manual and support files see the Lantronix WWW page at http://www.lantronix.com.

Resetting the Network Access Device to Factory Defaults

The non-volatile RAM that stores all configurable Network Access Device options, including the IP Address and passwords, can be reset to factory defaults.

Resetting to factory defaults can be done in two ways – by a privileged-user command at the “Local_n>>” prompt, or by a Reset button press during power up. This second method is necessary if the passwords are forgotten.

A privilege-user command reset is performed with the command:

```
INIT FACTORY
```

This command resets the Network Access Device to factory defaults and reboots the NAD.

A power-up button-press reset is performed as follows:

Important Note: The power-up button-press reset procedure below resets both the Sentry boards and the Network Access Device to factory defaults.

The power up button press reset must be done on the first Sentry at the beginning of a chain. The reset is performed by pressing and holding down the Reset button while turning on power with the On/Off toggle switch. Continue to hold down the Reset button for ten (10) seconds after turning on the power, and then let go.

Note: In the case of Sentry products that do not have a separate reset button, the A1 button on the button panel has a secondary function as a Reset button.

Sentry SNMP Support

The Sentry (with the network access device option) supports the Simple Network Management Protocol (SNMP). This allows a network management system to use SNMP “get” and “set” requests to retrieve information about, and control power to, the individual ports on the Sentry. Properly implemented and integrated, this feature could allow a network management system to automatically reboot a network device that it has detected to be down or locked-up.

The ServerTech MSS includes an SNMP v1 agent that supports the standard MIB I, MIB II, and RS-232 MIB objects. Additionally, the ServerTech MSS and the Sentry together support a private enterprise MIB extension that provides remote power control via SNMP. This collection of private enterprise MIB objects is called the Sentry MIB. For security reasons, the Sentry MIB extensions default to being disabled.

The Sentry MIB defines objects that allow a network manager to check the value of Sentry configuration items, to check the power status of individual ports on the Sentry, and to control power to the individual ports on the Sentry. Power to a port can be turned on, turned off, or rebooted. Ports with shutdown support will automatically signal a shut down to the operating system of the attached device prior to turning off or rebooting the device.

In addition to the Sentry SNMP support for the query and action type operations that allow externally originated SNMP actions to be passed to the Sentry from an attached MSS, Sentry SNMP support includes Sentry generated trap information. The trap information is collected at the Sentry and then passed to an attached MSS where it is formatted for SNMP and then delivered to an external SNMP trap destination. The Sentry MIB defines the trap objects that are generated by the Sentry. The Sentry MIB and associated SNMP definitions can be obtained directly from Server Technology via their anonymous FTP site.

The MIB file that defines the Sentry MIB objects, is available over the Internet via anonymous FTP at:

ftp://ftp.servertech.com/pub/SNMP/sentry2

SNMP related email should be directed to: mibmaster@servertech.com

The Sentry SNMP MIBs and OIDs can also be found in the appendix of this manual.

The Sentry SNMP trap support is designed to recognize new trap conditions and transmit messages as soon as possible. To prevent network congestion, trap conditions that remain in a steady state (i.e. in a continuing error condition) generate traps once a minute (by default), though this time can be increased.

Users must be aware of certain limitations that exist in the implementation of the SNMP trap notification design so that user expectations do not exceed the system capabilities. These limitations are:

Traps can only be transmitted when there is no active user session with the Sentry Chain. This means that if a Sentry chain is being used for connection via a pass-through switch to another device, and the user connections are frequent or are of long duration, traps messages will be delayed. Use of a Sentry chain for trap monitoring and for frequent or long duration user sessions is possible but may not be desirable.

Multiple trap conditions may occur with only a single trap message indication. For example, a trap message is sent for each change of state of a power module. If a user logs on and turns a single port on and off several times, only one trap message will be generated (after the user logs off) indicating a change to the current state, although the power module was cycled several times. As another example, if a temperature limit is exceeded then returns to normal and then is exceeded again (this may happen more than once) during an active user session, only a single trap message will be generated (after the user logs off) indicating the current state of the temperature trap.

There are six activities that are monitored by the Sentry in order to generate SNMP traps. Each of these activities and the traps they generate are described in the following sections.

Temperature Limit Exceeded Trap

Each Sentry board in a chain can have a single temperature probe that measures the current temperature at the probe in degrees Celsius. For each board, high and low temperature limits can be set. When these limits are exceeded, an SNMP trap will be generated. When the temperature returns to the normal range (i.e. a temperature within the high and low limits as specified by the user), another SNMP trap is generated. When the temperature first exceeds the specified limits, a high or low temperature error trap is generated as soon as possible. Once the first trap is generated, the trap becomes a steady state trap. A new trap will be generated every trap timer period (one minute by default) when a steady state temperature error trap occurs. When the temperature returns to the normal range and remains in the normal range until the end of the current trap timer period, a normal temperature trap is sent, and the repeating steady state error trap is canceled. The following description illustrates how the temperature trap mechanism is implemented.

For this illustration, the temperature high limit is set at 100 degrees Celsius and the low limit is set at 80 degrees Celsius. If the temperature rises to 101 degrees, a trap is generated and the steady state timer is set. During the steady state timer period the temperature falls to 99 degrees and then rises back to 100 degrees. When the timer expires, a second temperature out of limits trap is generated and the timer is set once again. During this timer period the temperature falls below 100 degrees and stays there until the timer expires. When the timer expires, a temperature normal trap is generated and the timer is not set. The temperature trap is no longer in a steady state and a new trap will not be generated until the temperature once again falls outside the limits.

There are three possible temperature traps that can be generated. They are:

Temperature out of limits high.
Temperature out of limits low.
Temperature in normal range.

All of the Temperature traps include the current Temperature value as indicated by the Sentry board temperature probe, as well as the Sentry location, and the identifier and name of the particular board which detected the trap condition from the connected temperature probe.

Sentry Start Up Trap

When the administrator enables the Sentry Start Up Trap, the Sentry board generates an SNMP trap whenever the board completes a start up. Even if the trap is enabled on all boards in a chain, only the first board will generate a single start up trap when reset. The Start Up trap includes the descriptive Location of the Sentry, as defined with the SET LOCATION command.

Control Status Change Trap

When the administrator enables the Control status Change Trap for an IPM, an SNMP trap is generated whenever the control value of the IPM is changed. If multiple control status change events occur during a period when it is not possible for the Sentry to send traps, only a single trap will be generated indicating the last control status value.

The following example illustrates the Control Status Change Trap. For this illustration the user has activated Control Status Change Traps for all ports on all boards in the Sentry chain. The user logs on to the Sentry and uses the ‘ON’ command to turn on several ports. While the user is logged on to an active session, traps are not sent, so all of the ports that were turned on have pending Control Status Change Traps. During this same session, the user realizes he has made a mistake and wants to start over, so he uses the ‘OFF’ command to turn all ports in the Sentry chain back off. The user then uses the ‘ON’ command to turn on the single port he wishes to leave in the ‘ON’ state. The user then logs off the system. After the user logs off, there will be a single SNMP trap generated for all of the ports in the system. Each trap will indicate the current control status of the port. There will only be a single trap for all ports even though the ports all had more than one control status change.

The Control Status Change trap includes the current Control Status of the port, as well as the Sentry Location, and the identifier and name of the particular port for which the Control Status change occurred.

Module Status Error Trap

When the user enables the Module Status Error Trap for an IPM on a Sentry board, an SNMP trap is generated whenever an error condition occurs on an IPM. Another SNMP trap is generated when the error condition is ended and the IPM returns to a normal state. Like the temperature limits exceeded trap, a steady state condition timer is set after the initial trap, and subsequent traps are generated on a timer expired basis until the module returns to the normal state and remains in the normal state until the end of the current trap timer period.

The four Module Status states that an IPM may have are:

Normal – the IPM is functioning normally.
No Response – the Sentry is unable to communicate with the IPM.
On Failure – the IPM is set to ON, but there is no power detected on the output side of the relay.
Off Failure – the IPM is set to OFF, but there is power detect on the output side of the relay.

The Module Status Error traps include the current Module Status of the port, as well as the Sentry Location, and the identifier and name of the particular port for which the Module Status error occurred.

Device Load Error Trap

Each of the IPMs attached to a Sentry board may have the ability to sense the power load flowing through the IPM. For each IPM on a Sentry board, high and low Device Load limits can be set. When these Device Load limits are exceeded, an SNMP trap will be generated. When the Device Load returns to the normal range (i.e. within the high and low limits as specified by the user), another SNMP trap is generated. When the Device Load first exceeds the specified limits, a trap is generated as soon as possible. Like the temperature limits exceeded trap, a steady state condition timer is set after the initial trap, and subsequent traps are generated on a timer expired basis until the Device Load returns to the normal range and remains in the normal range until the end of the current trap timer period.

There are three possible Device Load traps that can be generated. They are:

Device Load out of limits high..
Device Load out of limits low
Device Load in normal range.

All of the Device Load traps include the current Device Load value as indicated by the IPM, as well as the Sentry Location, and the identifier and name of the particular port which detected the Device Load trap condition from the connected IPM.

Input Load Error Trap

The Sentry external Power Tower products support the ability to sense the total load current that is flowing through the Power Tower. This value represents the total amount of current being drawn by all of the devices attached to the Power Tower. The Sentry supports the setting of Input current high and low limits. When these Input Load current limits are exceeded, an SNMP trap will be generated. When the Input Load current returns to the normal range (i.e. within the high and low limits as specified by the user), another SNMP trap is generated. When the Input Load current first exceeds the specified limits, a trap is generated as soon as possible. Like the temperature limits exceeded trap, a steady state condition timer is set after the initial trap, and subsequent traps are generated on a timer expired basis until the Input Load returns to the normal range and remains in the normal range until the end of the current trap timer period.

There are three possible Input Load current traps that can be generated. They are:

Input Load current out of limits high.
Input Load current out of limits low.
Input Load current in normal range.

All of the traps include the present Input Load current value as indicated by the IPM, as well as the Sentry Location, and the identifier and name of the particular board which detected the Input Load trap condition from the connected Power Tower.

Not all Sentry products support this feature. The input load current feature is only available on the Sentry external Power Tower product.

Sentry Shutdown and Windows NT UPS Service Configuration

Windows NT must be shut down prior to turning off power. When a user is at the computer, the user can manually perform the necessary shutdown. However, if the Windows NT system is used as an unattended or remote mission-critical server, the user is not at the computer to perform a shutdown prior to a remote power off or reboot action.

The Sentry Remote Power Control products solve this problem by providing a Shut Down notification for each system controlled by an individual Intelligent Power Module. When the optional Shut Down notification feature is present, the Sentry will automatically send a Shut Down signal to the operating system whenever an IPM is instructed to power off or reboot. A user-defined "Shutdown Delay" timer decrements as the shutdown signal is asserted. This delay allows the operating system time to shut down the system in an orderly manner. When the delay time expires, power is immediately turned off. The length of the Sentry "Shutdown Delay" is determined by the "Shutdown Delay" field on the Sentry Power Control Screen, as described earlier in this manual.

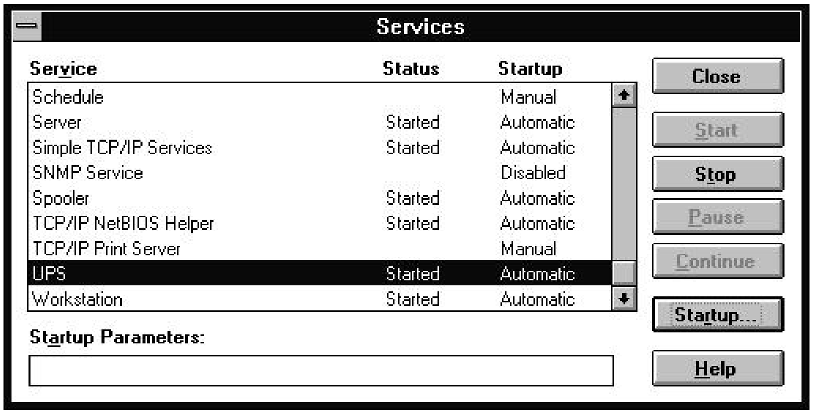
The mechanism for attaching the Sentry to the Windows NT system depends on the specific Sentry hardware model you have purchased. Please refer to the Sentry Installation and Setup manual that is included with your Sentry product for details on connecting your Sentry product to your Windows NT system.

Windows NT provides a UPS Service to monitor a serial port for the shutdown signal, and to provide the operating system shutdown when the signal is asserted.

There are two parts to configuring the Windows NT UPS Service for use with the Sentry:
Configuring the service to automatically startup when Windows NT loads.
Configuring the service for the proper COM port and operating parameters of the Sentry.

Both parts of the configuration are done through the "Services" and "UPS" icons in the Control Panel of Windows NT. The following screen shots show the required setting. See the on-line help for more information about each item on the screens.

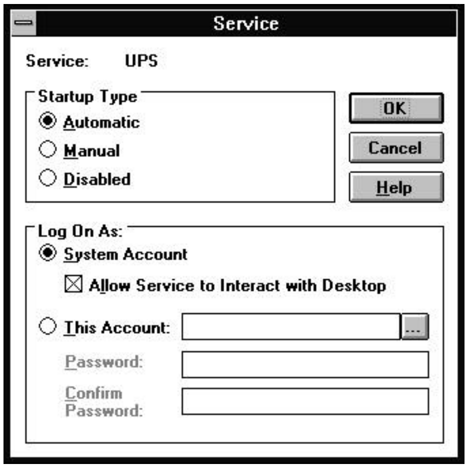
To configure the UPS service to automatically startup when Windows NT loads, select "Services" from the Control Panel. The Services window will be displayed:



Service	Status	Startup
Schedule		Manual
Server	Started	Automatic
Simple TCP/IP Services	Started	Automatic
SNMP Service		Disabled
Spooler	Started	Automatic
TCP/IP NetBIOS Helper	Started	Automatic
TCP/IP Print Server		Manual
UPS	Started	Automatic
Workstation	Started	Automatic

Startup Parameters:

Click on “UPS” and then the “Startup” button. The UPS Service startup parameters will be displayed:



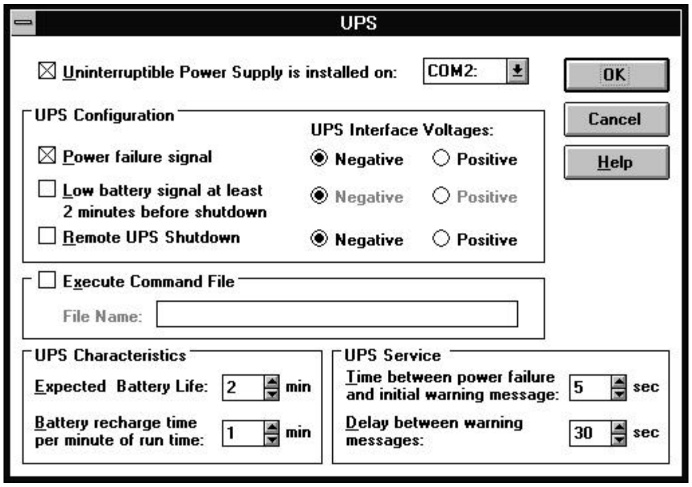
Service: UPS

Startup Type
● Automatic
○ Manual
○ Disabled

Log On As:
● System Account
☒ Allow Service to Interact with Desktop
○ This Account:
Password:
Confirm Password:

Choose the options shown above, and then click OK.

To configure the UPS Service for the proper COM port and operating parameters of the Sentry, select “UPS” from the Control Panel. The UPS window will be displayed:



☒ Uninterruptible Power Supply is installed on: COM2:

UPS Configuration

	UPS Interface Voltages:	
☒ Power failure signal	● Negative	○ Positive
☐ Low battery signal at least 2 minutes before shutdown	● Negative	○ Positive
☐ Remote UPS Shutdown	● Negative	○ Positive

☐ Execute Command File
File Name:

UPS Characteristics
Expected Battery Life: 2 min
Battery recharge time per minute of run time: 1 min

UPS Service
Time between power failure and initial warning message: 5 sec
Delay between warning messages: 30 sec

Selected the appropriate COM port and choose the other options as shown above, then click OK.
The value for the “Expected Battery Life” shown in the above screen shot is 2 minutes. This is the default setting in Windows NT and is also the minimum setting that Windows NT allows. The Sentry shutdown delay is configured on the Sentry Power Control screen via the “Shutdown Delay” field.

IMPORTANT: The “Expected Battery Life” must be less than the “Shutdown Delay” time configured on the Sentry Power Control, otherwise, power may be turned off before the Windows NT system has completed the shutdown.

When set for two minutes, the Windows NT system will start to shutdown immediately when the Sentry signals it to -- there is no “grace” time or initial warning messages, just a final shutdown message and then the actual shutdown. For this reason, you may want to increase the “Expected Battery Life” on the Windows NT UPS configuration screen and the “Shutdown Delay” on the Sentry Power Control Screen.

Every minute above 2 minutes will be time that Windows NT will broadcast and display warning messages about the impending shutdown, before starting the final shutdown. This gives users time to finish and save their work before the shutdown occurs.

When Windows NT boots, a user is expected to press <Ctrl><Alt><Del> to bring up the logon dialog box from which the user will login with their user name and password. This can pose a problem for remote booting and logon since the user is not at the system to press the keys.

Fortunately, Windows NT supports an Automatic Logon feature to allow the system to automatically logon with a default user name, default password, and default domain name. Instructions for enabling this Automatic Logon feature can be obtained from Microsoft's Knowledge Base section of their WWW pages:

```
http://support.microsoft.com/support/kb/articles/q97/5/97.asp
Article ID #: Q97597
Title: "How to Enable Automatic Logon in Windows NT"
```

Support and Warranty

Support

Server Technology, Inc. provides free product support between 8:30AM and 5:00 PM Pacific Time, Monday-Friday at the following Reno, Nevada, USA phone number:

(775) 284-2000

Server Technology, Inc. also has an e-mail address for support issues:

support@servertech.com

Warranty

Server Technology, Inc. extends a one-year limited warranty, from the date of purchase.

This warranty covers defects in material and workmanship for the Sentry Remote Power Manager under normal use and service, and any failure to perform substantially in accordance with this User's Manual.

This warranty does not cover any failure, which results from accident, abuse, misapplication or alternation. Incidental and consequential damages are not covered by this warranty and are not the responsibility of Server Technology, Inc.

For warranty issues, contact the Product Support Department at the number listed above. All repair and return shipments must be approved by Server Technology and must be accompanied by an RMA (return merchandise authorization) number and dated proof of purchase.

Appendix A - Sentry MIB

The following appendix is the Sentry2 SMIv2 SNMP MIB. The SMIv1 MIB can be obtained from the Server Technology FTP site as described earlier.

```
--
--  Copyright(C) 1999 Server Technology, Inc.
--

    Sentry2-MIB DEFINITIONS ::= BEGIN

    IMPORTS
        MODULE-IDENTITY, NOTIFICATION-TYPE,
        OBJECT-TYPE, Integer32, enterprises             FROM SNMPv2-SMI
        DisplayString, TEXTUAL-CONVENTION               FROM SNMPv2-TC;


    sentry2RemotePowerManager MODULE-IDENTITY
        LAST-UPDATED "0009251200Z" -- 25 Sep 2000
        ORGANIZATION "Server Technology, Inc."
        CONTACT-INFO
            "Server Technology, Inc.
             1040 Sandhill Drive
             Reno, NV 89511
             Tel: (775) 284-2000
             Fax: (775) 284-2065
             Email: mibmaster@servertech.com"
        DESCRIPTION
            "This is the MIB module for the second generation of the
             Sentry Remote Power Manager product family, which includes
             'Temperature-Sense', 'On-Sense', and 'Load-Sense' support.

             All products in the Sentry product family provide remote
             power control.  The basic element of control is a power
             module 'port'.  Up to four ports (1-4) are present on each
             power control circuit 'board'.  Up to twenty-six boards
             (A-Z) can be linked together in a 'chain'.

             Different community strings are used in the SNMP protocol
             to provide access to two mutually exclusive subsets of
             objects defined in this MIB.  Two community strings, one
             for read-only access and one for read-write access, allow
             access to the sentry2ChainGroup objects.  A third community
             string allows read-only access to the sentry2ErrorGroup
             objects.  Notifications (traps) are sent with a fourth
             community string.

             All Sentry network options, including enabling SNMP support,
             configuring the community strings, and defining the trap
             destination, are configurable through a telnet session to
             port 23.
            All Sentry power control options, including the naming of
            devices, the setting of trap threshold levels, and the
            enabling or disabling of specific traps, are configurable
            through a telnet session to port 2001.  A telnet session to
            port 2001 is an alternate method of accessing, configuring,
            and controlling the Sentry."
        REVISION "0009251200Z" -- 25 Sep 2000
        DESCRIPTION
            "Second revision.  Added the sentry2BoardInputLoad object
            and the sentry2BoardInputLoad High, Low, and Normal traps."
        REVISION "9912081100Z" -- 8 Dec 1999
        DESCRIPTION
            "First revision.  Added the sentry2ChainLocation object to
            the sentry2Board and sentry2Port traps."
        REVISION "9910051600Z" -- 5 Oct 1999
        DESCRIPTION
            "Initial release version."
       ::= { serverTech 2 }

    serverTech OBJECT IDENTIFIER ::= { enterprises 1718 }

    Sentry2BoardId ::= TEXTUAL-CONVENTION
        DISPLAY-HINT "1a"
        STATUS      current
        DESCRIPTION
            "A Sentry board in a Sentry chain is identified as
                 <a>
             where <a> is an upper-case letter in the range of A-Z.

             Examples of Sentry2BoardId are 'A' and 'C'."
        SYNTAX DisplayString(SIZE(1))

    Sentry2PortId ::= TEXTUAL-CONVENTION
        DISPLAY-HINT "2a"
        STATUS      current
        DESCRIPTION
            "A Sentry port in a Sentry chain is identified as
                 <a><n>
             where <a> is an upper case letter in the range of A-Z
             and <n> is a number in the range of 1-4.

             Examples of the Sentry2PortId are 'A1' and 'C4'."
        SYNTAX DisplayString(SIZE(2))


    sentry2ChainGroup   OBJECT IDENTIFIER ::= { sentry2RemotePowerManager 1}
    sentry2ErrorGroup   OBJECT IDENTIFIER ::= { sentry2RemotePowerManager 2}

--
--  Chain Group and Objects
--

    sentry2ChainLocation OBJECT-TYPE
        SYNTAX      DisplayString(SIZE(0..32))
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The location or name of the chain."
        ::= { sentry2ChainGroup 1 }
```

```
sentry2ChainLastBoard OBJECT-TYPE
    SYNTAX      Sentry2BoardId
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "An upper-case letter identifying the last board in
         a Sentry chain.  The value of Sentry2BoardId and the
         first octet of Sentry2PortId have a valid range of
         'A' to the value returned for this object."
    ::= { sentry2ChainGroup 2 }

--
--  Board Table and Objects
--

sentry2BoardTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF Sentry2BoardEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of Sentry board entries."
    ::= { sentry2ChainGroup 3 }

sentry2BoardEntry OBJECT-TYPE
    SYNTAX      Sentry2BoardEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A set of attributes for a conceptual row of
         sentry2BoardTable."
    INDEX       { sentry2BoardIndex }
    ::= { sentry2BoardTable 1 }

Sentry2BoardEntry ::= SEQUENCE {
    sentry2BoardIndex           Sentry2BoardId,
    sentry2BoardPageName        DisplayString,
    sentry2BoardCodeVersion     DisplayString,
    sentry2BoardTemperature     DisplayString,
    sentry2BoardInputLoad       DisplayString
}

sentry2BoardIndex OBJECT-TYPE
    SYNTAX      Sentry2BoardId
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The unique identifier of the board."
    ::= { sentry2BoardEntry 1 }

sentry2BoardPageName OBJECT-TYPE
    SYNTAX      DisplayString(SIZE(0..24))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The name of the board."
    ::= { sentry2BoardEntry 2 }
```

```
sentry2BoardCodeVersion OBJECT-TYPE
    SYNTAX      DisplayString(SIZE(0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The version of the application code that the board is
         running."
    ::= { sentry2BoardEntry 3 }

sentry2BoardTemperature OBJECT-TYPE
    SYNTAX      DisplayString(SIZE(0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The value from the temperature sensor attached to the
         board."
    ::= { sentry2BoardEntry 4 }

sentry2BoardInputLoad OBJECT-TYPE
    SYNTAX      DisplayString(SIZE(0..12))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current load (amperage) measured at the single
         power input to one or more power modules controlled
         by the board.  This value represents the load of all
         devices powered by the single power input."
    ::= { sentry2BoardEntry 5 }

--
--  Port Table and Objects
--

sentry2PortTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF Sentry2PortEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of Sentry port entries."
    ::= { sentry2ChainGroup 4 }

sentry2PortEntry OBJECT-TYPE
    SYNTAX      Sentry2PortEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A set of attributes for a conceptual row of
         sentry2PortTable."
    INDEX       { sentry2PortIndex }
    ::= { sentry2PortTable 1 }

Sentry2PortEntry ::= SEQUENCE {
    sentry2PortIndex            Sentry2PortId,
    sentry2PortPowerAction      INTEGER,
    sentry2PortDeviceName       DisplayString,
    sentry2PortControlStatus    DisplayString,
    sentry2PortModuleStatus     DisplayString,
    sentry2PortDeviceLoad       DisplayString
}
```

```
sentry2PortIndex OBJECT-TYPE
    SYNTAX      Sentry2PortId
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The unique identifier of the port."
    ::= { sentry2PortEntry 1 }

sentry2PortPowerAction OBJECT-TYPE
    SYNTAX      INTEGER {
                    powerOff(1),
                    powerOn(2),
                    reboot(3),
                    noop(4)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "This object is used to change sentry2PortControlStatus.
         Setting this object to 'powerOff' causes the port to
         turn power off to the attached device.  Setting this
         object to 'powerOn' causes the port to turn power on to
         the attached device.  Setting this object to 'reboot'
         causes the port to turn power off to the attached device,
         delay for the configured minimum-off time or 15 seconds,
         whichever is greater, and then turn power back on to the
         attached device.

         The actual operational effect may be delayed as a result
         of the pre-configured minimum-off time, minimum-on time,
         or shutdown delay.

         A snmp get of this object returns 'noop'."
    ::= { sentry2PortEntry 2 }

sentry2PortDeviceName OBJECT-TYPE
    SYNTAX      DisplayString(SIZE(0..24))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The name of the device attached to the power module."
    ::= { sentry2PortEntry 3 }

sentry2PortControlStatus OBJECT-TYPE
    SYNTAX      DisplayString(SIZE(0..12))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current status of the power control signal to the
         power module."
    ::= { sentry2PortEntry 4 }

sentry2PortModuleStatus OBJECT-TYPE
    SYNTAX      DisplayString(SIZE(0..12))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current operational status of the power module."
    ::= { sentry2PortEntry 5 }
    sentry2PortDeviceLoad OBJECT-TYPE
        SYNTAX      DisplayString(SIZE(0..12))
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The current load (amperage) of the device attached to
             the power module."
        ::= { sentry2PortEntry 6 }

--
--  Error Group and Objects
--

    sentry2ErrorReqId OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object contains the request-id of the most recent
             SNMP operation which returned an error-status of genErr."
        ::= { sentry2ErrorGroup 1 }

    sentry2ErrorCode OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This object contains a value identifying a particular
             error which occurred when processing the SNMP operation
             identified by sentry2ErrorReqId:

                Value   Error
                  100   Port not available
                  200   Link command timeout
                  210   Link command negative response
                  220   Link command invalid response
                  240   Last Board Query command failure
                  300   Query command failure
                  400   Operation command timeout
                  410   Operation command negative response
                  420   Operation command invalid response
                 1000   Session unexpectedly lost

             An expanded definition of these error codes may be
             obtained from Server Technology, Inc."
        ::= { sentry2ErrorGroup 2 }

--
--  Notifications
--

    sentry2NotificationGroup    OBJECT IDENTIFIER ::=
        { sentry2RemotePowerManager 100 }

    sentry2Events   OBJECT IDENTIFIER ::= { sentry2NotificationGroup 0 }
    -- the 0 is for V1 compatibility

    -- Chain Specific Traps
```

```
sentry2ChainStart NOTIFICATION-TYPE
    OBJECTS { sentry2ChainLocation }
    STATUS    current
    DESCRIPTION
        "This event is sent when the Sentry has completed the
         application-code boot process.  This can occur from
         either a power up or a resynchronization of the Sentry
         chain."
    ::= { sentry2Events 1 }

-- Board Specific Traps

sentry2BoardTemperatureHighError NOTIFICATION-TYPE
    OBJECTS { sentry2ChainLocation,
              sentry2BoardIndex,
              sentry2BoardPageName,
              sentry2BoardTemperature
            }
    STATUS    current

    DESCRIPTION
        "This event is sent when the value from a temperature
         sensor attached to a Sentry board is above a pre-
         configured high threshold level.

         This trap is repeated periodically while the error
         condition exists."
    ::= { sentry2Events 2 }

sentry2BoardTemperatureLowError NOTIFICATION-TYPE
    OBJECTS { sentry2ChainLocation,
              sentry2BoardIndex,
              sentry2BoardPageName,
              sentry2BoardTemperature
            }
    STATUS    current

    DESCRIPTION
        "This event is sent when the value from a temperature
         sensor attached to a Sentry board is below a pre-
         configured low threshold level.

         This trap is repeated periodically while the error
         condition exists."
    ::= { sentry2Events 3 }

sentry2BoardTemperatureNormal NOTIFICATION-TYPE
    OBJECTS { sentry2ChainLocation,
              sentry2BoardIndex,
              sentry2BoardPageName,
              sentry2BoardTemperature
            }
    STATUS    current

    DESCRIPTION
        "This event is sent when the value from a temperature
         sensor attached to a Sentry board returns to the normal
         range within the pre-configured high and low threshold
         levels, after having been above or below the threshold
         levels."
    ::= { sentry2Events 4 }
```

```
sentry2BoardInputLoadHighError NOTIFICATION-TYPE
    OBJECTS { sentry2ChainLocation,
              sentry2BoardIndex,
              sentry2BoardPageName,
              sentry2BoardInputLoad
            }
    STATUS    current

    DESCRIPTION
        "This event is sent when the value from the input load
         sensor of a Sentry board is above a pre-configured
         high threshold level.

         This trap is repeated periodically while the error
         condition exists."
    ::= { sentry2Events 11 }

sentry2BoardInputLoadLowError NOTIFICATION-TYPE
    OBJECTS { sentry2ChainLocation,
              sentry2BoardIndex,
              sentry2BoardPageName,
              sentry2BoardInputLoad
            }
    STATUS    current

    DESCRIPTION
        "This event is sent when the value from the input load
         sensor of a Sentry board is below a pre-configured
         low threshold level.

         This trap is repeated periodically while the error
         condition exists."
    ::= { sentry2Events 12 }

sentry2BoardInputLoadNormal NOTIFICATION-TYPE
    OBJECTS { sentry2ChainLocation,
              sentry2BoardIndex,
              sentry2BoardPageName,
              sentry2BoardInputLoad
            }
    STATUS    current

    DESCRIPTION
        "This event is sent when the value from the input load
         sensor of a Sentry board returns to the normal range
         within the pre-configured high and low threshold
         levels, after having been above or below the
         threshold levels."
    ::= { sentry2Events 13 }

-- Port Specific Traps

sentry2PortControlStatusChange NOTIFICATION-TYPE
    OBJECTS { sentry2ChainLocation,
              sentry2PortIndex,
              sentry2PortDeviceName,
              sentry2PortControlStatus
            }
    STATUS    current
```

```
        DESCRIPTION
            "This event is sent if the control status of a Sentry
             port has changed one-or-more times since the last
             notification period.  For example, a Sentry port has
             been turned on, off, shutdown, or rebooted.  The
             current control status at the time of the notification
             is included."
        ::= { sentry2Events 5 }

    sentry2PortModuleStatusError NOTIFICATION-TYPE
        OBJECTS { sentry2ChainLocation,
                  sentry2PortIndex,
                  sentry2PortDeviceName,
                  sentry2PortModuleStatus
                }
        STATUS    current
        DESCRIPTION
            "This event is sent when the module status of a
             Sentry port indicates an error condition.

             This trap is repeated periodically while the error
             condition exists."
        ::= { sentry2Events 6 }

    sentry2PortModuleStatusNormal NOTIFICATION-TYPE
        OBJECTS { sentry2ChainLocation,
                  sentry2PortIndex,
                  sentry2PortDeviceName,
                  sentry2PortModuleStatus
                }
        STATUS    current
        DESCRIPTION
            "This event is sent when the module status of a
             Sentry port returns to normal after being in an
             error condition."
        ::= { sentry2Events 7 }

    sentry2PortDeviceLoadHighError NOTIFICATION-TYPE
        OBJECTS { sentry2ChainLocation,
                  sentry2PortIndex,
                  sentry2PortDeviceName,
                  sentry2PortDeviceLoad
                }
        STATUS    current
        DESCRIPTION
            "This event is sent when the value from the load
             sensor of a Sentry port is above a pre-configured
             high threshold level.

             This trap is repeated periodically while the error
             condition exists."
        ::= { sentry2Events 8 }
    sentry2PortDeviceLoadLowError NOTIFICATION-TYPE
        OBJECTS { sentry2ChainLocation,
                  sentry2PortIndex,
                  sentry2PortDeviceName,
                  sentry2PortDeviceLoad
                }
        STATUS    current
        DESCRIPTION
            "This event is sent when the value from the load
             sensor of a Sentry port is below a pre-configured
             low threshold level.

             This trap is repeated periodically while the error
             condition exists."
        ::= { sentry2Events 9 }

    sentry2PortDeviceLoadNormal NOTIFICATION-TYPE
        OBJECTS { sentry2ChainLocation,
                  sentry2PortIndex,
                  sentry2PortDeviceName,
                  sentry2PortDeviceLoad
                }
        STATUS    current

        DESCRIPTION
            "This event is sent when the value from the load
             sensor of a Sentry port returns to the normal range
             within the pre-configured high and low threshold
             levels, after having been above or below the
             threshold levels."
        ::= { sentry2Events 10 }

END
```

Appendix B - Sentry OID Tree

```
ServerTech Sentry2 MIB Object-Id Tree

-- created from sentry2RemotePowerManager (0009251200Z)

serverTech(enterprises 1718)    1.3.6.1.4.1.1718
|                                              |
+--sentry2RemotePowerManager(2)                +- .2
   |                                               |
   +--sentry2ChainGroup(1)                         +- .1
   |  |                                            |   |
   |  +--sentry2ChainLocation(1) *                 |   +- .1 .0
   |  |                                            |   |
   |  +--sentry2ChainLastBoard(2) *                |   +- .2 .0
   |  |                                            |   |
   |  +--sentry2BoardTable(3)                      |   +- .3
   |  |  |                                         |   |   |
   |  |  +--sentry2BoardEntry(1)                   |   |   +- .1
   |  |     |                                      |   |       |
   |  |     +--sentry2BoardIndex(1)                |   |       +- .1
   |  |     |                                      |   |       |
   |  |     +--sentry2BoardPageName(2) *           |   |       +- .2 .<a>
   |  |     |                                      |   |       |
   |  |     +--sentry2BoardCodeVersion(3) *        |   |       +- .3 .<a>
   |  |     |                                      |   |       |
   |  |     +--sentry2BoardTemperature(4) *        |   |       +- .4 .<a>
   |  |     |                                      |   |       |
   |  |     +--sentry2BoardInputLoad(5) *          |   |       +- .5 .<a>
   |  |                                            |   |
   |  +--sentry2PortTable(4)                       |   +- .4
   |     |                                         |       |
   |     +--sentry2PortEntry(1)                    |       +- .1
   |        |                                      |           |
   |        +--sentry2PortIndex(1)                 |           +- .1
   |        |                                      |           |
   |        +--sentry2PortPowerAction(2) * +       |           +- .2 .<a> .<n>
   |        |                                      |           |
   |        +--sentry2PortDeviceName(3) *          |           +- .3 .<a> .<n>
   |        |                                      |           |
   |        +--sentry2PortControlStatus(4) *       |           +- .4 .<a> .<n>
   |        |                                      |           |
   |        +--sentry2PortModuleStatus(5) *        |           +- .5 .<a> .<n>
   |        |                                      |           |
   |        +--sentry2PortDeviceLoad(6) *          |           +- .6 .<a> .<n>
   |                                               |
   |                                               |
   +--sentry2ErrorGroup(2)                         +- .2
   |  |                                            |   |
   |  +--sentry2ErrorReqId(1) **                   |   +- .1 .0
   |  |                                            |   |
   |  +--sentry2ErrorCode(2) **                    |   +- .2 .0
   |                                               |
   |                                               |
   +--sentry2NotificationGroup(100)                +- .100
      |                                                  |
      +--sentry2Events(0)                                +- .0
```

```
         |                                                   |
         +--sentry2ChainStart(1)                             +- .1
         |                                                   |
         +--sentry2BoardTemperatureHighError(2)              +- .2
         |                                                   |
         +--sentry2BoardTemperatureLowError(3)               +- .3
         |                                                   |
         +--sentry2BoardTemperatureNormal(4)                 +- .4
         |                                                   |
         +--sentry2PortControlStatusChange(5)                +- .5
         |                                                   |
         +--sentry2PortModuleStatusError(6)                  +- .6
         |                                                   |
         +--sentry2PortModuleStatusNormal(7)                 +- .7
         |                                                   |
         +--sentry2PortDeviceLoadHighError(8)                +- .8
         |                                                   |
         +--sentry2PortDeviceLoadLowError(9)                 +- .9
         |                                                   |
         +--sentry2PortDeviceLoadNormal(10)                  +- .10
         |                                                   |
         +--sentry2BoardInputLoadHighError(11)               +- .11
         |                                                   |
         +--sentry2BoardInputLoadLowError(12)                +- .12
         |                                                   |
         +--sentry2BoardInputLoadNormal(13)                  +- .13

* SNMP GET requests operate on these leafs with the SENTRY SNMP GETCOMM
  community string.

+ SNMP SET requests operate on this leaf with the SENTRY SNMP SETCOMM
  community string.

** SNMP GET requests operate on these leafs with the SENTRY SNMP ERRCOMM
   community string.

<a> = 65 to 90 ("A" to "Z")

<n> = 49 to 52 ("1" to "4")

SET request variable bindings for sentry2PortPowerAction:

   1 = powerOff
   2 = powerOn
   3 = reboot
   4 = noop
```

Notes

Server Technology, Inc.

1040 Sandhill Drive, Reno, NV 89511 • (775) 284-2000 • Fax: (775) 284-2000
E-mail: sales@servertech.com • World Wide Web: http://www.servertech.com