

---

# **Sentry**

## **Remote Power Manager**

- R2xx
- R4xx
- 48xx
- 72xx

**Installation and Operations Manual**

**Instructions**

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

**Dangerous Voltage**

This symbol is intended to alert the user to the presence of un-insulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

**Protective Grounding Terminal**

This symbol indicates a terminal that must be connected to earth ground prior to making any other connections to the equipment.

**Life-Support Policy**

As a general policy, Server Technology does not recommend the use of any of its products in the following situations:

- life-support applications where failure or malfunction of the Server Technology product can be reasonably expected to cause failure of the life-support device or to significantly affect its safety or effectiveness.
- direct patient care.

Server Technology will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to Server Technology that:

- the risks of injury or damage have been minimized,
- the customer assumes all such risks, and
- the liability of Server Technology is adequately protected under the circumstances.

The term life-support device includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief or other purposes), auto-transfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults or infants), anesthesia ventilators, infusion pumps, and any other devices designated as "critical" by the U.S. FDA.

**Compliance**

Sentry Remote Power Managers have been safety tested/certified to the following standards:

AC voltage models: USA and Canada to UL 508 and CAN/CSA 22.2 No. 205  
European Union to EN60950:2000

DC voltage models: USA and Canada to UL 60950:2000 and CAN/CSA 22.2 No. 60950-00  
European Union to EN60950:2000

**USA Notification**

Warning: Changes or modifications to these units not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment under FCC rules.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

**Canadian Notification**

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

**Japanese Notification**

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

---

# Table of Contents

<b>CHAPTER 1: INTRODUCTION</b>	<b>1</b>
Features and Benefits .....	2
Technical Support .....	3
Quick Start Guide.....	3
<b>CHAPTER 2: INSTALLATION</b>	<b>5</b>
Common Accessories.....	6
Additional Required Items .....	6
Equipment Overview.....	6
Safety Precautions .....	8
Mounting.....	8
Chaining Multiple Sentry Remote Power Managers.....	8
Connecting to the Power Source .....	9
Connecting Devices.....	9
Connecting the Sentry RPM to your network .....	9
<b>CHAPTER 3: OPERATIONS</b>	<b>11</b>
Interfaces .....	12
Port Naming and Grouping .....	12
Usernames and Passwords .....	12
Logging In.....	13
Using the Command Line .....	13
Operations Commands .....	15
Administration Commands .....	20
Using the Control Screen .....	29
<b>CHAPTER 4: APPENDICES</b>	<b>33</b>
Resetting to Factory Defaults.....	35
Technical Specifications .....	36
Network Access Device .....	46
Modem .....	63
Sentry Shutdown .....	69
SNMP.....	72
External Intelligent Power Modules.....	78
R480-0-x.....	79
Sentry Any-to-Any Pass Through Switch.....	81
Warranty, Product Registration and Support .....	83



---

---

# Chapter 1: Introduction

<b>FEATURES AND BENEFITS</b>	<b>2</b>
Communication Access Modes .....	2
Power Distribution .....	2
Remote Power Management .....	2
Always-On Architecture.....	2
On-Sense .....	2
Load and Environment Measurement .....	2
Port Grouping.....	2
Security .....	2
User Interfaces and LEDs.....	3
Automatic Timeout .....	3
<b>TECHNICAL SUPPORT</b>	<b>3</b>
<b>QUICK START GUIDE</b>	<b>3</b>

---

# Chapter 1: Introduction

Server Technology Inc.'s family of Sentry™ products provides easy, practical, and secure solutions for power distribution, power management and load-measurement for remote internetworking equipment and branch AC circuits. These products support the elimination of unnecessary trips to remote locations by allowing remote control of the power on/off status for distant critical equipment, minimizing the impact of locked-up devices on mission-critical networks.

## Features and Benefits

Sentry Remote Power Managers (RPM) are available in a wide range of configurations for control of 4 to 24 devices for 100-120V up to 80A, 208-240V AC up to 64A and -48V or -72V DC up to 200A. See *Standard Models* in Technical Specifications.

### Communication Access Modes

Sentry Remote Power Managers are available in various configurations for access. Base models are equipped standard with direct RS-232 Console and out-of-band external modem access. Additionally, options supporting in-band web browser(HTML), Telnet, SNMP management and integrated out-of-band access are available.

### Power Distribution

Each Sentry Remote Power Manager distributes a maximum of 80A AC and 200A DC power (dependant on model) across a maximum of twenty-four attached devices.

### Remote Power Management

Each Sentry Remote Power Manager offers remote control over the power on/off status to a maximum of twenty-four devices and when chained to additional Sentry RPMs, a single connection offers control of a maximum of 104 devices.

### Always-On Architecture

Always-On architecture eliminates a single point of failure in the event of a Sentry logic failure or inadvertent switching off of the Sentry RPM power switch: Attached network devices will not lose power.

### On-Sense

The On Sense feature detects when power is present at the output receptacle of an Intelligent Power Module. This positively confirms when power is present and allows detection of error conditions.

### Load and Environment Measurement

Available on DC voltage Sentry Remote Power Managers the load measurement feature eliminates guesswork by supplying the individual outlet or aggregate operating loads in amperes. This allows on-site technicians to maximize the equipment installed and operated on a circuit without worry. Remote users also may access this information at any time from the Sentry Remote Power Managers command line or control screen interface for improved power measurement, planning and forecasting.

Additionally, monitoring installation environment temperatures is a feature optionally available for most Sentry Remote Power Managers.

### Port Grouping

For operations across multiple attached devices or devices with multiple or redundant power supplies, multiple Sentry Remote Power Manager ports may be assigned a single group name. Changes may then be applied to all ports in the named group with one easy command sequence.

### Security

The Sentry Remote Power Manager ships with three predefined usernames, including an administrator. The administrator may create up to 117 additional usernames, with individualized access to ports and commands. All usernames support password protection. For configurations requiring multiple fully-privileged user, the Sentry Remote Power Manager allows the administrator to grant administrative privileges to other users in the system.

Additional security measures supported include encrypted Telnet, IP-source restriction tables, SecurID, TACACS+ and MD5.

## User Interfaces and LEDs

The Sentry Remote Power Manager features two types of user interfaces: the command line and the control screen. For easy port recognition, both individual ports and port groups may be assigned descriptive names for use in control commands. For the on-site technician, LEDs on the Sentry Remote Power Manager indicate individual port power status.

## Automatic Timeout

For added system security, a user session will be automatically terminated after five minutes of inactivity; if a user is called away unexpectedly, an unprotected channel will not remain open indefinitely.

## Technical Support

Server Technology understands that there are often questions when installing and/or using a new product. Free Technical Support is provided from 8:30 AM to 5:00 PM, Monday-Friday, Pacific Time. See *Technical Support* in Warranty, Product Registration and Support for more information.

Server Technology, Inc.

1040 Sandhill Drive

Reno, Nevada 89521 USA

Tel: 775.284.2000

Fax: 775.284.2065

Web: [www.servertech.com](http://www.servertech.com)

Email: [support@servertech.com](mailto:support@servertech.com)

## Quick Start Guide

The following instructions will help you quickly install and configure your Sentry Remote Power Manager for use on your network. For detailed information on each step, go to the page number listed to the right.

**For your network security, Server Technology strongly recommends the changing of all predefined passwords for Control Screen and Network Access Device access prior to attachment to your network.**

1. Mount the Sentry Remote Power Manager ..... 8
2. Chain multiple Sentry Remote Power Managers..... 8
3. Connect to the power source(s)..... 8
4. Connect the devices to the Remote Power Manager ..... 9
5. Configure the Remote Power Manager ..... 9
  - Log into the Sentry RPM as the Administrator..... 13
  - Resynchronize the Sentry RPM Chain..... 28
  - Change passwords for all predefined users (Admn, Gen1, Gen2) ..... 25
  - Configure location, port and group naming ..... 23
  - Configure port names..... 30
  - Configure group names..... 31
  - Configure new user(s) with port and display access ..... 20
6. Configure the Network Access Device, if equipped ..... 46
  - Log into the Network Access Device ..... 47
  - Change access passwords (Login, priviledged mode). ..... 60
  - Configure all Network Access Device settings..... 46
7. Configure the Integrated Modem, if equipped and as required ..... 63
  - Log into the Integrated Modem ..... 64
  - Change setup password ..... 64
  - Configure all Integrated Modem settings..... 63
8. Connect the Sentry Remote Power Manager to your network ..... 9





---

# Chapter 2: Installation

<b>COMMON ACCESSORIES</b>	<b>6</b>
<b>ADDITIONAL REQUIRED ITEMS</b>	<b>6</b>
<b>EQUIPMENT OVERVIEW</b>	<b>6</b>
<b>SAFETY PRECAUTIONS</b>	<b>8</b>
<b>MOUNTING</b>	<b>8</b>
<b>CHAINING MULTIPLE SENTRY REMOTE POWER MANAGERS</b>	<b>8</b>
<b>CONNECTING TO THE POWER SOURCE</b>	<b>9</b>
<b>CONNECTING DEVICES</b>	<b>9</b>
<b>CONNECTING THE SENTRY RPM TO YOUR NETWORK</b>	<b>9</b>

---

## Chapter 2: Installation

Before installing your Sentry Remote Power Manager, refer to the Packing List included with the unit to ensure that you have all the items shipped with the unit and the additional items listed below required for proper installation.

### Common Accessories

- Mounting bracket hardware: two mounting brackets and four screws
- Input power cords for AC models
- Output power cords for AC models
- DB9-M to DB9-F straight-thru serial cable
- DB9-M to DB25-M external Modem serial cable  
(Models with integrated modem substitute with – RJ11 to RJ 11 crossover cable)
- External temperature probe, if equipped
- Pass-through cable/adaptor kit(s), for models including pass-through support
- Document Library CD-ROM

### Additional Required Items

- Phillips screwdriver
- 10mm socket wrench or nut-driver for DC models
- Screws, washers and nuts to attach the Remote Power Manager to your rack

### Equipment Overview

The Power On/Off switch is used to provide power to the Sentry Remote Power Manager logic. This switch will not turn power off at the outlets unless otherwise noted on the unit. See *Safety Precautions* in Chapter 1: Introduction.

The Console port is used for cable connection to a PC or terminal server. The Modem port is used for cable connection to an external modem. And the Link port is used for cable connection to chained Sentry Remote Power Managers or the Sentry ATA Pass-Through Switch. For more information on the Sentry ATA Pass-Through Switch see 0Sentry Any-to-Any Pass Through Switch.

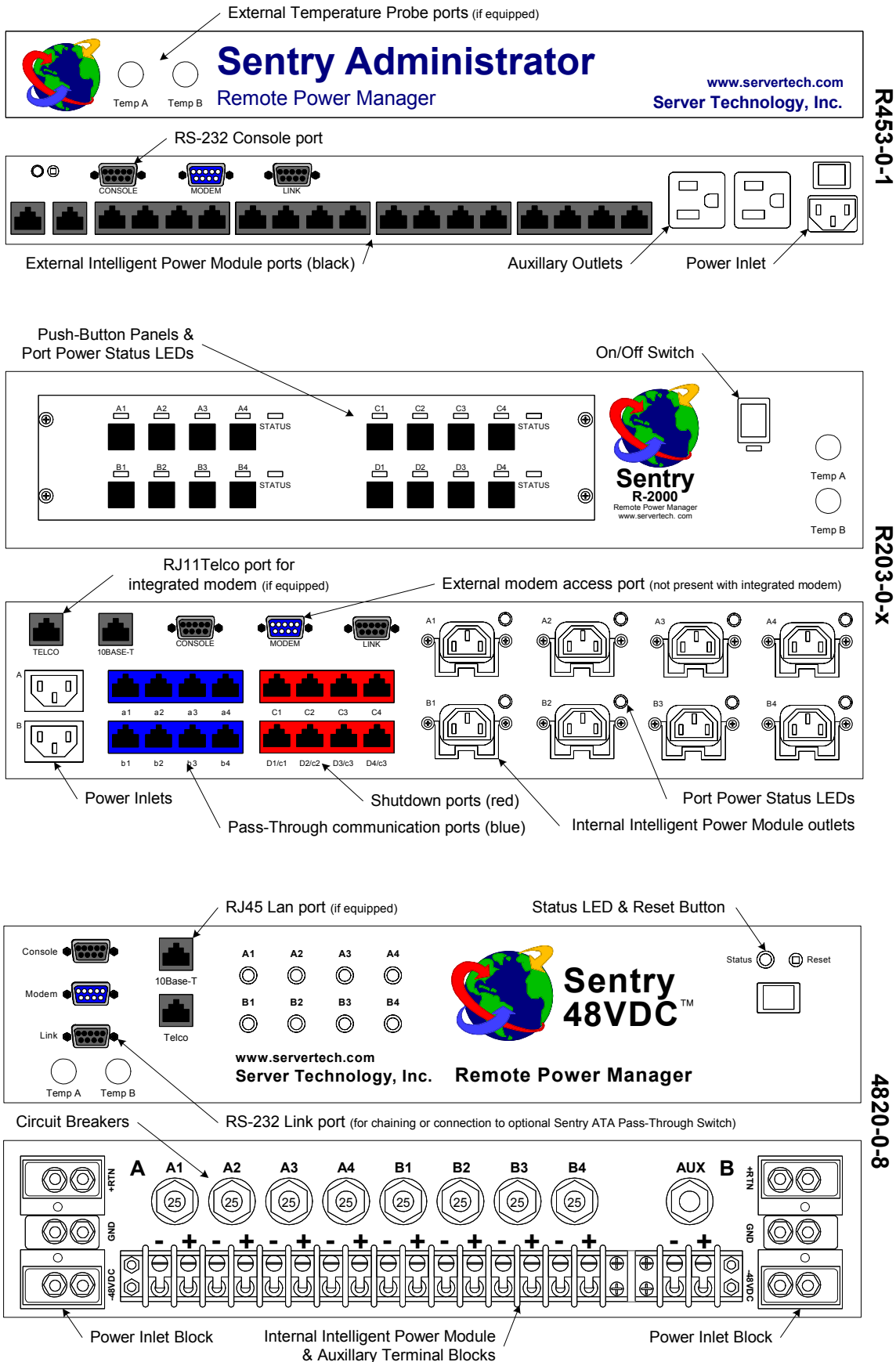
The Telco port is used for cable connection for the optional integrated modem and the 10Base-T port is used for cable connection for the optional integrated LAN. The Temp ports are used for the optional external temperature probes.

Sentry RPMs have up-to twenty-four internal Intelligent Power Module (IPM) outlets or terminal pairs and/or up-to 16 external Intelligent Power Module ports. Each outlet/terminal pair supplies power to an attached device, and can be individually turned on and off. External Intelligent Power Module ports are used for cable connection to external IPMs for distributed power supply and control. See 0 for more information on external IPMs.

The outlet power status LED will illuminate when each outlet or terminal pair is powered.

A letter/number combination is printed above each RPM port, outlet or terminal pair. The ports are labeled A1 through A4, B1 through B4, C1 through C4 etc. These names may be used in commands that require a port name. See *Port Naming and Grouping* in Chapter 3: Operations for more information.

The power inlet(s) connects the Sentry RPM to the electrical power source.



R453-0-1





R203-0-X

4820-0-8

Figure 2.1 Sentry RPM Views

## Safety Precautions

This section contains important safety and regulatory information that should be reviewed before installing and using a Sentry Remote Power Manager. For input and output current ratings, see Ratings in OTechnical Specifications.

	Only for installation by qualified service personnel.	<i>À faire installer uniquement par une personne qualifiée.</i>	Nur zur Installation durch qualifiziertes Fachpersonal.
	Always disconnect all power supply cords before opening to avoid electrical shock.	<i>Afin d'éviter tout choc électrique, assurez-vous de toujours débrancher les câbles d'alimentation électrique avant d'ouvrir.</i>	Ziehen Sie vor dem Öffnen immer die Netzkabel heraus, um die Gefahr eines elektrischen Schlags zu vermeiden.
	CAUTION: On-off switch does not turn power off at outlets.	<i>AVERTISSEMENT! L'interrupteur unipolaire ne désalimente pas le courant aux prises électriques.</i>	ACHTUNG! Durch Betätigung des Ein-Aus-Schalters wird die Stromzufuhr an den Anschlussstellen nicht ausgeschaltet.
	WARNING! High leakage current! Earth connection is essential before connecting supply!	<i>AVERTISSEMENT! Courant de fuite élevé! Une mise à la terre est essentielle avant de connecter l'appareil à une source d'alimentation électrique.</i>	ACHTUNG! Hoher Verluststrom! Ein Erdungsanschluss ist vor dem Einschalten der Stromzufuhr erforderlich.
	AC voltage models only: CAUTION: Double Pole/Neutral Fusing.	<i>Modèles à tension alternative seulement: MISE EN GARDE: Fusibles bipolaires/neutres.</i>	Nur Wechselstrom-Modelle: VORSICHT: zweipolige/ neutrale Sicherung.
	DC voltage models only: Connect to VDC source that is electrically isolated from the AC source and reliably connected to earth.  Grounding wire should be bare copper and one size larger than the inlet cables.  Remove fuses/open circuit breakers for terminal pairs prior to connecting inlets to power source.  Inlet & outlet safety covers must be installed for safe operation.	<i>Modèles à tension continue seulement: Brancher à une source de tension continue isolée de la source de tension alternative et mise à la terre adéquatement.  Le fil de mise à la terre doit être en cuivre nu et d'une taille supérieure aux câbles d'entrée.  Retirer les fusibles et ouvrir les disjoncteurs pour connecter les paires de bornes avant de brancher les câbles d'entrée à la source d'alimentation.  Pour une utilisation sécuritaire, les couvercles de sûreté des prises d'entrée et de sortie doivent être installés.</i>	Nur Gleichstrom-Modelle: Schließen Sie das Gerät an eine Gleichstromquelle an, die von der Wechselstromquelle galvanisch getrennt und sachgemäß geerdet ist.  Verwenden Sie zur Erdung einen Kupferdraht, der um eine Stärke stärker ist als die Eingangskabel.  Entfernen Sie die Sicherungen/schalten Sie die Leistungsschalter für die Klemmenpaare aus, bevor Sie die Eingänge an die Stromquelle anschließen.  Zum sicheren Betrieb müssen die Ein- und Ausgangsabdeckungen installiert sein.

## Mounting

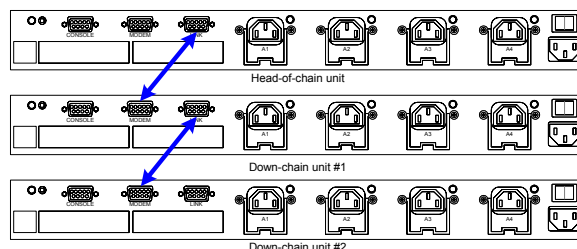
1. Select the appropriate bracket mounting points for proper mounting depth within the rack.
2. Attach one bracket to these mounting points with two screws.
3. Repeat with the other mounting bracket on the opposite side of the enclosure.
4. Install the enclosure into your rack, using the slots in each bracket. The slots allow about ¼ inch of horizontal adaptability to align with the mounting holes of your rack.

**NOTE:** Mounting bracket kits for 23" wide rack or cabinets are available. Contact your Server Technology Sales Representative for more information.

## Chaining Multiple Sentry Remote Power Managers

Sentry supports chaining Remote Power Managers up-to a maximum of 104 total outlets/terminal pairs and/or ports.

1. Attach included DB9-M to DB9-F straight-thru serial cable to the first Sentry RPM (head-of-chain) Link port.
2. Attach the other end of the DB9-M to DB9-F straight-thru serial cable to the next Sentry RPM (down-chain) Modem port.
3. For additional Sentry RPMs, repeat the connections above from the last down-chain Sentry RPM.



**Figure 2.2 Example Sentry Chain**

**NOTE:**

1. Sentry Remote Power Managers with the optional integrated modem may NOT be attached down-chain.
2. Using a Sentry Remote Power Manager with the optional integrated Ethernet as down-chain unit disables access from that Ethernet port.

## Connecting to the Power Source

1. For DC models, verify power source polarity and remove the fuses, open circuit breakers for all outlet terminal pairs.
2. Attach the appropriate input power cord/cable(s) for your installation's operating voltage to the Sentry RPM and/or external IPM.
3. Attach the opposite end of the Sentry RPM power cord/cable(s) to the power source.

## Connecting Devices



---

**CAUTION:** On-off switch does not turn power off at outlets.  
**AVERTISSEMENT!** L'interrupteur unipolaire ne désalimente pas le courant aux prises électriques.  
**ACHTUNG!** Hoher Verluststrom! Ein Erdungsanschluss ist vor dem Einschalten der Stromzufuhr erforderlich.

---

### To avoid the possibility of noise due to arcing:

Keep the device's on/off switch in the off position until after it is attached to the Sentry RPM outlet/terminal pair or IPM outlet.

-or-

Log in to the Sentry RPM and turn off the outlets/terminal pairs and ports before connecting the devices. After connecting the devices, turn them on using the Sentry RPM.



---

**Always disconnect the power supply cord before opening to avoid electrical shock.**  
**Afin d'éviter les chocs électriques, débranchez le câble électrique avant d'ouvrir.**  
**Immer Netzleitung auskuppeln vor dem Aufmachen um elektrischen Schlag zu vermeiden.**

---

## Connecting the Sentry RPM to your network

The Sentry RPM has up to three connection points for attachment to your network. See Chapter 4: Appendices for more information on data connection ports.

1. The Console port provides RS-232 serial connection for direct console access or access through another serial device such as a terminal server.
2. The Modem port provides RS-232 serial connection for direct console access or access through an external modem.
3. The Telco port provides dial in out-of-band access to the integrated modem, if equipped. (RPMs with integrated modems will not be equipped with the Modem port.)
4. The 10Base-T port provides in-band Ethernet access (10Base-T half duplex) to the Network Access Device, if equipped.



---

---

# Chapter 3: Operations

<b>INTERFACES</b>	<b>12</b>
<b>PORT NAMING AND GROUPING</b>	<b>12</b>
<b>USERS AND PASSWORDS</b>	<b>12</b>
<b>LOGGING IN</b>	<b>13</b>
<b>USING THE COMMAND LINE</b>	<b>13</b>
<b>OPERATIONS COMMANDS</b>	<b>15</b>
Turning ports on .....	15
Turning ports off .....	15
Rebooting ports .....	15
Displaying port status .....	16
Accessing the control screen .....	16
Connecting to a serial device.....	17
Displaying serial port information.....	17
Displaying out-of-band authentication setting information.....	17
Displaying modem setting information .....	18
Displaying the current temperature .....	18
Displaying the Sentry firmware version.....	18
Displaying the available port information and status .....	18
Displaying the current session user, port of connection and data-rate .....	19
Starting a new session .....	19
Ending a session.....	19
<b>ADMINISTRATION COMMANDS</b>	<b>20</b>
Adding a username .....	20
Granting port access to a username .....	21
Deleting port access for a username .....	21
Deleting a username .....	21
Displaying port information .....	22
Displaying user information.....	22
Creating a serial pass-through port name .....	23
Deleting a serial pass-through port name .....	23
Displaying serial pass-through port name associations.....	24
Creating a location description and login banner .....	24
Enabling or disabling the Sentry banner.....	24
Enabling or disabling user access to the control screen.....	24
Changing a password .....	25
Enabling or disabling active signal checking for serial connections.....	25
Enabling or disabling confirmation for control screen operations.....	26
Enabling or disabling push-button port control panels.....	26
Enabling or disabling out-of band network authentication.....	27
Setting the modem data-rate.....	27
Enabling or disabling modem initialization strings.....	28
Granting and removing administrative privileges .....	28
Resynchronizing the Sentry chain.....	28
<b>USING THE CONTROL SCREEN</b>	<b>29</b>
Location field .....	29
Port Name field .....	30
Control Status field.....	30
Module Status field .....	30
Device Load field.....	30
Minimum-On Time field.....	30
Minimum-Off Time field .....	31
Shutdown Delay field.....	31
Wake-up State field.....	31
Group field .....	31
Access field .....	32
Page field.....	32
Temperature field .....	32

---

## Chapter 3: Operations

### Interfaces

The Sentry has two interfaces: command line and control screen. When a valid user logs in, the command line prompt (Sentry:) appears. From this prompt, commands may be issued according to the user's privileges. The control screen is accessed from the command line with the Show command. You may return to the command line from the control screen by typing **c**.

You may end a Sentry session either from the command line or the control screen.

---

**NOTE:** Sentry supports only one simultaneous session through the Console, Modem or Telnet ports. For information on HTML sessions and limitations, see *HTML* in *ONetwork Access Device*.

---

### Port Naming and Grouping

When a command calls for a Sentry port name, you may specify it in one of two ways: a predefined absolute name or a descriptive name assigned by the administrator.

An absolute name is specified by a period (.) followed by a group letter and port number. To specify an absolute port name, enter a period followed by the labeled port ID value.

---

**NOTE:** For chained Sentry units, the head-of-chain Sentry Remote Power Manager assigns group letters beginning with its own groups starting with A, with each next consecutive port group in the chain being assigned the next consecutive group letter. For example, in a chain of two 8-port RPMs, groups A & B refer to A1-A4 and B1-B4 on the head-of-chain unit and groups C & D refer to A1-A4 and B1-B4 on the 1<sup>st</sup> down-chain unit.

---

Alternatively, descriptive port names may be created on the control screen and used in commands that require a port name. See *Using the Control Screen* in this chapter for more information about descriptive port names.

Additionally, Sentry ports may be assigned group names on the control screen, enabling you to issue a command that affects all ports in the group. Specify the group name with the command, such as on, off or reboot. See *Using the Control Screen* for more information about group names.

### Usernames and Passwords

The Sentry has three predefined usernames, shown in the following table.

#### Predefined Usernames

Name	Password	Privileges
Admn	adm	Fully-privileged
Gen1	gen1	Semi-privileged
Gen2	gen2	Semi-privileged

---

**NOTE:** Predefined usernames may NOT be removed. For security, Server Technology recommends changing the passwords for the predefined usernames prior to connection to your network. See *Changing a password* for more information about changing passwords.

---

An additional 117 users may be added.

By default, only the Admn user may perform administrative operations such as adding/deleting usernames and command privileges, changing passwords and displaying port and user information. The Admn user may also view the status of all Sentry ports, access the control screen and control power to all ports.

---

**NOTE:** By default, the Gen1 and Gen2 users may view the status of all Sentry ports, access the control screen and control power to all ports. The administrator may change these privileges.

---

The administrator creates additional usernames with the Add User command, and then uses the Add Port command to grant these users the right to view the status of and control power to specific Sentry ports. The administrator uses the Set Show command to grant control screen access to additional users.

The administrator may grant administrative privileges to another user with the Admnp command. This command may also be used to remove administrative privileges previously granted. This feature allows the Sentry to have more than one administrator-level user.



Additional usernames must contain from 1-16 characters; spaces are not allowed. A username is not case sensitive. Passwords may contain up to 16 characters, and are case sensitive. The administrator may change a password with the Set Password command. See Administration Commands in this chapter for more information about commands that create and manage usernames.

---

**NOTE:** For security, when a password is typed, either blanks or asterisks appear on the screen instead of the typed password characters.

---

## Logging In

Logging into the Sentry Remote Power Manager through either the Console or Modem serial port requires the use of a terminal or terminal emulation software. The terminal or emulation software must be configured to support ANSI or VT100, a supported data rate (300, 1200, 2400, 4800, 9600, 19200, or 38400 BPS)- 8 data bits-no parity-one stop bit and Device Ready output signal (DTR or DSR).

### To log in to the Sentry:

1. Press **Enter** twice. The following appears, where **x.x** is the firmware version:

```
Sentry Version x.x
Username:
```

2. At the Username: prompt, enter a valid username and press **Enter**.

If you do not enter a valid username within 60 seconds, the session ends with the message:  
Your time is up. Try again later  
Session ended.

3. At the Password: prompt, enter a valid password and press **Enter**.

If you do not enter a valid password within 60 seconds, the session ends with the message:  
Your time is up. Try again later  
Session ended.

If you enter an invalid password, the following message appears:  
Username/Password entered is NOT valid  
Username:

You are given three attempts to enter a valid username and password combination. If all three fail, the session ends with the message:  
Username/Password entered is NOT valid  
Check your Username/Password and try again later  
Session ended.

When you enter a valid username and password, the Sentry command prompt (Sentry:) appears. If a location identifier was defined, it will be displayed before the Sentry: prompt. See *Creating a location description and login banner* in this chapter for more information.

## Using the Command Line

You may enter commands in uppercase, lowercase or using a combination. You must enter all command characters correctly; there are no command abbreviations. The Admn user may issue any command. Other usernames may be granted access to some or all commands.

An administrator may lock ports on the control screen. When locked, a port's on/off state may not be changed from the command line or the control screen until an administrator unlocks the port. See *Using the Control Screen* for more information about locking and unlocking ports.

The command line supports two types of commands: operations and administration. The following tables list and briefly describes each command.

## Operations Command Summary

Command	Description
Connect	Connects to a serial device
Login	Brings up the Username: prompt
Off	Turns one or more ports off
On	Turns one or more ports on
Quit	Ends a session
Reboot	Reboots one or more ports
Report	Displays available port information for current user
Show	Displays the control screen
Show Connect	Displays the on/off status of active signal checking for serial ports
Show Modem	Displays the Sentry settings for the modem data-rate and initialization strings
Show Netauth	Displays the on/off status for out-of-band network authentication
Show Session	Displays the username, port of connection and connection speed for the current session
Status	Displays the on/off status of one or more ports
Temp	Displays the current temperature on one or all control screen pages
Vers	Displays the Sentry firmware version

## Administrative Command Summary

Add Port	Grants a username access to one or all ports
Add User	Adds a username
Add Sname	Adds a descriptive name to a serial pass-through port
Admnp	Grants or removes administrative privileges for a username
Del Port	Removes access to one or all ports for a username
Del User	Deletes a username
Del Sname	Deletes a descriptive name from a serial pass-through port
List Port(s)	Displays information about one or all ports
List User(s)	Displays information about one or all users
List Sname	Displays descriptive name associations for all serial pass-through ports
Restart	Performs a warm boot of the Sentry Remote Power Manager
Resync	Resynchronizes the chain of Sentry Remote Power Managers
Set Banner	Enables or disables the Sentry banner displayed at the Username: prompt
Set Connect	Enables or disables active signal checking for serial connections
Set Location	Specifies a descriptive field for the control screen and login banner
Set Modem	Configures the modem data-rate and initialization strings for Sentry
Set Netauth	Enables or disables out-of-band authentication
Set Panel	Enables or disables push-button panels
Set Password	Changes the password for a username
Set Screen	Enables or disables confirmation for control screen operations that change port states
Set Show	Enables or disables Show command access for a username

### **To display the names of commands that you may execute:**

At the command prompt, press **Enter**. A list of valid commands for your username appears.

## Operations Commands

Operations commands manage Sentry port states, provide information about the Sentry environment and control session operations.

For most operations commands that affect port states, you may specify multiple port names on one command line, separated by a space or a comma, to a maximum of 50 characters.

---

**NOTE:** Users must be granted access to affect any change in port state.

---

### **Turning ports on**

The On command turns on one or more ports. When the command completes, a display indicates the number of ports that were turned on and the number of ports that are locked in their current state.

#### **To turn ports on:**

At the Sentry: prompt, type **on**, followed by one or more port names separated by spaces or commas, and press **Enter**, or

Type **on**, followed by a group name, and press **Enter**, or

Type **on all** and press **Enter**.

#### **Examples**

The following command turns the second port on, using the port's absolute name:

```
Sentry: on.a2<Enter>
```

The following command turns on all the ports in the group named ops\_srv:

```
Sentry: on ops_srv<Enter>
```

The following command turns on ports A1 and C3, using the ports' absolute names:

```
Sentry: on.a1 .c3<Enter>
```

### **Turning ports off**

The Off command turns off one or more ports. When the command completes, a display indicates the number of ports that were turned off and the ports that are locked in their current state.

#### **To turn ports off:**

At the Sentry: prompt, type **off**, followed by one or more port names separated by spaces or commas, and press **Enter**, or

Type **off**, followed by a group name, and press **Enter**, or

Type **off all** and press **Enter**

#### **Examples**

The following command turns the sixth and eighth ports off, using the ports' absolute names:

```
Sentry: off.b2 .b4<Enter>
```

The following command turns off the port named ops\_2:

```
Sentry: off ops_2<Enter>
```

The following command turns off all ports:

```
Sentry: off all<Enter>
```

### **Rebooting ports**

The Reboot command reboots one or more ports. This operation turns the port(s)off, delays for a period of time and then turns the port(s)on. The delay interval is 15 seconds by default, or the minimum-off time specified on the control screen, whichever is greater.

When the command completes, a display indicates the number of ports that were rebooted and the ports that are locked in their current state.

If you plan to reboot a large number of ports simultaneously by specifying all ports or a group name that is assigned to many ports, it may be beneficial to set staggered minimum-off time values among the ports. This enables you to avoid an excessive in-rush of current and possible circuit overload. See *Using the Control Screen* for information about the minimum-off time.

### To reboot one or more ports:

At the Sentry: prompt, type **reboot**, followed by one or more port names separated by spaces or commas, and press **Enter**, or

Type **reboot**, followed by a group name, and press **Enter**, or

Type **reboot all** and press **Enter**.

### Examples

The following command reboots the ports named ops\_2 and shp\_2:

```
Sentry: reboot ops_2 shp_2<Enter>
```

The following command reboots all the ports in the group named ops\_srv:

```
Sentry: reboot ops_serv<Enter>
```

The following command reboots all ports:

```
Sentry: reboot all<Enter>
```

## Displaying port status

The Status command displays the on/off status of one or more ports. For the three predefined usernames Admn, Gen1 and Gen2, this command may be used to display the status of all ports, including ports for which power control access is not allowed. For additional usernames, the command displays the status of only those ports for which the username has power control access.

The display indicates the number of ports that are on as well as those that are off. If you do not specify any parameter with this command, the status of all ports is displayed.

### To display on/off status of one or more ports:

At the Sentry: prompt, type **status**, followed by one or more port names separated by spaces or commas, and press **Enter**, or

Type **status**, followed by a group name, and press **Enter**, or

Type **status all** and press **Enter**, or

Type **status** and press **Enter**.

### Examples

The following command displays the on/off status of the port named shp\_2:

```
Sentry: status shp_2<Enter>
```

The following command displays the on/off status of all ports:

```
Sentry: status<Enter>
```

## Accessing the control screen

The Show command displays the control screen, which contains 1 to 26 pages of information, depending on type of Sentry Remote Power Manager and type/number of additional chained Sentry RPMs. You may specify a page by its absolute name: .A for page 1, .B for page 2, .C for page 3, .D for page 4, etc. You may also use a page name defined on the control screen. If you do not specify a page name, page 1 is displayed. See Using the Control Screen for more information about control screen pages.

The Show command is always available to the predefined usernames Admn, Gen1 and Gen2. By default, added usernames are not allowed to use the Show command. The administrator may use the Set Show command to enable and disable Show command access for other usernames.

### To access the control screen:

At the Sentry: prompt, type **show**, optionally followed by a page name, and press **Enter**. If you omit a page name, the first page is displayed.

To return to the command line from the control screen, press **c**.

## **Connecting to a serial device**

The Connect command allows pass-through serial connection to devices attached to one of the three standard serial ports (Console, Modem, Link), a pass-through communication port (Switch) or the internal Network Access Device (Network). See Network Access Device for more information.

---

**NOTE:** When attaching a device other than an external modem to the Modem port, disabling of the default modem initialization string is recommended. See *Setting Modem baud rate and initialization strings* in Network Access Device.

---

### **To connect to a serial device:**

At the Sentry: prompt, type **connect**, followed by the serial port name and press **Enter**.

#### **Examples**

The follow command connects to the serial device connected to the Link serial port:

```
Sentry: connect link<Enter>
```

The following command connects to the internal Network Access Device:

```
Sentry: connect network<Enter>
```

The follow command connects to the serial device connected to the pass-through communication port a1:

```
Sentry: connect .a1<Enter>
```

The follow command connects to the serial device connected to the pass-through communication port named router1:

```
Sentry: connect router1<Enter>
```

The port name was previously defined using the Add Sname command or from the Control Screen.

### **To disconnect from a serial device:**

Type **!\*login** and press **Enter**.

---

**NOTE:** Disconnecting from a pass-through communication session returns the user to the login prompt.

---

## **Displaying serial port information**

The Show Connect command displays the active signal checking status for the serial ports (Console, Modem, Link, Switch, Network).

### **To display the active signal checking status for a serial port:**

At the Sentry: prompt, type **show connect**, followed by the serial port name and press **Enter**.

#### **Examples**

The following command displays the active signal checking status for the Console port:

```
Sentry: show connect console<Enter>
Connect "CONSOLE" settings:
DSR Check: On
CTS Check: Off
```

## **Displaying out-of-band authentication setting information**

The Show Netauth command is used to display the out-of-band network authentication settings for the console and modem ports.

### **To display the out-of-band authentication settings:**

At the Sentry: prompt, type **show netauth** and press **Enter**.

#### **Example**

The following command requests information on the out-of-band authentication settings:

```
Sentry: show netauth
NetAuth settings:
Modem:      Off
Console:    Off
```

## Displaying modem setting information

The Show Modem command is used to display the modem data-rate and initialization strings settings.

### To display the modem settings:

At the Sentry: prompt, type **show modem** and press **Enter**.

### Example

The following command requests information on the modem settings:

```
Sentry: show modem<Enter>
Modem Settings:
Rate:      9600
Init 1:    Default
Init 2:    Default
Init 3:    Default
Attn:     Default
Hangup:   Default
```

## Displaying the current temperature

The Temp command is used to display the temperature reading from the optional external temperature probe(s).

### To display the current temperature

At the Sentry: prompt, type **temp**, followed by the absolute page name or **all**, and press **Enter**.

### Examples

The following command displays the temperature for page B:

```
Sentry: temp .b
.B          Current Temperature: 29.5 Deg C
```

The following command displays the current temperature for all pages:

```
Sentry: temp all
.A          Current Temperature: 27.0 Deg C
.B          Current Temperature: 29.5 Deg C
```

## Displaying the Sentry firmware version

The Vers command displays the Sentry firmware version.

### To display the firmware version:

At the Sentry: prompt, type **vers** and press **Enter**.

## Displaying the available port information and status

The Report command is used to display port information and status for all assigned ports for the current user.

### To display available port information and status:

At the Sentry: prompt, type **report** and press **Enter**.

### Example

```
Sentry: report<Enter>
Port  Port      Group      Control  Module
ID   Name         Name       Status   Status
.A1  Port_A1     Group_A   Lckd On  Normal
.A2  Port_A2     Group_A   Off      Normal
.C1  Port_C1     Group_A   On       Normal
```

## **Displaying the current session user, port of connection and data-rate**

The Show Session command is used to display the username, port of connection and connection data-rate for the current session.

### **To display the session information:**

At the Sentry: prompt, type **show session** and press **Enter**.

### **Example**

```
Sentry: show session<Enter>
Session:
  User: (Administrative)
  Port: NETWORK
  Rate: 9600
```

---

**Note:** This command is primarily used for diagnostics to verify proper communication data-rates for serial pass-through connections. See *Connecting to a serial device* in this section for more information on serial pass-through connections.

---

## **Starting a new session**

The Login command activates the Username: prompt. The current session ends, allowing a user to log in and start a new session under a different username.

### **To start a new session:**

At the Sentry: prompt, type **login** and press **Enter**. The Username: prompt appears.

## **Ending a session**

You may end a session from the command line or the control screen.

If you made configuration changes during the session, they are automatically stored in non-volatile memory. After you end the session, wait for the following message before taking any action that will power down the Sentry:

```
Updating configuration memory ...
Update complete
Session ended
```

A session ends automatically after five minutes of inactivity.

### **To end a session:**

From the Sentry: prompt, type **quit** and press **Enter**, or

From the control screen, press **q**.

## Administration Commands

Administration commands include the Add, Del, List and Set commands, plus the Admnp command. Some of these commands manage usernames and their privileges. Other administration commands affect the control screen.

Administration commands may only be issued by a user with administrative privileges, such as the predefined Admn user or another user who has been granted administrative privileges with the Admnp command.

### To display a list of available Add commands:

At the Sentry: prompt, type **add** and press **Enter**.

The following display appears:

```
ADD commands are:  
USER PORT SNAME
```

### To display a list of available Del commands:

At the Sentry: prompt, type **del** and press **Enter**.

The following display appears:

```
DEL commands are:  
USER PORT SNAME
```

### To display a list of available List commands:

At the Sentry: prompt, type **list** and press **Enter**.

The following display appears:

```
LIST commands are:  
USER USERS PORT PORTS SNAME TRAPS
```

### To display a list of available Set commands:

At the Sentry: prompt, type **set** and press **Enter**.

The following display appears:

```
SET commands are:  
BANNER CONNECT LOCATION MODEM NETAUTH PANEL PASSWORD SHOW SCREEN  
TEMPH TEMPL LOADL LOADH ILOADL ILOADH ENABLET DISABLET TRAPTME
```

## Adding a username

The Add User command adds a username and password. See *Usernames and Passwords* on page 12 for more information.

### To add a username:

At the Sentry: prompt, type **add user**, optionally followed by a 1-16 character username. Spaces and colon characters are not allowed, and usernames are not case sensitive. Press **Enter**.

At the Password: prompt, type a password of up to 16 alphanumeric and other typeable characters (ASCII 32 to 126 decimal). Passwords are case sensitive. Press **Enter**.

To specify no password, press **Enter** at the prompt.

At the Verify Password: prompt, retype the password. Press **Enter**.

To verify no password, press **Enter** at the prompt.

### **Examples**

The following command adds username JaneDoe:

```
Sentry: add user JaneDoe<Enter>  
Password: *****<Enter>  
Verify New Password: *****<Enter>
```

For security, password characters are displayed as asterisks.

The following command adds username JohnDoe:

```
Sentry: add user<Enter>  
Username: JohnDoe<Enter>  
Password: *****<Enter>  
Verify Password: *****<Enter>
```



## **Granting port access to a username**

The Add Port command grants a username access to one or all ports.

To grant access for more than one port, but not all ports, you must use multiple Add Port commands. When the command completes successfully, the following message appears, where x indicates the number of ports:

```
x port(s)added Command Completed Successfully
```

### **To grant port access to a username:**

At the Sentry: prompt, type **add port**, optionally followed by a username and a port name. Press **Enter**, or Type **add port**, followed by a username, then **all**. Press **Enter**.

If you enter an invalid username or port name, the command aborts with the message:

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

### ***Examples***

The following commands use absolute port names to grant the username JaneDoe access to ports A1, A2 and C2:

```
Sentry:add port janedoe .a1<Enter>
Sentry:add port janedoe .a2<Enter>
Sentry:add port janedoe .c2<Enter>
```

The following commands use the ports' descriptive names to grant the username JaneDoe access to ports ops\_1, ops\_2 and shp\_2:

```
Sentry:add port janedoe ops_1<Enter>
Sentry:add port janedoe ops_2<Enter>
Sentry:add port janedoe shp_2<Enter>
```

The following command grants access to all ports for the username JohnDoe:

```
Sentry: add port<Enter>
Username: johndoe<Enter>
Port Name: all<Enter>
```

## **Deleting port access for a username**

The Del Port command removes a username's access to one or all ports. You cannot remove access to any port for the Admn user. When the command completes successfully, the following message appears, where x indicates the number of ports:

```
x port(s)deleted Command Completed Successfully
```

### **To delete port access for a username:**

At the Sentry: prompt, type **del port**, optionally followed by a username and a port name. Press **Enter**, or Type **del port all**. Press **Enter**.

If you enter an invalid username or port name, the command aborts with the message:

```
0 port(s)deleted. Command Completed Successfully
```

## **Deleting a username**

The Del User command removes a username. You cannot delete the predefined usernames Admn, Gen1 or Gen2. When the command completes successfully, the following message appears, where x indicates the number of ports:

```
x port(s)deleted Command Completed Successfully
```

### **To delete a username:**

At the Sentry: prompt, type **del user**, optionally followed by a username. Press **Enter**.

```
Name entered is NOT valid.
```

## Displaying port information

The List Port and List Ports commands display information about one or all ports, respectively. This information includes:

- Descriptive port name, if applicable
- Group name assigned to the port, if any
- Usernames who may access the port

When requesting information about all ports, the display begins with port A1's information, followed by a prompt to either continue with the next port's information or quit the display. If you choose to continue, port A2's information is displayed, followed by a prompt to continue or quit. You may choose to quit at any time. After the information for all ports has been displayed, or after quitting, you are returned to the command prompt.

### **To display information about one port:**

At the Sentry: prompt, type **list port**, optionally followed by a port name. Press **Enter**.

### **To display information about all ports:**

At the Sentry: prompt, type **list ports** and press **Enter**.

### **Examples**

The following command requests information about port B1 by specifying its absolute port name:

```
Sentry: list port .b1<Enter>
.B1 hr_1 hr_srv
Usernames:
ADMN GEN1 GEN2
JOHNDOE
Username List for .B1 Complete
```

The display indicates that port B1 has the descriptive name hr\_1 and is in the port group named hr\_srv. The usernames who may access this port are Admn, Gen1, Gen2 and JohnDoe.

The following command requests information about all ports:

```
Sentry: list ports<Enter>
.A1 ops_1 ops_serv
Usernames:
ADMN GEN1 GEN2
JANEDOE
Username List for .A1 Complete
Press:(N)ext,(Q)uit:
```

The first screen of the resulting display indicates that port A1 has a descriptive port name of ops\_1 and is in the port group named ops\_serv. The usernames who may access port A1 are Admn, Gen1, Gen2 and JaneDoe. The page ends with a prompt to continue with the display for the next port, A2, or quit and return to the Sentry: prompt.

## Displaying user information

The List User and List Users commands display information about one or all users, respectively. When requesting information about one user, the display includes a list of all ports the user may access, and whether the Show command is enabled or disabled for the user. When requesting information about all users, the display indicates whether the Show command is enabled or disabled for each user and whether each user has been given administrative privileges.

### **To request information about one user:**

At the Sentry: prompt, type **list user**, optionally followed by a username. Press **Enter**.

To request information about all users:

At the Sentry: prompt, type **list users** and press **Enter**.

## Examples

The following command displays information about the username JaneDoe:

```
Sentry: list user janedoe<Enter>
Active Port List for Username JANEDOE Show command disabled
A1 ops_1 ops_srv
A2 ops_2 ops_srv
C2 shp_2
List Complete
```

The display indicates that JaneDoe may not use the Show command to access the control screen. JaneDoe may access the following ports: A1 which has a descriptive name of ops\_1 and is in the port group named ops\_srv, A2 which has a descriptive name of ops\_2 and is in the port group named ops\_srv and C2 which has a descriptive name of shp\_2.

The following command requests information about all users:

```
Sentry: list users<Enter>
ADMN Show command enabled Administrative user
GEN1 Show command enabled
GEN2 Show command enabled
JANEDOE Show command disabled
JOHNDOE Show command enabled
List Complete
```

### **Creating a serial pass-through port name**

The Add Sname command assigns an additional descriptive name to a pass-through port. You may use this name in commands that require a serial pass-through port name, as an alternative to using the port's absolute or descriptive name. See *Port Name field* on page 30 for additional information.

---

#### NOTE:

1. Serial pass-through port names must be unique.
  2. Multiple names may be assigned to a single port.
  3. The Sentry RPM supports a maximum of 32 pass-through port names using the Add Sname command.
  4. Serial pass-through port names assigned with the Add Sname command are NOT bound by port privilege security unlike Port Names assigned from the Control Screen. See *Port Name field* on page 30 for additional information.
- 

### **To specify a serial pass-through port name:**

At the Sentry: prompt, type **add sname**, followed by a descriptive name of up to 16 alphanumeric and other typeable characters (ASCII 32 to 126 decimal), followed by the absolute port name. And press **Enter**.

#### **Example**

The following command adds the descriptive name Router1 to pass-through port .a1:

```
Sentry: add sname Router1 .a1<Enter>
```

### **Deleting a serial pass-through port name**

The Del Sname command removes a descriptive name to a pass-through port.

### **To remove a serial pass-through port name:**

At the Sentry: prompt, type **del sname**, followed by the port's descriptive name and press **Enter**.

#### **Example**

The following command removes the descriptive name Router1 previously assigned to pass-through port .a1:

```
Sentry: del sname Router1<Enter>
```

## Displaying serial pass-through port name associations

The List Sname command displays all assigned pass-through port names with the associated absolute port name.

### **To display serial pass-through port name associations**

At the Sentry: prompt type **list sname** and press **Enter**.

#### **Example**

The following command displays the serial pass-through port name associations:

```
Sentry: list sname
ROUTER1          .A1
ROUTER2          .A2
```

## Creating a location description and login banner

The Set Location command specifies text that appears in the control screen's Location field. The text is also appended to a Welcome to banner that appears when a user successfully logs in.

If you do not issue this command, or if you issue this command without specifying any text, the control screen's Location field will be blank and no Welcome to banner will be displayed.

When this command completes successfully, the following message appears:

```
All pages changed locations
```

### **To create a location description and login banner:**

At the Sentry: prompt, type **set location**, optionally followed by up to 16 characters. Spaces are allowed. Press **Enter**.

Omitting any characters after typing 'set location' deletes any previously specified text.

#### **Examples**

The following command specifies Florida HQ as the descriptive location for the control screen and the login banner:

```
Sentry: set location Florida HQ<Enter>
```

The following command deletes any previously specified location description:

```
Sentry: set location<Enter>
```

In this case, the control screen's Location field will be blank, and no welcome banner will be displayed after a successful login.

## Enabling or disabling the Sentry banner

The Set Banner command is used to enable or disable the Sentry banner displayed at the Username: prompt.

### **To enable or disable the Sentry banner:**

At the Sentry: prompt type **set banner**, followed by **on** or **off** and press **Enter**.

## Enabling or disabling user access to the control screen

The Set Show command enables or disables a username's access to the Show command. This determines whether the username may access the control screen.

When the command completes successfully, one of the following messages is displayed, where USERNAME is the username specified in the command:

```
Show command enabled for USERNAME
Show command disabled for USERNAME
```

### **To enable or disable control screen access:**

At the Sentry: prompt, type **set show**, optionally followed by a username and **on** or **off**. Press **Enter**.

If you do not specify a username, you are prompted for it (Username:). If you do not specify on or off, you are prompted for it (Specify ON or OFF:).

If you specify an invalid username, the command aborts with the message:

```
Name entered is NOT valid.
```

## Examples

The following command enables Show command access for the user JohnDoe:

```
Sentry: set show johndoe on<Enter>
```

The following command disables Show command access for the user JaneDoe:

```
Sentry: set show<Enter>  
Username: janedoe<Enter>  
Specify ON or OFF: off<Enter>
```

## Changing a password

The Set Password command changes a username's password. To change the password for any user other than Admn, you do not need to know the current password. To change the password for the Admn user, you must know the current password.

For security, when you type a password, the characters appear as asterisks (\*) on the screen. When the command completes successfully, a confirmation message is displayed. Passwords are case-sensitive. See Usernames and Passwords for more information.

### To change a password:

At the Sentry: prompt, type **set password**, optionally followed by a username and press **Enter**.

If you specify an invalid username, the command aborts with the message:

```
Name entered is NOT valid
```

If you are changing the password for the Admn user, the Enter Current Password: prompt appears. Type the current password and press **Enter**.

At the Enter New Password: prompt, type the new password and press **Enter**. Passwords may contain up to 16 characters, and spaces are not allowed. To specify no password, press **Enter** at the prompt.

At the Verify New Password: prompt, retype the new password and press Enter. To verify no password, press **Enter** at the prompt.

## Examples

The following command changes the password for the user named JohnDoe:

```
Sentry: set password johndoe<Enter>  
Enter New Password: *****<Enter>  
Verify New Password: *****<Enter>
```

For security, password characters display as asterisks.

The following command blanks the password for the user named JaneDoe:

```
Sentry: set password<Enter>  
Username: janedoe<Enter>  
Enter New Password: <Enter>  
Verify New Password: <Enter>
```

## Enabling or disabling active signal checking for serial connections

The Set Connect command enables or disables active signal checking for pass-through serial connections to devices attached to any of the available serial ports.

### Predefined Values

Serial Port	DSR Checking	CTS Checking
Console	on	off
Modem	on	on
Link	on	on
Network	off	on
Switch	on	off

### To enable or disable active signal checking for serial connections:

At the Sentry: prompt, enter **set connect**, followed by serial port name and **dsrcheck**, **nodsrcheck**, **ctscheck** or **noctscheck** parameter. Press **Enter**.

---

**NOTE:** The Set Connect Switch command applies to ALL integrated pass-through ports. Individual port signal checking settings are NOT possible.

---

If you omit the serial port name or spell it incorrectly, the command aborts with the message:

```
SET CONNECT options are:
<serial port name>
```

If you omit the **dsrcheck/nodsrcheck/ctscheck/noctscheck** parameter or spell it incorrectly, the command aborts with the message:

```
SET CONNECT <serial port name> options are:
DSRCHECK NODSRCHECK CTSCHECK NOCTSCHECK
```

### Examples

The following command disables DSR checking for the Modem serial port:

```
Sentry: set connect modem nodsrcheck<Enter>
```

The following command enables CTS checking for the Console serial port:

```
Sentry: set connect console ctscheck<Enter>
```

The following command disables DSR checking for all pass-through serial ports:

```
Sentry: set connect switch nodsrcheck<Enter>
```

### Enabling or disabling confirmation for control screen operations

The Set Screen command enables or disables a confirmation query when requesting port power changes on the control screen. When the Confirm option is set, the user is prompted with **Are you sure? (Y/N)** when an on, off or reboot operation is initiated on the control screen. When the Noconfirm option is set, the requested operation is completed immediately. The default value is Noconfirm. The Set Screen setting applies to all usernames.

### To enable or disable confirmation for control screen operations:

At the Sentry: prompt, enter **set screen**, followed by **confirm** or **noconfirm** and press **Enter**.

If you omit the confirm/noconfirm parameter or spell it incorrectly, the command aborts with the message:

```
SET SCREEN options are
NOCONFIRM CONFIRM
```

### Example

The following command enables control screen confirmation queries:

```
Sentry: set screen confirm<Enter>
```

### Enabling or disabling push-button port control panels

The Set Panel command enables or disables the push-button port control panels available on some Sentry Remote Power Managers.

### To enable the push-button panels

At the Sentry: prompt, type **set panel default** and press **Enter**.

### To disable the push-button panels:

At the Sentry: prompt, type **set panel none** and press **Enter**.

## **Enabling or disabling out-of band network authentication**

The Sentry Network Access Device (NAD), available in some Sentry RPM models, supports both TACACS+ and SecurID authentication protocols. See Network Access Device for more information on the Sentry NAD, TACACS+ and SecurID.

By default, these authentication protocols only apply to Telnet sessions (in-band). Sentry also provides support for authentication for Console and Modem port connections (out-of-band). When enabled, connections through the Console and/or Modem ports are redirect through the NAD authentication using the enabled authentication protocol. By default, network authentication for the Console and Modem port is off.

The Set Netauth command is used to enable or disable out-of-band authentication on the Modem and Console ports.

### **To enable network authentication:**

At the Sentry: prompt, type **set netauth**, followed by **console** or **modem**, and **on**. Press **Enter**.

#### ***Example***

The following enables network authentication for the console port:

```
Sentry: set netauth console on<Enter>
```

### **To disable network authentication:**

At the Sentry: prompt, type **set netauth**, followed by **console** or **modem**, and **off**. Press **Enter**.

#### ***Example***

The following disables network authentication for the modem port:

```
Sentry: set netauth modem off<Enter>
```

## **Setting the modem data-rate**

The Sentry supports multiple initialization data rates for external or the integrated modem available in some Sentry RPM models. The Set Modem Rate command is used to set this value. Valid data-rates are 300, 600, 1200, 2400, 4800, 9600, 19200, 38400 or None. The default value is 9600.

---

**NOTE:** 'None' is used to disable all modem initialization string support.

---

### **To set the modem data-rate:**

At the Sentry: prompt, type **set modem rate**, followed by the data-rate and press **Enter**.

#### ***Example***

The following command sets the modem data-rate to 38400 BPS:

```
Sentry: set modem rate 38400<Enter>
```

## **Enabling or disabling modem initialization strings**

Sentry initializes the modem whenever the Sentry is initially powered, the modem is powered or connected and after all modem sessions. The Set Modem command is used to enable or disable these initialization strings.

Predefined initializations strings are enabled by default.

---

**NOTE:** The Set Modem Rate command may be used to disable all initialization strings. See *Setting the modem data-rate for more information*.

---

### **Predefined Modem Initialization Strings**

String Type	String	Description
Attention	@@@	Switches the modem to command mode
Hang-up	ATH	Forces a hang-up of an active connection
Init 1	AT	Gets modem attention
Init 2	AT E0 Q1 S0=3 S2=42 S12=50 &C1 &D2	Initializes default settings required by Sentry
Init 3	AT S0=1	Sets the modem to answer on the 1 <sup>st</sup> ring

---

**NOTE:** For high-speed external modems supporting *variable data-rate mode*, Server Technology recommends the modem operating mode be set to *fixed data-rate mode* to avoid the data-rate being changed to a non-supported rate.

The modem manual must be referred to as the command(s) required to set the configuration to *fixed data-rate mode* vary significantly from manufacturer to manufacturer. The modem should be configured directly from a PC using a terminal program and the command &W be used to save the new configuration to memory and set it to default.

---

### **To enable or disable modem initialization strings:**

At the Sentry: prompt, type **set modem**, followed by **attention**, **hangup**, **init1**, **init 2** or **init3** and **default**(enabled) or **none**(disabled). Press **Enter**.

### **Examples**

The following command disabled the Init 3 string (the modem will answer on ring 3):

```
Sentry: set modem init3 none<Enter>
```

The following command enables the Attention string:

```
Sentry: set modem attention default<Enter>
```

## **Granting and removing administrative privileges**

The Admnp command grants or removes administrative privileges for usernames other than the predefined Admn user. This command allows a Sentry to have more than one administrative-level user. You cannot remove administrative privileges from the Admn user.

### **To grant or remove administrative privileges for a username:**

At the Sentry: prompt, type **admnp**, followed by **on** or **off**, optionally followed by a username and press **Enter**.

If you do not specify a username, you are prompted for it (Username:).

### **Examples**

The following command grants administrative privileges to the username JohnDoe:

```
Sentry: admnp on johndoe<Enter>
```

The following command removes administrative privileges from the username JohnDoe:

```
Sentry: admnp off<Enter>  
Username: johndoe<Enter>
```

## **Resynchronizing the Sentry chain**

The Resync command is used to resynchronize the connection/control of all chained Sentry Remote Power Manager. This commands ends the current session and then resynchronizes the chain.

---

**NOTE:** Resynchronization requires approximate 90 seconds during which connection to the Sentry RPM is not possible.

---

### **To resynchronize the Sentry chain**

At the Sentry: prompt, type **resync** and press **Enter**.



## Using the Control Screen

The control screen contains Sentry configuration and status information. Figure 3.1 shows an example of the first page of a control screen.

```
Power Control System (c) Server Technology, Inc. 1 of 2
Location: Input Load:N/A
Port Name: [ ] [ ] [ ] [ ]
Control Status: (x)On (x)On ( )On (x)On
               ( )Off ( )Off (x)Off ( )Shtdwn
Module Status: Normal Normal Normal Normal
Device Load: 12.25A 0.00A Not On 4.50A
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 02:30
Wake-Up State: On On On On
Group: [ ] [ ] [ ] [ ]
Access: All All All All
Page: [ ] Temperature: 26.0
Press: C)mnd, E)dit,N)ext, Q)uit, Space-Bar to Select
```

### Figure 3.1 Example Control Screen

Each page contains information about four ports. Page 1 contains information about ports A1 through A4 and page 2 contains information about ports B1 through B4, page 3 contains information about ports C1 through C4 etc.

The Show command accesses the control screen from the command line. Use the Arrow keys on your keyboard to move the cursor from field to field. The help line at the bottom of the screen displays key commands that, when typed on your keyboard, perform specific operations. The following chart describes these keys.

### Control Screen Help Line

Key	Action
C )mnd	Pressing C activates the Sentry command line.
E )dit	Pressing E moves the cursor to the end of the current entry in an editable field. Each press of the Backspace key erases one character. When you finish editing the field, press Enter or Tab.
N )ext	Pressing N displays the next control screen page.
P )revious	Pressing P displays the previous control screen page.
Q )uit	Pressing Q ends the session. This is equivalent to the Quit command in the command line.
Space-Bar to Select	Pressing the Spacebar toggles among preset values. You may also use the Spacebar in the Control Status rows to change a port 's state to the state of the current cursor location: On or Off. Alternatively, you may use the Plus (+) and Minus (-) keys on the numeric keypad to switch among preset values.

Some fields on the control screen are display-only and cannot be changed. Other fields may be changed by toggling among preset values or by entering text. The following sections describe each control screen field.

### Location field

The display-only Location field may contain text that was specified with the Set Location command. The text in this field is also appended to a Welcome to banner that appears when a user successfully logs in.

## **Input Load field**

This feature is not currently supported by the Sentry Remote Power Manager.

## **Port Name field**

The editable Port Name field may contain a descriptive name for the device connected to the port. You may use this name in commands that require a port name, as an alternative to using the port's absolute name. See *Port Naming and Grouping* for more information about port names. This descriptive name, by default, is also applied to the associated pass-through communication port if equipped.

---

**NOTE:** Assigned port privilege security applies to this descriptive name for BOTH power and pass-through connections.

---

### **To specify a port name:**

Position the cursor in the relevant Port Name field.

Type **e**. If you are changing an existing name, press the **Backspace** key to erase characters. Type a 1-8 character name. Press **Enter** or **Tab**.

## **Control Status field**

The editable Control Status field indicates the port's current state with a character in the On or Off field. An **x** indicates the port is accessible, an asterisk (\*) indicates that the administrator has locked the port, or that the current username does not have access rights to the port and an **o** indicates an error condition.

### **To turn a port on or off:**

Position the cursor in the port's desired state (On or Off) and press the **Spacebar** or the **Plus (+)** key. The **x** will move to the new state.

### **To reboot a port:**

Position the cursor in the port's On or Off field and press **r**. If the port is already off, it will turn on immediately. If the port is on, it will turn off, delay and then turn back on. The delay interval is either 15 seconds or the minimum-off time, whichever is greater. During the reboot delay, the Off field contains an **r**, indicating that the port is going to reboot.

### **To lock or unlock a port:**

Position the cursor in the port's On or Off field and press **l** to lock or **u** to unlock. A locked port has an asterisk (\*) in the On or Off field and cannot be controlled by other usernames; only an administrator may lock or unlock a port.

## **Module Status field**

The display-only Module Status field indicates the port's current status.

### **Module Status Field Values**

<b>Display</b>	<b>Description</b>	<b>Control Status field</b>
Normal	The port is working correctly.	'x'
No Rspns	The interface cannot communicate with the port.	'o'
OnS Fail	The port was instructed to be on, but it is off.	'o' in On field
Off Fail	The port was instructed to be off, but it is on.	'o' in Off field

## **Device Load field**

The display-only Device Load field indicates the current load in amperes of the device attached to that port of the Sentry Remote Power Manager. This feature is currently supported in DC voltage Sentry RPMs only.

## **Minimum-On Time field**

The editable Minimum-On Time field indicates the minimum amount of time that a port will stay on before it can be turned off by a command. The default value is 0. Manual commands in the control screens On and Off fields are always immediate and ignore this value.

### **To change a port's minimum-on time value:**

Position the cursor in the port's Minimum-On Time field and press the **Spacebar** or the **Plus (+)** or **Minus (-)** key. Each press moves through preset values to a one hour maximum.

### **Minimum-Off Time field**

The editable Minimum-Off Time field indicates the minimum amount of time that a port will stay off before it can be turned on by a command. The default is 0. Manual commands in the control screen's On or Off fields are always immediate, ignoring this value except during a reboot. During a reboot, whether initiated from the command line or the control screen, the value in this field determines the time that a port remains in the off state during the reboot cycle, if it is longer than 15 seconds.

You may use this value to stagger the startup of ports when a command is issued to reboot multiple ports at the same time. For example, setting different minimum-off time values may be useful when you issue a Reboot All command or a Reboot command for a large group.

It may be important in your configuration to set the minimum-off time values differently to avoid a circuit overload caused by an excessive in-rush of current that may occur when too many devices power up simultaneously.

#### **To change a port 's minimum-off time value:**

Position the cursor in the port's Minimum-Off Time field and press the **Spacebar** or the **Plus (+)** or **Minus (-)** key. Each press moves through preset values to a one hour maximum.

### **Shutdown Delay field**

The editable Shutdown Delay field indicates the amount of time that a port will remain powered while the Sentry RPM asserts a power loss/shutdown signal to the attached server, prior to turning off in response to an Off or Reboot command. This field is displayed only in certain model Sentry Remote Power Managers supporting orderly shutdown of Window NT/2000/XP servers. For more information on Sentry Shutdown see 0Sentry Shutdown.

The default value is 2 minutes and 30 seconds.

#### **To change a port 's shutdown delay time value:**

Position the cursor in the port's Shutdown Delay field and press the **Spacebar** or the **Plus (+)** or **Minus (-)** key. Each press moves through preset values to an eight minute maximum.

### **Wake-up State field**

The editable Wake-up State field indicates the state that the port will go to when the Sentry is powered up, either during normal operation or when power is restored after an outage. The options are On and Off. The default is On.

Only ports that are set with a wake-up state of Off will remain off.

#### **To change a port 's wake-up state:**

Position the cursor in the field and press the **Spacebar**, the **Plus (+)** key or the **Minus (-)** key. Each press toggles between On and Off.

### **Group field**

The editable Group field may contain a descriptive name. All ports with the same group name may be acted upon simultaneously with the On, Off and Reboot commands from the command line. Individual on, off and reboot commands initiated on the control screen do not affect other ports that have been assigned the same group name. Only command line actions that contain the group name parameter will cause all ports within the same group to power up, down or reboot as a group.

If you assign the same group name to a significant number of ports, consider staggering the minimum-off time values of the affected ports to help prevent an excessive in-rush load from occurring when a command is issued to reboot the group.

#### **To specify a group name:**

Position the cursor in the port's Group field.

Press **e**. If you are changing an existing name, press the **Backspace** key to erase characters. Type a 1-8 character name. Press **Enter** or **Tab**.

## **Access field**

The editable Access field allows the administrator to easily change port access for the usernames Admn, Gen1 and Gen2. Port access for additional usernames must be enabled with the Add Port command from the command line.

### **To change port access for the Admn,Gen1 or Gen2 usernames:**

1. Position the cursor in the port 's Access field.
2. Use the **Spacebar**, the **Plus (+)** key or the **Minus (-)** key to switch among the preset options:  
*All* -grants port access to Admn, Gen1 and Gen2; this is the default  
*Admn* -grants port access to Admn  
*Gen1* -grants port access to Admn and Gen1  
*Gen2* -grants port access to Admn and Gen2

## **Page field**

The editable Page field may contain a name for the current control screen page. When you want to display a specific page of the control screen, you may use this page name as a parameter in the Show command, or you may specify a page with its absolute name: .A for page 1,.B for page 2,.C for page 3,.D for page 4 etc.

### **To specify a page name:**

1. Position the cursor in the Page field.
2. Press **e**. If you are changing an existing name, use the **Spacebar** to erase characters. Type a 1-8 character string. Press **Enter** or **Tab**.

## **Temperature field**

The display-only Temperature field indicates the current temperature at the external temperature probe(s) optionally available on Sentry Remote Power Managers. Temperature is reported in degrees Celsius in .5 degree increments.

---

---

# Chapter 4: Appendices

<b>RESETTING TO FACTORY DEFAULTS</b>	<b>35</b>
To reset the Sentry RPM to factory defaults from the command line: .....	35
To reset the Sentry RPM to factory defaults using the reset button: .....	35
<b>TECHNICAL SPECIFICATIONS</b>	<b>36</b>
Standard Models.....	36
Ratings.....	39
Inlet Connections.....	39
Outlet Connections.....	40
Output Circuit Protection .....	41
Data & Signal Connections .....	42
Push Button Controls .....	44
LED Indicators .....	44
<b>NETWORK ACCESS DEVICE</b>	<b>46</b>
Interface.....	46
Initial Configuration .....	46
Logging in .....	47
Basic Commands.....	47
Opening a Sentry Session.....	49
Encrypted Telnet .....	50
HTML .....	51
SNMP .....	52
TACACS+ .....	55
SecurID .....	56
Out-of-Band Authentication.....	57
Authentication Fallback .....	58
IP Security Tables .....	58
Additional Security Options.....	60
Resetting to Factory Defaults .....	62
<b>MODEM</b>	<b>63</b>
Modem Connection Port .....	63
Initial Configuration .....	63
Logging in .....	64
Setting the setup password .....	64
Configuring the Country Code .....	64
Enabling or disabling Callback Security .....	65
Setting Callback dial strings.....	66
Setting Callback passwords.....	66
Resetting a Callback memory location.....	67
Setting the maximum Callback attempts .....	67
Setting the Callback delay.....	67
Callback Security Calling Procedures.....	68
Displaying Callback failed attempts counter.....	67
Resetting the Callback failed attempts counter .....	67
<b>SENTRY SHUTDOWN</b>	<b>69</b>
Connections.....	69
Configuring Windows .....	69
Automatic Logon.....	71
<b>SNMP</b>	<b>72</b>
MIB, OID and Support.....	72
SNMP Support .....	72
Traps.....	72
Commands.....	74
<b>EXTERNAL INTELLIGENT POWER MODULES</b>	<b>78</b>
Standard Models.....	78

<b>R480-0-x</b>	<b>79</b>
Equipment Overview .....	79
Operations Commands .....	79
Technical Specifications .....	80
<b>SENTRY ANY-TO-ANY PASS THROUGH SWITCH</b>	<b>81</b>
Standard Models .....	81
Commands .....	81
Data Connections .....	82
<b>WARRANTY, PRODUCT REGISTRATION AND SUPPORT</b>	<b>83</b>
Warranty and Limitation of Liability .....	83
Product Registration .....	83
Technical Support .....	83
Return Merchandise Authorization .....	84

---

## Chapter 4: Appendices

### Resetting to Factory Defaults

You may reset the non-volatile RAM that stores all configurable Sentry RPM options. This clears all administrator-editable fields on the control screen and resets all command line configurable options to their default values, including usernames and passwords.

You may reset the Sentry RPM to factory defaults by issuing a command or by pressing the reset button on the front-panel of the Sentry RPM. You must have administrator-level privileges to issue the command. Using the reset button may be necessary when a forgotten password prevents administrator login. Either method updates the current working configuration to the factory defaults.

#### **To reset the Sentry RPM to factory defaults from the command line:**

At the Sentry: prompt, type **set cnfg all factory** and press **Enter**.

When the command completes successfully, the following message appears, where **n** is the total number of ports on the RPM divided by 4:

```
Config changed on n board(s), 0 ignore(s).
```

---

**NOTE:** The Set Cnfg All Factory command does NOT affect configuration settings for the Network Access Device if equipped.

---

#### **To reset the Sentry RPM to factory defaults using the reset button:**

Remove power from the RPM.

On the the RPM, locate the reset button (A1 on models with push button panels), then depress and hold the reset button for at least ten seconds while reapplying power to the RPM.

---

**NOTE:**

1. Resetting the RPM using the reset button resets the ALL configurable options for the RPM AND the Network Access Device, if equipped.
  2. Resetting the RPM using the reset button resets ONLY the RPM at the beginning of a Sentry chain. The remainder of the Sentry chain must be reset from the command line.
-

# Technical Specifications

## Standard Models

### AC Models - 100-120V, 50/60Hz

Model	Inlet(s)	Outlets	Outlet Protection <sup>1</sup>	Additional Ports
R200-0-1	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	
R201-0-1	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	4 ext. IPM
R202-0-1	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 ext. IPM
R203-0-1	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 pass-thru
R204-0-1	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	4 ext. IPM, 12 pass-thru
R205-0-1	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 ext. IPM, 8 pass-thru
R210-0-1	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 shutdown
R211-0-1	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	4 ext. IPM, 12 shutdown
R212-0-1	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 ext. IPM w/ shutdown, 8 shutdown
R213-0-1	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 pass-thru, 8 shutdown
R220-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	
R221-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 ext. IPM
R222-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	8 ext. IPM
R223-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	12 ext. IPM
R224-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 pass-thru
R225-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 ext. IPM, 8 pass-thru
R226-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	8 pass-thru
R230-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 shutdown
R231-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 ext. IPM, 8 shutdown
R232-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	8 ext IPM w/ shutdown, 4 shutdown
R234-0-1	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 pass-thru, 4 shutdown
R308-0-1	8 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	
R400-0-1	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	
R401-0-1	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	4 ext. IPM
R402-0-1	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	4 pass-thru
R410-0-1	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	4 shutdown
R411-0-1	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	4 ext. IPM port, 4 pass-thru port
R412-0-1	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	4 pass-thru, 4 shutdown
R450-0-1	IEC 60320 C14	-	Fuse (I)	4 ext. IPM
R451-0-1	IEC 60320 C14	-	Fuse (I)	8 ext. IPM
R452-0-1	IEC 60320 C14	-	Fuse (I)	12 ext. IPM
R453-0-1	IEC 60320 C14	-	Fuse (I)	16 ext. IPM
R454-0-1	IEC 60320 C14	-	Fuse (I)	4 ext. IPM port, 4 pass-thru
R455-0-1	IEC 60320 C14	-	Fuse (I)	8 ext. IPM, 8 pass-thru
R460-0-1	IEC 60320 C14	-	Fuse (I)	4 ext. IPM w/ shutdown
R461-0-1	IEC 60320 C14	-	Fuse (I)	8 ext. IPM w/shutdown
R462-0-1	IEC 60320 C14	-	Fuse (I)	12 ext. IPM w/ shutdown
R463-0-1	IEC 60320 C14	-	Fuse (I)	16 ext. IPM w/ shutdown
R464-0-1	IEC 60320 C14	-	Fuse (I)	4 ext IPM w/ shutdown, 4 pass-thru
R465-0-1	IEC 60320 C14	-	Fuse (I)	8 ext. IPM w/ shutdown, 8 pass-thru
R480-0-1	IEC 60320 C14	2 IEC 60320 C13	Fuse (I)	2 ext. IPM, 2 pass-thru

<sup>1</sup> I-Internal; no customer access, PTR-Push to Reset

<sup>2</sup> Additional IEC 60320/C14 inlet for powering Sentry logic.



## AC Models - 208-240, 50/60Hz

Model	Inlet(s)	Outlets	Outlet Protection <sup>1</sup>	Additional Ports
R200-0-2	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	
R201-0-2	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	4 ext. IPM
R202-0-2	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 ext. IPM
R203-0-2	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 pass-thru
R204-0-2	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	4 ext. IPM, 12 pass-thru
R205-0-2	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 ext. IPM, 8 pass-thru
R210-0-2	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 shutdown
R211-0-2	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	4 ext. IPM, 12 shutdown
R212-0-2	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 ext. IPM w/ shutdown, 8 shutdown
R213-0-2	2 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	8 pass-thru, 8 shutdown
R220-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	
R221-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 ext. IPM
R222-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	8 ext. IPM
R223-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	12 ext. IPM
R224-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 pass-thru
R225-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 ext. IPM, 8 pass-thru
R226-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	8 pass-thru
R230-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 shutdown
R231-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 ext. IPM, 8 shutdown
R232-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	8 ext IPM w/ shutdown, 4 shutdown
R234-0-2	4 IEC 60320 C20 <sup>2</sup>	4 IEC 60320 C19	Breaker (PTR)	4 pass-thru, 4shutdown
R308-0-2	8 IEC 60320 C14	8 IEC 60320 C13	Fuse (I)	
R400-0-2	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	
R401-0-2	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	4 ext. IPM
R402-0-2	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	4 pass-thru
R410-0-2	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	4 shutdown
R411-0-2	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	4 ext. IPM port, 4 pass-thru port
R412-0-2	IEC 60320 C14	4 IEC 60320 C13	Fuse (I)	4 pass-thru, 4shutdown
R450-0-2	IEC 60320 C14	-	Fuse (I)	4 ext. IPM
R451-0-2	IEC 60320 C14	-	Fuse (I)	8 ext. IPM
R452-0-2	IEC 60320 C14	-	Fuse (I)	12 ext. IPM
R453-0-2	IEC 60320 C14	-	Fuse (I)	16 ext. IPM
R454-0-2	IEC 60320 C14	-	Fuse (I)	4 ext. IPM port, 4 pass-thru
R455-0-2	IEC 60320 C14	-	Fuse (I)	8 ext. IPM, 8 pass-thru
R460-0-2	IEC 60320 C14	-	Fuse (I)	4 ext. IPM w/ shutdown
R461-0-2	IEC 60320 C14	-	Fuse (I)	8 ext. IPM w/shutdown
R462-0-2	IEC 60320 C14	-	Fuse (I)	12 ext. IPM w/ shutdown
R463-0-2	IEC 60320 C14	-	Fuse (I)	16 ext. IPM w/ shutdown
R464-0-2	IEC 60320 C14	-	Fuse (I)	4 ext IPM w/ shutdown, 4 pass-thru
R465-0-2	IEC 60320 C14	-	Fuse (I)	8 ext. IPM w/ shutdown, 8 pass-thru
R480-0-2	IEC 60320 C14	2 IEC 60320 C13	Fuse (I)	2 ext. IPM, 2 pass-thru

<sup>1</sup> I-Internal; no customer access, PTR-Push to Reset

<sup>2</sup> Additional IEC 60320/C14 inlet for powering Sentry logic.

## DC Models -48V

Model	Inlet(s) <sup>1</sup>	Outlets <sup>1</sup>	Outlet Protection <sup>1</sup>	Additional Ports
4805/35-XL-20	2 blocks (CL)	20 pairs (SD) 4 pairs (DS)	Fuse (GMT) Breaker (L)	
4805/35-XLT-12	2 blocks (CL)	8 pairs (SD) 4 pairs (DS)	Fuse (GMT) Breaker (L)	
4805-XL-24	2 blocks (CL)	24 pairs (SD)*	Fuse (GMT)	
4805-XLT-16	2 blocks (CL)	16 pairs (SD)*	Fuse (GMT)	
4820-0-4	2 blocks (CL)	4 pairs (SS)	Breaker (PP)	
4820-0-8	2 blocks (CL)	8 pairs (SS)	Breaker (PP)	
4835-0-4	2 blocks (CL)	4 pairs (DS)	Breaker (L)	
4850-0-4	2 blocks (CL)	4 pairs (DS)	Breaker (L)	
4870-0-4	2 blocks (CL)	4 pairs (DS)	Fuse (TPC)	
R450-0-3	1 block (SS)	-	Fuse (I)	4 ext. IPM
R451-0-3	1 block (SS)	-	Fuse (I)	8 ext. IPM
R452-0-3	1 block (SS)	-	Fuse (I)	12 ext. IPM
R453-0-3	1 block (SS)	-	Fuse (I)	16 ext. IPM
R454-0-3	1 block (SS)	-	Fuse (I)	4 ext. IPM port, 4 pass-thru
R455-0-3	1 block (SS)	-	Fuse (I)	8 ext. IPM, 8 pass-thru
R460-0-3	1 block (SS)	-	Fuse (I)	4 ext. IPM w/ shutdown
R461-0-3	1 block (SS)	-	Fuse (I)	8 ext. IPM w/shutdown
R462-0-3	1 block (SS)	-	Fuse (I)	12 ext. IPM w/ shutdown
R463-0-3	1 block (SS)	-	Fuse (I)	16 ext. IPM w/ shutdown
R464-0-3	1 block (SS)	-	Fuse (I)	4 ext IPM w/ shutdown, 4 pass-thru
R465-0-3	1 block (SS)	-	Fuse (I)	8 ext. IPM w/ shutdown, 8 pass-thru

<sup>1</sup>CL-Compression Lug, DS-Dual Stud, GMT-GMT, TPC-TPC, L-Latching, PP-Push/Pull, SD-Screw down, SS-Single Screw

## DC Models -72V

Model	Inlet(s) <sup>1</sup>	Outlets <sup>1</sup>	Outlet Protection <sup>1</sup>	Additional Ports
7220-0-8	2 blocks (CL)	8 pairs (SS)	Breaker (L)	

<sup>1</sup>CL-Compression Lug, L-Latching, SS-Single Screw

## Ratings

Available Configurations Configurations Disponibles Verfügbare Konfigurationen						
Model Modèle Modelle	Input Current Ratings <sup>1</sup> L'indice du courant d'entrée Eingangsstromstärke			Output Current Ratings L'indice du courant de sortie Ausgangsstromstärke		
		Voltage Tension Spannung	Current Courant Strom		Outlet Prise Anschlussstelle	Total Total Insgesamt
R20x-0-1 - R21x-0-1	A, B	100-120V AC 50/60Hz	15	A1, A2, A3, A4 B1, B2, B3, B4	10 10	15
R22x-0-1 - R23x-0-1	A1, A2, A3, A4	100-120V AC 50/60Hz	20	A1, A2, A3, A4	20	15
R30x-0-1	A1, A2, A3, A4, B1, B2, B3, B4	100-120V AC 50/60Hz	10	A1, A2, A3, A4, B1, B2, B3, B4	10	15
R40x-0-1 - R41x-0-1	A	100-120V AC 50/60Hz	15	A1, A2, A3, A4	10	15
R45x-0-1 - R46x-0-1	A	100-120V AC 50/60Hz	15	Auxiliary (2)	10	10
R480-0-1	A	100-120V AC 50/60Hz	15	A1, A2	10	15
R20x-0-2 - R21x-0-2	A, B	208-240V AC 50/60Hz	10	A1, A2, A3, A4 B1, B2, B3, B4	10 10	15
R22x-0-2 - R23x-0-2	A1, A2, A3, A4	208-240V AC 50/60Hz	16	A1, A2, A3, A4	16	15
R30x-0-2	A1, A2, A3, A4, B1, B2, B3, B4	208-240V AC 50/60Hz	10	A1, A2, A3, A4, B1, B2, B3, B4	6	10
R40x-0-2 - R41x-0-2	A	208-240V AC 50/60Hz	10	A1, A2, A3, A4	6	10
R45x-0-2 - R46x-0-2	A	208-240V AC 50/60Hz	10	N/A	N/A	N/A
R480-0-2	A	208-240V AC 50/60Hz	10	A1, A2	6	10
4805-XL-24	A, B	-48 VDC	100	A1, A2, A3, A4, B1, B2, B3, B4 C1, C2, C3, C4, D1, D2, D3, D4, E1, E2, E3, E4, F1, F2, F3, F4	5 5	100
4805-XLT-16	A, B	-48 VDC	100	A1, A2, A3, A4, B1, B2, B3, B4 C1, C2, C3, C4, D1, D2, D3, D4	10 10	100
4805/35-XL-20	A, B	-48 VDC	100	A1, A2, A3, A4, B1, B2, B3, B4 E1, E2 C1, C2, C3, C4, D1, D2, D3, D4 E3, E4	10 35 10	100
4805/35-XLT-12	A, B	-48 VDC	100	A1, A2, A3, A4 C1, C2 B1, B2, B3, B4 C3, C4	10 70 10 70	100
4820-0-4	A, B	-48 VDC	100	A1, A2 B1, B2	20 20	100
4820-0-8	A, B	-48 VDC	100	A1, A2, A3, A4, B1, B2, B3, B4	20 20	100
4835-0-4	A, B	-48 VDC	100	A1, A2 B1, B2	35 35	100
4850-0-4	A, B	-48 VDC	100	A1, A2 B1, B2	50 50	100
4870-0-4	A, B	-48 VDC	100	A1, A2 B1, B2	70 70	100
R45x-0-3 - R46x-0-3	A	-48 VDC	20	N/A	N/A	N/A
7220-0-8	A, B	-72 VDC	100	A1, A2, A3, A4, B1, B2, B3, B4	20 20	100

<sup>1</sup> All current ratings are in amperes. Tous les indices de courant sont en ampères. Alle Angaben der Stromstärke erfolgen in Ampere.

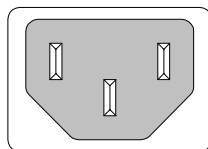
## Inlet Connections

Sentry Remote Power Managers and Intelligent Power Modules require connection to an external power source(s) to power the logic for remote power management. The number and type of inlet connections vary dependant on model. See *Standard Models* for more information on Sentry RPM models and 0 for more information on Intelligent Power Modules.

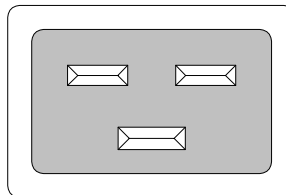
### AC Models

AC Sentry Remote Power Managers are equipped with one, two, five or eight inlet connections. The primary or 'A' power inlet must be connected to a power source for power management functionality.

**Note:** On R308-0-x models, the A1 power inlet must be connected to a power source for power management functionality.



IEC 60320/C14



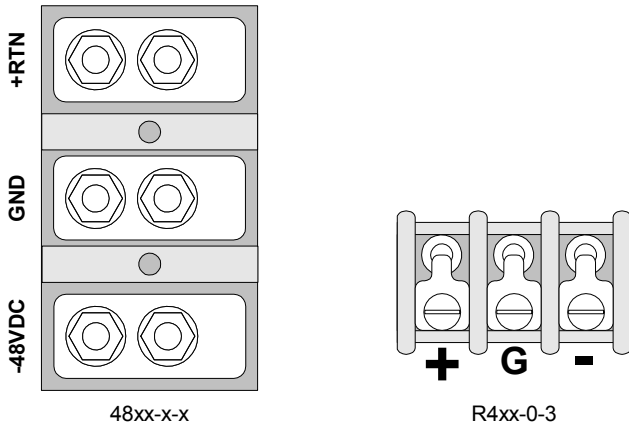
IEC 60320/C20

## DC models

DC Sentry Remote Power Managers are equipped with either one or two input blocks each containing three clearly labeled terminal positions. Connections are made using two-hole copper compression lugs for dual-stud blocks or nylon insulated ring lugs for single-screw blocks.

**WARNING: Reverse polarity will damage the Sentry Remote Power Manager!  
Verify proper polarity before connecting to a power source!**

### Two-hole Copper Compression Lugs



Cable Size(AWG)	Stud Size	Color Code	Thomas&Betts Model	Grainger Stock
#6 str.	1/4"	Blue	54205	3LL91
#4 str	1/4"	Gray	54206	3LL92
#2 str	1/4"	Brown	54207	3LL93
#1 str	1/4"	Green	54208	3LL94

*Grainger catalog #390 (1999-2000)*

### Nylon-Insulated Ring Lugs

Cable Size(AWG)	Stud Size	Color Code	Thomas&Betts Model	Grainger Stock
#22-16	6	Red	RA18-8	3KG16
#22-16	10	Red	RA18-10	3KF97
#18-14	6	Blue	RB14-8	3KG42
#18-14	10	Blue	RB14-10	3KG24
#12-10	10	Yellow	RC10-10	3KG51

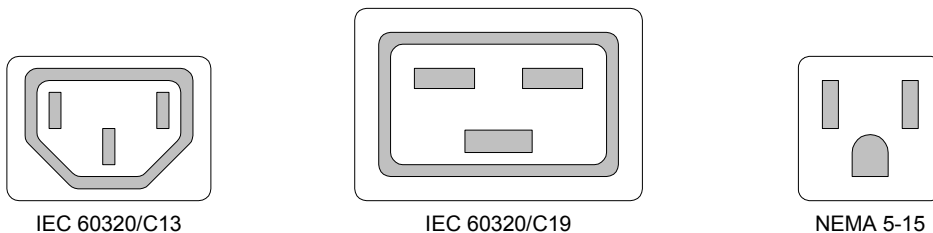
*Grainger catalog #390 (1999-2000)*

## Outlet Connections

Sentry Remote Power Managers are equipped with outlet connections for the devices requiring power management. See *Standard Models* for more information on Sentry RPM models.

### AC Models

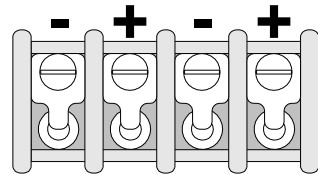
AC Sentry Remote Power Managers are equipped with two, five, eight or no outlet connections.



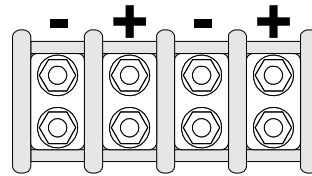
## DC models

DC Sentry Remote Power Managers are equipped with two to twenty-four terminal outlet pairs each containing clearly labeled terminal positions. Connections are made using two-hole copper compression lugs for dual-stud blocks, nylon insulated ring lugs for single-screw blocks and bare stripped wire for high-density screw-down blocks. For recommended hardware, see page 40.

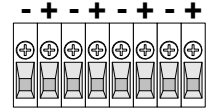
## Output Circuit Protection



Single-screw Terminal



Dual Stud Terminal



Screw-down Terminal

Sentry Remote Power Managers feature output circuit protection on all outlet connectors in the form of internal or external fuses and/or circuit breakers. See *Standard Models* for more information on Sentry RPM models.

## AC Models

AC Sentry Remote Power Manager outlet circuits are protected by either internal fuses or push-to-reset circuit breakers

### **Internal Fuse**

AC Sentry Remote Power Managers with outlet ratings of 15A or less feature internal fuses for circuit protection. These fuses are for circuit protection only and are not designed to be customer serviceable.

### **Push to Reset Circuit Breaker**

Push to Reset circuit breakers are provided on AC Sentry Remote Power Managers featuring outlet rating capacities of greater than 15A.

---

**NOTE:** This type of circuit breaker is not designed to be opened/tripped manually.

---

## DC models

DC Sentry Remote Power Manager outlet circuits are protected by either customer serviceable fuses or circuit breakers.

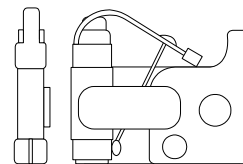
### **GMT Fuse**

DC Sentry Remote Power Managers with high-density outlet terminal pairs are equipped with GMT fuses for circuit protection. GMT fuses offer the following features:

- Fast-acting
- Positive visual indication for blown fuse
- Easily replaceable without special tools
- Protective splatter-cap safety cover
- Color-coded current ratings from .5A to 10A for use with a Sentry RPM

### **GMT Fast-Acting Indicating Fuses**

Amperes	Color code	Bussman Part Number
1	Gray	GMT-1A
2	Orange	GMT-2A
3	Blue	GMT-3A
4	White/Brown	GMT-4A
5	Green	GMT-5A
7½	Black/White	GMT-7½A
10	Red/White	GMT-10A



CooperBussman product data-sheet #5008.  
See data-sheet for complete listing of available GMT fuses.

## TPC Fuse

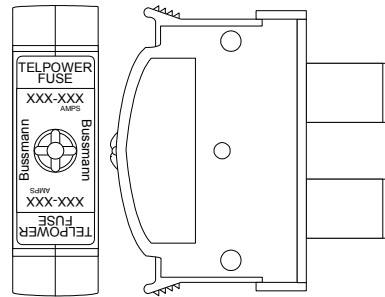
DC Sentry Remote Power Managers with high-power outlet terminal pairs may be equipped with TPC fuses for circuit protection. TPC fuses offer the following features:

- Current-limiting
- 100,000A interrupt rating
- LED indicator for blown fuse
- Easily replaceable without special tools
- Containment of arcs, molten metals and gases during fuse opening
- Color-coded current ratings from 25A to 75A for use with a Sentry RPM

### TPC Telpower® Current Limiting Fuses

Amperes	Color code	Bussman Part Number
25	Yellow	TPC-25
30	Red	TPC-30
40	Purple	TPC-40
50	White	TPC-50
60	Gray	TPC-60
75	Orange	TPC-75

CooperBussman product data-sheet #5023



### Push-Pull Circuit Breaker

DC Sentry Remote Power Managers with low-density outlet terminal pairs rated less than 35A are equipped with Push-Pull circuit breakers for circuit protection.

**NOTE:** This type of circuit breaker may used as a local on/off switch however Server Technology does NOT recommend using the breaker in this fashion for any newly attached device.

### Latching Circuit Breaker

DC Sentry Remote Power Managers with low-density outlet terminal pairs rated greater than 35A may be equipped with thermal circuit breakers for circuit protection.

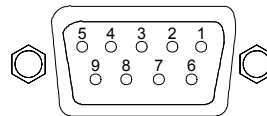
**NOTE:** This type of circuit breaker may used as a local on/off switch.

## Data & Signal Connections

### Console Port

Sentry Remote Power Managers are equipped standard with a DB9-female RS-232C DCE Console serial port. This connector is typically used for direct local access, but may also be used for connection from other serial devices such as a terminal server. A DB9-male to DB9-female straight-through serial cable is provided for connection to a PC DB9-male DTE serial port.

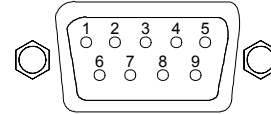
Pin	DCE Signal Name		Input/Output
1	Data Carrier Detect	DCD	Output
2	Receive Data	RD	Output
3	Transmit Data	TD	Input
4	Data Terminal Ready	DTR	Input
5	Signal Ground		
6	Data Set Ready	DSR	Output
7	Request to Send	RTS	Input
8	Clear to Send	CTS	Output



## Modem Port

Sentry Remote Power Managers without an integrated modem are equipped with a DB9-male RS-232C DTE Modem serial port. This connector is typically used to connect to an external modem, but may also be used to connect to any RS-232C device. A 9-pin female to 25-pin male cable is included for connecting the Sentry RPM to an external modem.

Pin	DTE Signal Name		Input/Output
1	Data Carrier Detect	DCD	Input
2	Receive Data	RD	Input
3	Transmit Data	TD	Output
4	Data Terminal Ready	DTR	Output
5	Signal Ground		
6	Data Set Ready	DSR	Input
7	Request to Send	RTS	Output
8	Clear to Send	CTS	Input



**Note:** To connect to a PC serial port, a null-modem adapter and a female-to-female gender changer are required in addition to the included cable.

### Configuration of an external modem

See Chapter 3: Operations for more information regarding the configuration of the Sentry RPM for use with an external modem.

In most cases, nothing is required for a modem to operate with a Sentry RPM; Sentry will initialize the modem automatically. External modem requirements for operation with Sentry are:

- Hayes Smart Modem compatible
- Does not echo data or send result codes.
- Automatically answers incoming calls.
- Supports 300, 1200, 2400, 4800, 9600, 19200, 38400 bit per second (BPS) data-rates.
- Connection configured for 8 data bits, 1 stop bit and no parity.
- Data Carrier Detect (DCD) follows the state of connection.
- Data Set Ready (DSR) is asserted when the modem is ready to communicate.

If problems are encountered, disconnect the modem, reset it to factory defaults following the manufacturer's instructions and try again.

## Link Port

Sentry Remote Power Managers are equipped standard with a DB9-female RS-232C DCE Link serial port. The pinouts for this port match the pinouts given for the Console port described earlier.

**NOTE:** The Link port does not function as an access port for the Sentry.

## IPM Port

Certain model Sentry RPMs are equipped with 4, 8, 12 or 16 black RJ12 IPM ports for control of external IPMs. RJ12 crossover cables are provided for connection to the IPMs. See External Intelligent Power Modules for more information on external IPMs.

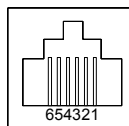
### IPM Port with Shutdown Support

Certain model Sentry RPMs are equipped with 4, 8, 12 or 16 black RJ12 IPM ports for control of external IPMs and shutdown signaling for Windows NT/2000/XP servers. RJ12 Y-cables are provided along with adapters for connection to a standard RS-232C 9 pin DTE UPS service enabled serial port.

## **Pass-through Port**

Certain model Sentry RPMs are equipped with 4, 8, 12 or 16 blue RJ12 Pass-through ports for connection to serial devices. RJ12 crossover cables are provided for connection along with adapters for connection to standard RS-232C 9 and 25 pin, DTE and DCE serial ports.

Pin	DTE Signal Name		Input/Output
1	Signal Ground		
2	Data Set Ready	DSR	Input
3	Data Receive		Input
4	Data Transmit		Output
5	Data Terminal Ready	DTR	Output
6	Signal Ground		



## **Shutdown Port**

Certain model Sentry RPMs are equipped with 4, 8 or 16 red RJ12 Shutdown ports for gentle shutdown Windows NT/2000 equipment. RJ12 crossover cables are provided along with adapters for connection to a standard RS-232C 9 pin DTE UPS service enabled serial port.

## **Temperature Probe Port**

External temperature probes are optionally available for most Sentry Remote Power Managers. A Sentry RPM may have a maximum of two connections for external probes.

**NOTE:** These ports will be available only on Sentry RPMs originally ordered with the environment monitoring option. Please contact your Server Technology Sales Representative for more information.

## **Push Button Controls**

Certain model Sentry RPMs are equipped with push button panels for direct control of individual ports. The following table describes the port response to the push button:

Port State	Short Push	Long Push
On	Turn port off	Lock port on
Off	Turn port on	Lock port off
Locked On	N/A	Unlock port (Port remains on)
Locked Off	N/A	Unlock port (Port remains off)
In Shutdown Operation*	Immediately turn port off	Cancel shutdown (Port remains on)

\*Shutdown enabled IPMs only.

## **LED Indicators**

### **Power On/Off and Status**

Sentry RPMs are equipped standard with a single LED next to the power inlet. During normal operation the LED will display one of the following patterns (patterns not listed indicate an error condition):

Pattern	Power Status	Activity Status
Flashing bright-dim	On	Sentry is idle
Flashing on-off	On	Sentry has an open session or is processing a task
Off	Off	None

### **Port Status**

Sentry RPMs are equipped with a status LED for each power receptacle. A lit/on LED indicates that power is being supplied at the port and a darkened/off LED indicates that there is no power at the port.



## **Push Button Panels**

Certain Sentry RPMs models are equipped with push button panels for direct control of individual ports. On these models, there is a single LED next to each push button. During normal operation the LED will display one of the following patterns:

<b>Pattern</b>	<b>Port Status</b>
On	On
Off	Off
On with 2 intermittent flashes	Locked on
Off with 2 intermittent flashes	Locked off
Off with 1 intermittent flash	Off - in Reboot operation - On imminent
Flashing bright-dim (slow)*	On - in Shutdown operation - Off imminent
Flashing bright-dim (rapid)	Long button push (See <i>Push Button Controls</i> page 44)

*\*Shutdown enabled IPMs only.*

## Network Access Device

The Sentry Network Access Device (NAD) is a 10Base-T half duplex Network Access Device that provides access to the Sentry Remote Power Manager over a TCP/IP Ethernet network.

### Interface

The Sentry NAD supports a command line interface. When a valid password(s) is provided, the operations mode Local\_x>: prompt appears.

Sentry NAD configuration commands must be issued in the privileged mode or Local\_x>>: prompt. See *Accessing Privileged mode* later in this section for more information.

Commands may be entered in uppercase, lowercase or using a combination. The NAD command line supports command abbreviations. The following table lists and briefly describes each basic command commonly used for Sentry.

### Basic Command Summary

Command	Description
Set privileged	Displays privileged mode log in prompt
Change ipaddress	Sets the IP address
Change gateway	Sets the Gateway
Change subnet mask	Sets the Subnet Mask
Show server	Displays settings including IP address, subnet mask, gateway, and more.
Initialize delay	Reboots the NAD with a specified delay
Show sentry	Displays Sentry settings including SNMP, SecurID, TACACS, HTTP and more

You may exit the NAD session from the command line by typing **logout** and pressing **Enter**.

### Initial Configuration

To enable access to the Sentry RPM over a network, the NAD must be configured with an IP Address, Subnet Mask, and Default Gateway. This may be done by a serial port connection, Arp/Ping, DHCP, BootP or RARP.

Provided are instructions to configure the NAD through a serial connection from the Sentry: prompt. The instructions use commands detailed in *Basic Commands* and assume that the default passwords have not been changed.

### Predefined Passwords

Password	Level	NAD mode	Prompt
access	1	operations	Login Password>
system	2	privileged	Password>

**NOTE:** For security, Server Technology recommends changing the predefined passwords prior to connection to your network. See *Additional Security Options* for more information about changing passwords.

### To initially configure the NAD for network access:

1. Log in to the NAD. See *To log in from the Sentry: prompt:* on page 47.
2. At the Local> prompt, type **set privileged** and press **Enter**. The Password> prompt appears.
3. At the Password> prompt, type **system** and press **Enter**.  
When you enter the valid password the Local>> prompt appears. The >> signifies that you have entered privileged mode.
4. At the Local>> prompt, type **change ipaddress**, followed by the IP address to be assigned and press **Enter**.
5. Type **change gateway**, followed by the gateway address to be assigned and press **Enter**.
6. Type **change subnet mask**, followed by the subnet mask to be assigned and press **Enter**.
7. Type **show server** and press **Enter** to display the NAD characteristic page and verify the finished network configuration.
8. Type **init delay 0** and press **Enter** to reinitialize the NAD with the new settings.  
Re-initialization will take about one minute.
9. Type **!\*login** and press **Enter** to break the Sentry serial connection to the NAD. The Sentry RPM will display the Disconnecting... banner and return to the Sentry username: prompt.

## Logging in

You may log directly in to the Sentry NAD operations mode in two ways: from the Sentry: prompt or by Telnet. The instructions below assume that the default password has not been changed.

### To log in from the Sentry: prompt:

---

**NOTE:** These instructions reflect communication to the Sentry RPM by either the Console or Modem port.

---

1. At the Sentry: prompt, type **connect network** and press **Enter**.
2. After receiving the Connection Complete banner, press **Enter** once. The following banner appears, where **x.x/x(xxxxxx)** is the firmware version:  
Servertech MSSLite Version STx.x/x(xxxxxx)  
Login password>
3. At the Login password> prompt, type **access** and press **Enter**.

When you enter the valid password, the Local> prompt appears.

### To log in through Telnet:

1. Open a Telnet session to the assigned IP address using port 23.

#### **Example**

The following command opens a session to IP address 64.42.31.245 using Microsoft Windows' Start>Run:

```
telnet 64.42.31.245 23<Enter>
```

2. The following banner appears, where **x.x/x(xxxxxx)** is the firmware version:  
Servertech MSSLite Version STx.x/x(xxxxxx)  
Login password>
3. At the Login password> prompt, type **access** and press **Enter**. When you enter the valid password, the Username> prompt appears.
4. At the Username> prompt, type any character(s) and press **Enter**.

When you enter the valid password with any username, the Local> prompt appears.

## Basic Commands

### Accessing Privileged mode

The Set Privileged command is used for access to privileged mode. This mode is required to configure all NAD settings and support.

#### **To access privileged mode:**

1. At the Local>> prompt, type **set privileged** and press **Enter**.
2. At the subsequent Password> prompt, enter the privileged mode password and press **Enter**.

When you enter the valid password, the Local> prompt appears. The >> signifies that you have entered privileged mode.

### Setting an IP address

The Change IPaddress command sets the NAD's TCP/IP address.

#### **To set the IP address:**

At the Local>> prompt, type **change ipaddress**, followed by the IP address and press **Enter**.

#### **Example**

The following command sets the NAD IP address to 64.42.31.208:

```
Local>> change ipaddress 64.42.31.208<Enter>
```

### Setting the gateway

The Change Gateway command sets the NAD's default Gateway address.

#### **To set the Gateway:**

At the Local>> prompt, type **change gateway**, followed by the gateway address and press **Enter**.

#### **Example**

The following command sets the NAD gateway to 64.42.31.239:

```
Local>> change gateway 64.42.31.239<Enter>
```

## **Setting the subnet mask**

The Change Subnet Mask command sets the NAD's Subnet Mask.

### **To set the Subnet Mask:**

At the Local>> prompt, type **change subnet mask**, followed by the subnet mask and press **Enter**.

### **Example**

The following command sets the NAD Subnet Mask to 255.0.0.0:

```
Local>> change subnet mask 255.0.0.0<Enter>
```

## **Displaying basic NAD settings**

The Show Server command displays the basic NAD settings including the hardware (MAC) address, IP address, gateway, subnet and more.

### **To display the basic NAD settings:**

At the Local>> prompt, type **show server** and press **Enter**.

### **Example**

The following command requests basic information about the NAD settings:

```
Local>> show server<Enter>
MSSLite Version ST3.6/8(011025)          Uptime:                3:39:20
Hardware Addr: 00-80-a3-25-a2-28Name/Nodenum:  MSS_25A228/ 0
Ident String: MSSLite

Inactive Timer (min):                    5
Password Limit:                           3   Session Limit:         4
Retrans Limit:                            10  Node/Host Limits:     20

TCP/IP Address:                           64.42.31.208   Subnet Mask:           255.0.0.0
Nameserver:                               (undefined)   Backup Nameserver:    (undefined)
TCP/IP Gateway:                           64.42.31.239   Backup Gateway:       (undefined)
Domain Name:                               (undefined)   IP Time:              None
DHCP Server:                               None          TCP Keepalives:       Enabled
Load Address:                             00-00-00-00-00-00  Lease Time:           0:00
Prompt:                                    Local_ %n%P>

Characteristics:
Incoming Logins:  Telnet   (Passwords Required)
```

## **Displaying NAD Sentry extended settings**

The Show Sentry commands displays the settings for Sentry specific extended support of SNMP, HTML, TACACS+, SecurID and more. These settings are defined using 'Sentry' commands described in the following sections.

To display the Sentry extended settings:

At the Local>> prompt, type **show sentry** and press **Enter**.

### **Example**

The following command request information on the Sentry extended settings:

```
Local>> show sentry<Enter>
Sentry Settings:
  Auto-CR:          enabled
  Auth-Fallback:    disabled (password set)
  Unencrypted sockets: enabled

Sentry SNMP parameters:
  SNMP service:      disabled      Timeout:          15 seconds
  Port Speed:        9600
  Communities: GET:  sentry
                   SET:  sentry-set
                   ERROR: sentry-error
                   TRAP: sentry-trap
  Trap Host 1:       (undefined)   Trap Host 2:      (undefined)

SecurID parameters:
  Primary:           (undefined)   Secondary:        (undefined)
  Timeout:          3               Maxtries:         5
  Encryption:       DES             Port:             5500

TACACS settings:
  Server:           (undefined)   Key:              (blank)

Sentry HTTP service:  enabled      HTTP Socket:      80
```

## **Reinitializing the NAD**

The Initialize Delay command reinitializes the NAD storing all changes. The valid range for the delay parameter is 0 (immediate) to 120 (in minutes).

---

**NOTE: Re-initialization requires approximately 1½ minutes during which access to/through the NAD is denied.**

---

### **To reinitialize the NAD:**

At the Local>> prompt, type **init delay**, followed by the delay value and press **Enter**.

### **Example**

The following command causes the NAD to reinitialize immediately:

```
Local>> init delay 0<Enter>
```

## **Opening a Sentry Session**

In order to access the Sentry Remote Power Manager control interface through the NAD, you must open a Telnet session to port 2001 of the assigned IP.

Once the telnet connection is established, the Sentry RPM will present the standard Sentry log in prompt. At this point, the Sentry RPM will respond to all commands as described in Chapter 3: Operations.

### **Example**

The following command opens a Sentry session to IP address 64.42.31.245 using Microsoft Windows' Start>Run:

```
telnet 64.42.31.245 2001<Enter>
Sentry Version x.x
Username:
```

---

**NOTE: If the standard Sentry log-in prompt does not appear after the connection is established, press and hold Enter for one second to initialize a Sentry session.**

---

## **Encrypted Telnet**

The Sentry NAD includes Windows OS support for Two-Fish encrypted Telnet connections using a maximum key size of 56 bits to encrypt all data.

Connections are made with a Win32 PC with the Tcpscram.exe Telnet application: This application is available on the Server Technology ftpsite:

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

The following table lists and briefly describes the commands used to enable and support encrypted Telnet.

### **Encrypted Telnet Command Summary**

<b>Command</b>	<b>Description</b>
Crypt password	Sets the Encrypted Telnet password
Sentry telnet	Enables or disables non-encrypted Telnet ports

### **Enabling encrypted Telnet**

To enable an encrypted Telnet connection, the NAD must first be configured with an encryption password and Tcpscram.exe must be configured for the encrypted connection.

1. Set the NAD encryption password with the Crypt Password command.
2. In Tcpscram.exe:
  - Select the encryption option box
  - Specify the NAD IP address
  - Specify the Telnet port to connect to
    - Port 2100 – to open an NAD operations/configuration session
    - Port 2101 – to open a Sentry Sentry RPM session
  - Specify the encryption password set in item 1

### **Setting an encryption password**

The Crypt Password command is used to set the encrypted Telnet password (key). The password may be up to 7 alphanumeric characters (56 bits) and is case sensitive. To preserve the password case, it must be enclosed with quotes.

---

**NOTE:** If the password is not enclosed in quotes, it will be converted to all upper case.

---

The NAD must be reinitialized after setting the password.

#### **To set an encryption password:**

At the Local>> prompt, type **crypt password**, followed by the password and press **Enter**.

#### ***Example***

The following command sequence sets the encryption password to 'LetMeIn':

```
Local>> crypt password 'LetMeIn'<Enter>
```

### **Enabling/disabling non-encrypted Telnet ports**

By default, non-encrypted ports remain enabled when encrypted connections are enabled. For additional security, these ports may be disabled.

The Sentry Telnet command is used to enable or disable connection to non-encrypted ports.

#### **To enable non-encrypted ports:**

At the Local>> prompt, type **sentry telnet normal** and press **Enter**.

#### **To disable non-encrypted ports:**

At the Local>> prompt, type **sentry telnet secure** and press **Enter**.

## HTML

The Sentry NAD includes an embedded HyperText Transfer Protocol (HTTP) server for support of a HyperText Markup Language (HTML) user interface. Using a standard HTML browser, the Sentry HTML interface offers port control and status monitoring, and environmental monitoring of input loads, device loads and ambient temperature (as supported by the Sentry RPM).

The HTML interface supports 10 simultaneous users.

### NOTE:

1. Administrative configuration, such as user, password and port assignment, is NOT available through this interface.
2. HTML sessions commands are locked-out by any session opened through the Console/Modem ports or Telnet. Server Technology recommends use of the HTML interface for general port control and status monitoring and reservation of the Console, Modem and Telnet sessions strictly for administrative level tasks.

The top screenshot displays the 'Power Outlet Status and Control' interface. It features a navigation menu on the left and a main content area with a table of devices. The table has columns for Name, Control Status, Module Status, Device Load, Action, and Action Result. The bottom screenshot displays the 'Environmental Monitoring' interface, showing a table with columns for Name, Temperature, and Input Load.

Figure 4.1 Example HTML pages

HTML support is disabled by default.

Figure 4.1 shows examples of Outlet Control and Environmental Monitoring HTML interfaces. The following table lists and briefly describes the commands used to enable and support HTML.

### HTML Command Summary

Command	Description
Sentry http	Enables or disables HTML support
Sentry http socket	Sets the HTTP server socket

### Enabling and disabling HTML support

For support for HTML access to the Sentry the embedded HTTP server must be enabled. The Sentry HTTP command is used to enable or disable the HTTP server.

The NAD must be reinitialized after enabling/disabling HTML support.

#### To enable or disable the HTTP server:

At the Local>> prompt, type **sentry http**, followed by **enabled** or **disabled** and press **Enter**.

### Changing the HTTP server socket

With HTML support enabled, the HTTP server watches and responds to requests on the default server socket number 80. For additional security, this socket number may be changed. The Sentry HTTP Socket command is used to change the HTTP server's socket number.

The valid range for the socket number parameter is 2048 to 65535.

The NAD must be reinitialized after changing the HTTP server socket.

#### To change the HTTP server socket:

At the Local>> prompt, type **sentry http socket**, followed by the socket number and press **Enter**.

#### Example

The following command changes the HTTP server socket number to 2048:

```
Local>> sentry http socket 2048
```

#### To reset the HTTP server socket:

At the Local>> prompt, type **sentry http socket default** and press **Enter**.

## **SNMP**

The Sentry NAD includes support for the Simple Network Management Protocol (SNMP). For more information on Sentry SNMP support, please see 0SNMP.

SNMP support is disabled by default.

The following table lists and briefly describes the commands to enable and configure the NAD for SNMP support:

### **SNMP Command Summary**

<b>Command</b>	<b>Description</b>
Sentry snmp	Enables or disables SNMP support
Sentry snmp timeout	Sets the SNMP timeout period
Sentry snmp speed	Sets the SNMP data-rate
Sentry snmp trapdest	Sets the destination IP addresses for traps
Sentry snmp trapcomm	Sets the trap community string
Sentry snmp getcomm	Sets the 'get' community string
Sentry snmp setcomm	Sets the 'set' community string
Sentry snmp errcomm	Sets the community string for extended Sentry error information

The NAD must be reinitialized after enabling/disabling or changing SNMP configurations.

### **Enabling/disabling SNMP support**

The Sentry SNMP command is used to enable or disable SNMP support.

#### **To enable SNMP support:**

At the Local>> prompt, type **sentry snmp**, followed by **enabled** or **disabled** and press **Enter**.

### **Setting the timeout period**

For Get/Set SNMP request that requires communication to the Sentry RPM, the NAD opens a serial session with Sentry during which time other connection paths (Console, Modem, Telnet) are blocked. The timeout period defines the maximum period of inactivity before automatically closing the Sentry session and reopening access to all paths.

The Sentry SNMP Timeout command is used to set this inactivity timeout period. The valid range for the period parameter is 5 to 55 (in seconds). The default period is 15.

#### **To set the SNMP timeout period:**

At the Local>> prompt, type **sentry snmp timeout**, followed by the timeout period and press **Enter**.

#### ***Example***

The following command sets the SNMP timeout period to 55.

```
Local>> sentry snmp timeout 55<Enter>
```

### **Setting the Sentry SNMP data-rate**

The Sentry SNMP Speed command is used to set the data-rate at which the Sentry RPM responds to SNMP requests. Valid entries for the data-rate are 300, 1200, 2400, 4800, 9600, 19200 and 38400 bps. The default data-rate is 9600.

#### **To set the SNMP data-rate:**

At the Local>> prompt, type **sentry snmp speed**, followed by the data-rate and press **Enter**.

#### ***Example***

The following command sets the data-rate to 38400:

```
Local>> sentry snmp speed 38400<Enter>
```



## **Setting trap destinations**

The Sentry SNMP Trapdest command is used to set the IP addresses of SNMP management stations receiving all traps. Sentry supports a maximum of two trap destinations; one must be defined to enable trap generation.

### **To set the trap destination:**

At the Local>> prompt, type **sentry snmp trapdest**, the Ipaddress(s) separated by a space, and press **Enter**.

### **Example**

The following sets the trap destination to 64.42.31.208:

```
Local>> sentry snmp trapdest 64.42.31.208<Enter>
```

The following sets the trap destinations to 64.42.31.208 and 64.42.31.211:

```
Local>> sentry snmp trapdest 64.42.31.208 64.42.31.211<Enter>
```

### **To reset the trap destination:**

At the Local>> prompt, type **sentry snmp trapdest 0.0.0.0** and press **Enter**.

## **Setting the trap community string**

The Sentry SNMP Trapcomm command is used to set the community string, which is included with all generated traps. This string must be defined to enable trap generation.

The trap community string may be 1 to 15 characters. To preserve the string case, it must be enclosed with quotes. The default trap community string is "sentry-trap".

---

**NOTE:** If the string is not enclosed in quotes, it will be converted to all upper case.

---

### **To set the trap community string:**

At the Local>> prompt, type **sentry snmp trapcomm**, followed by the string and press **Enter**.

### **Example**

The following sets the community string to "ops\_serv":

```
Local>> sentry snmp trapcomm "ops_serv"
```

### **To clear the trap community string:**

At the Local>> prompt, type **sentry snmp trapcomm ""** and press **Enter**.

## **Setting the Get/Set community strings**

Sentry supports three SNMP community strings that provide varying levels of access to object subset defined in the Sentry MIB. See 0SNMP for more information regarding the Sentry MIB and OID.

---

**NOTE:** The community string "public" is a reserved string for the Get community string for the NAD native SNMP support for MIB I, MIB II, and RS232 MIB objects and may not be used.

---

Community strings may be 1 to 15 characters. To preserve the string case, it must be enclosed with quotes.

---

**NOTE:** If the string is not enclosed in quotes, it will be converted to all upper case.

---

### **To clear get/set community strings:**

At the Local>> prompt, type **sentry snmp**, followed by the string identifier and "". Press **Enter**.

### **Examples**

The following command clears the Getcomm community string:

```
Local>> sentry snmp getcomm ""<Enter>
```

The following command clears the Errcomm community string:

```
Local>> sentry snmp Errcomm ""<Enter>
```

## Getcomm

The Getcomm string provides access to sentry2ChainGroup read-only MIB objects. Use of this string will open a Sentry session. The default Getcomm string is “sentry”.

### To set the Getcomm community string:

At the Local>> prompt, type **sentry snmp getcomm**, followed by the string and press **Enter**.

## Setcomm

The Setcomm string provides access to sentry2ChainGroup read-only MIB objects and the read-write sentry2PortPowerAction MIB object. Use of this string will open a Sentry session. The default Setcomm string is “sentry-set”

### To set the Setcomm community string:

At the Local>> prompt, type **sentry snmp setcomm**, followed by the string and press **Enter**.

## Errcomm

The Sentry Get community string for extended Sentry error information is defined by the Errcomm string. The Errcomm string provides access to the sentry2ErrorGroup read-only MIB objects. Use of this string will NOT open a Sentry session. The default Errcomm string is “sentry-error”

### To set the Errcomm community string:

At the Local>> prompt, type **sentry snmp errcomm**, followed by the string and press **Enter**.

## Examples

The following command sets the Setcomm community string to “Sentry Remote Power Manager set”:

```
Local>> sentry snmp setcomm "Sentry Remote Power Manager set"<Enter>
```

The following command set the Errcomm community string to “Sentry Remote Power Manager error”:

```
Local>> sentry snmp errcomm "Sentry Remote Power Manager set"<Enter>
```

## **TACACS+**

The Sentry NAD includes support for TACACS+ Authentication and Authorization.

---

**NOTE:**

1. Support is compatible with TACACS+ servers only and Accounting is only supported for Start and Stop for Telnet session in to the Sentry.
  2. For authentication support the Console and Modem ports (out-of-band), see *Enabling or disabling out-of band network authentication* in Chapter 3: Operations.
- 

Enabling this support requires the assignment of a TACACS+ server IP address and key. The following table lists and briefly describes the commands to enable and configure the NAD for TACACS+ support:

### **TACACS+ Command Summary**

---

<b>Command</b>	<b>Description</b>
Sentry tacacs server	Sets the TACACS+ server IP address
Sentry tacacs key	Sets the TACACS+ key string

---

The NAD must be reinitialized after changing TACACS+ configurations.

### **Setting the TACACS+ server IP address**

The Sentry TACACS Server command is used to set the IP address for the TACACS+ server.

---

**NOTE:**

1. Once TACACS+ support is enabled, Telnet connection to the Sentry is not possible without TACACS authentication.
  2. Use of an invalid key will prevent Telnet connection without reinitializing the NAD.
  3. If the TACACS+ server is not available, Telnet connection is not possible unless Authentication Fallback has been enabled. See Authentication Fallback for more information.
  4. With TACACS+ support enabled the standard NAD password protection acts as an additional security layer. To disable this protection see Additional Security Options.
- 

#### **To set the TACACS+ server IP address:**

At the Local>> prompt, type **sentry tacacs server**, followed by the IP address and press **Enter**.

#### ***Example***

The following command sets the TACACS+ server IP address to 64.42.31.239:

```
Local>> sentry tacacs server 64.42.31.239<Enter>
```

#### **To reset the TACACS+ server IP address:**

At the Local>> prompt, type **sentry tacacs server 0.0.0.0**

### **Setting the TACACS+ key string**

The Sentry TACACS Key command is used to set the TACACS+ key string. The string may be 1 to 32 standard keyboard characters. To preserve the string case, it must be enclosed with quotes. The key must match the key specified on the TACACS+ server or authentication will fail.

---

**NOTE:** If the string is not enclosed in quotes, it will be converted to all upper case.

---

#### **To set the TACACS+ key:**

At the Local>> prompt, type **sentry tacacs key**, followed by the key and press **Enter**.

#### ***Example***

The following set the TACACS+ key to "tacacs":

```
Local>> sentry tacacs key "tacacs"<Enter>
```

#### **To clear the trap community string:**

At the Local>> prompt, type **sentry tacacs key ""** and press **Enter**.

## SecurID

The Sentry NAD includes support for RSAs' SecurID Authentication. For more information on SecurID, go to RSA's website at [www.rsasecurity.com](http://www.rsasecurity.com).

Enabling this support requires the assignment of either a primary or secondary ACE/Server IP address. Additionally, a 'Communication Server' Sentry client must be configured in the ACE/Server Database Administration.

The following table lists and briefly describes the commands to enable and configure the NAD for SecurID support:

---

### NOTE:

1. Prior to enabling SecurID support, the Sentry unit should be fully configured and operational. The instructions provided assume a thorough understanding of the ACE/Server configuration items and processes.
  2. For authentication support the Console and Modem ports (out-of-band), see *Enabling or disabling out-of-band network authentication* in Chapter 3: Operations.
- 

### SecurID Command Summary

---

Command	Description
Sentry securid	Sets the ACE/Server IP address
Sentry securid timeout	Sets the SecurID timeout period
Sentry securid maxretry	Sets the maximum number of authentication retries
Sentry securid encryption	Sets the method of encryption
Sentry securid port	Sets the ACE/Server socket
Sentry securid factory	Resets all SecurID configurations to factory

---

The NAD must be reinitialized after changing SecurID configurations.

### Setting the ACE/Server IP address

The Sentry Securid command is used to set the primary and secondary ACE/Server IP addresses.

---

### NOTE:

1. Changing an ACE/Server IP address clears the NAD Node Secret.
  2. With SecurID support enabled the standard NAD password protection acts as an additional security layer. To disable this protection see *Additional Security Options*.
- 

#### To set the ACE/Server IP address:

At the Local>> prompt, type **sentry securid**, followed by **primary** or **secondary**, and the IP address. Press **Enter**.

#### Examples

The following sets the primary server IP address to 64.42.31.208:

```
Local>> sentry securid primary 64.42.31.208<Enter>
```

The following sets the secondary server IP address to 64.42.31.209:

```
Local>> sentry securid secondary 64.42.31.209<Enter>
```

#### To clear the ACE/Server IP address:

At the Local>> prompt, type **sentry securid**, followed by **primary** or **secondary**, and **none**. Press **Enter**.

### Setting the SecurID timeout period

The Sentry Securid Timeout command is used to set the delay between authentication request retries. The valid range for the delay parameter is 1 to 255 (in seconds). The default value for the delay is 3.

#### To set the SecurID timeout period:

At the Local>> prompt, type **sentry securid timeout**, the delay and press **Enter**.

#### Example

The following command sets the SecurID timeout to 30 seconds:

```
Local>> sentry securid timeout 30<Enter>
```

### **Setting the maximum number of retries**

The Sentry Securid Maxretry command is used to set the maximum number of authentication retries before disconnecting.

The valid range for the number of retries is 1 to 255.

The default value is 5.

#### **To set the maximum number of retries:**

At the Local>> prompt, type **sentry securid maxtry**, the max number and press **Enter**.

#### ***Example***

The following command set the maximum number of authentication retries to 10:

```
Local>> sentry securid maxtry 10<Enter>
```

### **Setting the SecurID encryption method**

The Sentry Securid Encryption command is used to select the method of encryption. This setting must match the client configuration on the ACE/Server.

#### **To set the encryption method:**

At the Local>> prompt, type **sentry securid encryption**, followed by 'SDI' or 'DES' and press **Enter**.

#### ***Example***

The following command selects the encryption method DES:

```
Local>> sentry securid encryption des<Enter>
```

### **Setting the authentication socket**

The Sentry Securid Port command is used to set the authentication socket number of the ACE/Server.

This setting must match the configured port on the ACE/Server.

The default value is 5500.

#### **To set the authentication socket:**

At the Local>> prompt, type **sentry securid port**, followed by the socket number and press **Enter**.

#### ***Example***

The following sets the authentication socket number to 4400:

```
Local>> sentry securid port 4400<Enter>
```

### **Resetting the SecurID configuration to factory**

The Sentry Securid Factory command is used to reset all Sentry SecurID configuration parameter to their factory defaults

#### **To reset the SecurID configuration:**

At the Local>> prompt, type **sentry securid factory** and press **Enter**.

### **Out-of-Band Authentication**

Sentry TACACS+ and SecurID authentication support is available for users connecting to the Sentry through the Console or Modem ports (out-of-band). When enabled, console or modem port connections are directed to the NAD for out-of-band authentication.

### **Enabling or disabling out-of-band authentication**

The command to enable or disable out-of-band authentication support is Set Netauth and is entered at the Sentry command line. See *Enabling or disabling out-of-band network authentication* in Chapter 3: Operations for more information.

### **Displaying out-of-band authentication settings**

The command to display out-of-band authentication support is Show Netauth and is entered at the Sentry command line. See *Displaying out-of-band authentication setting information* in Chapter 3: Operations for more information.

## **Authentication Fallback**

Typically during SecurID and TACACS+ operations, access is denied to Sentry if authentication fails due to the server or network path to the server being down. To mitigate this scenario, the NAD supports authentication fallback.

When enabled, instead of denying access, the NAD prompts for a local fallback password. Authentication fallback occurs after all retry attempts and timeouts.

The following table lists and briefly describes the commands to enable and configure the NAD for authentication fallback:

### **Authentication Fallback Command Summary**

<b>Command</b>	<b>Description</b>
Sentry authfallback	Enables or disables authentication fallback support
Sentry fallbackpass	Set the local fallback password

### **Enabling or disabling authentication fallback**

The Sentry Authfallback command is used to enable or disable authentication fallback.

#### **To enable or disable authentication fallback:**

At the Local>> prompt, type **sentry authfallback**, followed by **enabled** or **disabled** and press **Enter**.

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

### **Setting the fallback password**

The Sentry Fallbackpass command is used to set the authentication fallback password. The password may be 0 to 16 standard keyboard characters. To preserve the string case, it must be enclosed with quotes.

**NOTE: If the string is not enclosed in quotes, it will be converted to all upper case.**

#### **To set the authentication fallback password:**

At the Local>> prompt, type **sentry fallbackpass**, followed by the password and press **Enter**.

#### ***Example***

The following command sets the authentication fallback password to “Last chance”

```
Local>> sentry fallbackpass "Last chance"<Enter>
```

**NOTE: If the password is not set or set to blank (“”) and authentication fallback has been enabled, when a fallback occurs access to Sentry will be allowed without a password.**

## **IP Security Tables**

The Sentry NAD includes support for IP Security Tables. IP security allows administrators to restrict incoming connections by defining enabled IP sources in the IP Security Tables. IP security restrictions apply to all in-band connections to Sentry including TCP and UDP, Telnet, HTML, and SNMP.

The following table lists and briefly describes the commands to configure the NAD for IP Security Tables support:

### **IP Security Tables Command Summary**

<b>Command</b>	<b>Description</b>
Change ipsecurity	Enables or disables source IP addresses
Show ipsecurity	Displays all table entries
Delete ipsecurity	Deletes IP Security table entries

## **Enabling or disabling IP addresses**

The Change IPsecurity command is used to enable or disable IP address access to the NAD.

### **To enable or disable an IP address:**

At the Local>> prompt, type **change ipsecurity**, followed by the IP address, enabled or **disabled** and press **Enter**.

---

#### **NOTE:**

1. 255 in any segment of the IP address restricts all IP addresses in that range.
  2. **NOTE:** By default, connections are allowed unless the IP Security Table includes an entry to disable connections from that IP address. Server Technology recommends issuing the command to disable 255.255.255.255 (all addresses) **ONLY AFTER** all other table entries have been issued to avoid completely disabling access which requires resetting of the NAD to regain access.
- 

### ***Examples***

The following enables connection from 64.42.31.207:

```
Local>> change ipsecurity 64.42.31.207 enabled<Enter>
```

The following command enables connections from 64.42.31.1 to 64.42.31.254

```
Local>> change ipsecurity 64.42.31.255 enabled<Enter>
```

The following command disables connections from 64.42.31.1 to 64.42.31.254 not explicitly enabled in other table entries such as the first example:

```
Local>> change ipsecurity 64.42.31.255 disabled<Enter>
```

The following command disables connections from ALL IP addresses not explicitly enabled in other table entries such as the first example:

```
Local>> change ipsecurity 255.255.255.255
```

## **Deleting IP Security Table entries**

The Delete Ipsecurity command is used remove entries from the IP Security Table.

### **To delete a table entry:**

At the Local>> prompt, type **delete ipsecurity**, followed by the IP address entry from the table and press **Enter**.

#### ***Example***

The following command deletes the table entry for 64.42.31.207:

```
Local>> delete ipsecurity 64.42.31.207<Enter>
```

The following command deletes the table entry for 64.42.31.255:

```
Local>> delete ipsecurity 64.42.31.255<Enter>
```

## **Displaying the IP Security Table entries**

The Show Ipsecurity command is used to display current entries in the IP Security Table.

### **To display the IP Security Table:**

At the Local>> prompt, type **show ipsecurity** and press **Enter**.

#### ***Example***

The following command requests information on the IP Security Table:

```
Local>> show ipsecurity<Enter>
Address           Incoming  Outgoing  Port List
64.42.31.255      Enabled   Enabled   (All) Net Logins
64.42.31.108      Disabled  Disabled  (All) Net Logins
64.42.31.128      Disabled  Disabled  (All) Net Logins
255.255.255.255   Disabled  Disabled  (All) Net Logins
```

## **Resetting the IP Security Table**

The Delete Ipsecurity command is used to reset the IP Security Table removing all entries.

To reset the IP Security Table:

At the Local>> prompt, type **delete ipsecurity all** and press **Enter**.

## Additional Security Options

In addition to Encrypted Telnet, TACACS+, SecurID, and IP Security Tables support, the NAD implements a two-level password scheme – Login password and Privileged Mode password.

The Login password allows session access to the NAD but does not allow any configuration, while second level password, the Privileged Mode password, allows administrative rights for setting up and configuring the NAD. An administrator has the ability to change these passwords. The NAD supports disabling of the Login password, which may be useful when using third party authentication protocols such as TACACS+ or SecurID.

### Predefined Passwords

Password	Level	NAD mode
access	1	operations
system	2	privileged

**NOTE:** For security, Server Technology recommends changing the predefined passwords prior to connection to your network. See *Additional Security Options* for more information about changing passwords.

Additional security options include, redirecting or disabling session access to the NAD by Telnet on port 23, disabling and enabling inactivity timeouts.

The following table lists and briefly describes the commands used for these additional security options:

### Security Options Command Summary

Command	Description
Change telnetdest	Sets the destination port for Telnet port 23 connections
Change inactive logout	Enables/disables automatic logout due to inactivity
Change inactive timer	Sets the inactivity timer for automatic logout
Change loginpass	Changes the operations mode password
Change privpass	Changes the privileged mode password
Change incoming	Enables/disables incoming Telnet port 23 connections
Change password protect	Enables/disables password protection for serial connections
Change password incoming	Enables/disables password protection for Telnet port 2001 connections
Change password limit	Sets the number of password attempts allowed when accessing privileged mode

## Setting Level 1 & 2 passwords

The Change Loginpass and Change Privpass commands are used to set the Login and Privileged mode password, respectively. The password may be 1 to 6 alphabetic letters. To preserve the string case, it must be enclosed with quotes.

**NOTE:** If the string is not enclosed in quotes, it will be converted to all upper case.

### To set the Login password (Level 1):

At the Local>> prompt, type **change loginpass**, followed by the password and press **Enter**.

#### Example

The following sets the Login password to “LvlOne”

```
Local>> change loginpass "LvlOne"<Enter>
```

### To set the Privileged mode password (Level 2):

At the Local>> prompt, type **change privpass**, followed by the password and press **Enter**.

#### Example

The following sets the Privileged password to “LvlTwo”

```
Local>> change privpass "LvlTwo"<Enter>
```



## **Setting the number of password attempts allowed**

The Change Password Limit command is used to set the number of password attempts allowed before automatic disconnection.

The valid range for the attempt allowed is 0 (no limit) to 100.

The default value is 3.

### **To set the number of password attempts allowed:**

At the Local>> prompt, type **change password limit**, followed by the allowed number and press **Enter**.

#### ***Example***

The following set the password attempts allowed to 5:

```
Local>> change password limit 5<Enter>
```

## **Enabling or disabling the Login password**

The Change Incoming, Change Password Incoming and Change Password Protect commands are used to enable or disable the Login password for connections to port 23, port 2001 and the Sentry Connect Network command, respectively.

### **To enable or disable the password for Telnet port 23 connections:**

At the Local>> prompt, type **change incoming**, followed by **password** or **nopassword** and press **Enter**.

The default value is 'password'.

### **To enable or disable the password for Telnet port 2001 connections:**

At the Local>> prompt, type **change password incoming**, followed by **enabled** or **disabled** and press **Enter**.

The default value is 'disabled'.

### **To enable or disable the password for the Sentry Connect Network connections:**

At the Local>> prompt, type **change password protect**, followed by **enabled** or **disabled** and press **Enter**.

The default value is 'enabled'.

## **Setting the destination port for port 23 connections**

By default, connections to port 23 open an NAD operations/configuration session. It is possible to redirect the connection to open a Sentry session by default. The Change Telnetdest command is used to set the NAD destination port for connections to port 23.

### **To set port 23 to open a Sentry session:**

At the Local>> prompt, type **change telnetdest**, followed by **serial** and press **Enter**.

### **To reset port 23 to open an NAD operations/configuration session:**

Resetting the port 23 destination requires opening a Telnet session to port 7000. At the # prompt, log into the NAD and issue the following command:

At the Local>> prompt, type **change telnetdest**, followed by **console** and press **Enter**.

---

**NOTE:** Port 7000 may be used as an alternate administrative entry point to the NAD's operations/configuration interface. When connecting to port 7000, the NAD will provide a # prompt for the login password.

---

## **Enabling or disabling the inactivity timeout**

The Change Inactive Logout command is used to enable or disable the inactivity timeout.

---

**NOTE:** For serial pass-through connection from the Sentry command line, the Sentry inactivity timeout is NOT enforced. However, if enabled the NAD inactivity timer remains enforced for better security for serial pass-through connections.

---

### **To enable or disable the inactivity timeout:**

At the Local>> prompt, type **change inactive logout**, followed by **enabled** or **disabled** and press **Enter**.

## **Setting the inactivity timer**

The Change Inactive Timer command is used to set the inactivity timer.  
The valid timer range is 5 to 60 seconds OR 1 to 120 minutes.  
The default value is 5 minutes.

### **To set the inactivity timer:**

At the Local>> prompt, type **change inactive timer**, followed by the timer range and **s** (seconds) or **m** (minutes). Press **Enter**

### **Examples**

The following command sets the inactivity timer to 45 seconds:

```
Local>> change inactive timer 45s<Enter>
```

The following command sets the inactivity timer to 20 minutes:

```
Local>> change inactive timer 20m<Enter>
```

## **Resetting to Factory Defaults**

You may reset the non-volatile RAM that stores all configurable NAD options. This resets all command line configurable options and passwords to their default values.

You may reset the NAD to factory defaults by issuing a command at the Local>> prompt or by pressing the reset button on the Sentry RPM. You must be in Privileged mode to issue the command. Using the reset button may be necessary when a forgotten password prevents administrator login. Either method updates the current working configuration to the factory defaults.

### **To reset the NAD to factory defaults from the command line:**

At the Local>> prompt, type **initialize factory** and press **Enter**.

### **To reset the NAD to factory defaults using the reset button:**

See 0Resetting to Factory Defaults.

---

**NOTE:** Resetting the NAD using the reset button resets the ALL configurable options for the NAD AND the Sentry RPM

---

## Modem

The Sentry integrated Modem, available in some Sentry RPM models, is a v.92 (56K) Global Security Modem and provides out-of-band access to the Sentry Remote Power Manager. The Sentry integrated Modem additionally supports Callback Security.

---

**NOTE:** Sentry RPMs with integrated modems manufactured prior to June 30, 2003 may contain older OEM modem modules. Use the ATI3 command to positively identify the type of integrated modem; the new Security Modem will display 'MT5634SMI' in the response string. For support on configuring older modems, please contact Technical Support.

---

**NOTE:** Sentry RPMs with integrated modems are equipped with an RJ12 Telco connector in place of the standard DB9-male Modem connector with the exception for R40x and R41x models with the optional integrated Ethernet and the R480. These models have a 2-pin DB9 male Telco connector and ship standard with a DB9 to RJ12 Telco adapter. Adapters required to convert these connections for country specific use are the responsibility of the customer.

---

The following table lists and briefly describes the commands to configure the Sentry to initialize the integrated Modem:

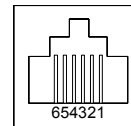
### Modem Command Summary

Command	Description
Connect Modem	Connects serially to the modem for configuration
Set Modem	Configures the Sentry modem initializations
Show Modem	Displays the Sentry configured data-rate and initialization string status

These commands are issued from the Sentry prompt and are described in detail in Chapter 3: Operations.

### Modem Connection Port

Pin	Signal Name
3	Tip
4	Ring



### Initial Configuration

The Sentry integrated Modem requires no initial configuration, with the exception of the Country Code, to operate as a standard modem without the optional security mechanisms enabled; Callback Security is disabled by default.

Provided are instructions to configure the modem through a serial connection from the Sentry: prompt. The instructions below assume that the default password has not been changed.

### Predefined Setup Password

Password
MTSMODEM

---

**NOTE:** For security, Server Technology recommends changing the predefined password prior to connection to your network. See *Additional Security Options* for more information about changing password.

---

### To initially configure the modem:

1. At the Sentry: prompt, type **connect modem** and press **Enter**.
2. After receiving the Connection Complete banner, type **ate1q0v1** and press **Enter**. This enables the modem's command echo and enables verbose result code mode.
3. Type **at#sMTSMODEM** and press **Enter**.  
If the password is incorrect, the modem will display **ERROR**.
4. Type **at%t19,0**, followed by the appropriate Country Code (see page 64) and press **Enter**.
5. Type **ati19** and press **Enter** to verify the configured Country Result Code.
6. Type **atz** and press **Enter** to reset the modem with the new settings.
7. Type **!\*login** and press **Enter** to break the Sentry serial connection to the modem. The Sentry will display the **Disconnecting...** banner and return to the Sentry username: prompt.

---

**NOTE:** Server Technology recommends use of the ATZ command after any configuration changes to insure that they are stored and that the modem is reinitialized with them.

---

## Logging in

You may log directly into the Sentry integrated Modem to configure the Country Code, enable Callback Security or other features. To log into the modem follow steps 1 through 3 from *To initially configure the modem*.

## Setting the setup password

The modem command AT#S= command is used to set the Setup password. The password may be 1 to 8 characters and is case sensitive.

### To set the Setup password:

After successfully logging into the modem, type **at#s=**, followed by the password and press **Enter**.

Type **atz** and press **Enter** to reset the modem with the new settings.

### Example

The following set the Setup password to “OpenUp”:

```
at#s=OpenUp<Enter>
OK
atz<Enter>
OK
```

## Configuring the Country Code

The Sentry integrated Modem is compliant for use per Telecom Certification for the countries listed in the following table. The AT%T19,0, command is used to set the country code. The default value is 34.

**NOTE: For countries not listed, please contact Technical Support.**

### Country Codes (Approved as of February 2003)

Country	Code	Result Code	Country	Code	Result Code
Argentina	34	52	Japan	10	16
Australia	1	1	Liechtenstein	34	52
Austria	34	52	Luxembourg	34	52
Belgium	34	52	Malaysia	30	48
Brazil	34	52	Mexico	34	52
Canada	34	52	Netherlands	34	52
Chile	34	52	New Zealand	9	9
China	34	52	Norway	34	52
Cyprus	34	52	Philippines	30	48
Czech Republic	25	37	Poland	30	48
Denmark	34	52	Portugal	34	52
Estonia	34	52	Russia	34	52
Finland	34	52	Singapore	30	48
France	34	52	Slovak Republic	30	48
Germany	34	52	South Africa*	35	53
Greece	34	52	South Korea	34	52
Hong Kong	99	48	Spain	34	52
Hungary	99	48	Sweden	34	52
Iceland	34	52	Switzerland	34	52
India	30	48	Taiwan	34	52
Indonesia	30	48	Thailand	34	52
Ireland	34	52	Turkey	34	52
Israel	30	48	United Kingdom	34	52
Italy	34	52	United States	34	52

\*Compliance requires use of an approved surge protection device in conjunction with modem.

### To configure the country code:

After successfully logging into the modem, type **at%t19,0**, followed by the country code and press **Enter**.

Type **atz** and press **Enter** to reset the modem with the new settings.

#### **Example**

The following command sets the modem for compliance in Singapore:

```
at%t19,0,30<Enter>
OK
atz<Enter>
OK
```

### To verify the configured country code:

Type **ATI19** and press **Enter**. The displayed Result Code should match the code listed in the previous table.

## **Enabling or disabling Callback Security**

Callback Security provides a higher level of security against unauthorized access by requiring the connecting user to be at a predefined location when establishing a modem session to the Sentry.

When enabled, Callback Security requires submission of a valid callback password at initial connection. This password is compared to a predefined callback number/password table for a return call by the modem. The modem then terminates the initial connection and returns the call to the predefined number associated with the supplied password and upon reconnection the user is required to resubmit the callback password before proceeding with the Sentry username/password authentication.

The **AT#CBS** command is used to enable or disable Callback Security.

---

**NOTE:** To use Callback Security, Auto-answer must be enabled on the calling modem (S0=1).

---

### To enable Callback Security:

After successfully logging into the modem, type **at#cbs2** and press **Enter** to enable Callback Security.

Type **at&w** and press **Enter** to store the settings in nonvolatile memory.

Type **atz** and press **Enter** to reset the modem with the new settings.

#### **Example**

The following commands enable Callback Security:

```
at#cbs2<Enter>
OK
at&w<Enter>
OK
atz<Enter>
OK
```

### To disable Callback Security:

Type **at#cbs0** and press **Enter** to disable Callback Security.

Type **at&w** and press **Enter** to store the settings in nonvolatile memory.

Type **atz** and press **Enter** to reset the modem with the new settings.

#### **Example**

The following commands disable Callback Security:

```
at#cbs0<Enter>
OK
at&w<Enter>
OK
atz<Enter>
OK
```

## **Setting Callback dial strings**

The Sentry integrated Modem supports definition of up to 30 callback dial strings.

The AT&Z command is used to set a dial string. Dial strings may be up to 34 characters and may include other AT commands.

### **To set a Callback dial string:**

After successfully logging into the modem, type **at&z**, followed by the memory location (0-29), **=at**, **dt** (tone-dial) or **dp** (pulse-dial) and the number/dial string. Press **Enter**.

### **Examples**

The following command sets the dial string for memory location 0 to tone-dial, 1-775-284-2000:

```
at&z0=atdt17752842000<Enter>
```

The following command sets the dial string for memory location 29 to pulse-dial, 1-775-555-1212:

```
at&z29=atdp17755551212<Enter>
```

### **To verify and reset the modem with the configured dial strings:**

Type **at&v** and press **Enter**.

Type **atz** and press **Enter**.

---

**NOTE:** Callback Security dial strings may also be configured to allow a user to bypass the stored number with a dynamic entry or make a direct connection without a callback. Server Technology does not recommend the use of these options as they have a negative effect on security for the modem connection.

To enable these options additional characters are required when setting a dial string:

- + enables dynamic callback dial string entry
- enables direct connection without a callback
- ,?? Used with '+' enables use of dynamic extension entry

### **Examples**

The following command enables dynamic callback string and extension entry where the extension length is 5 characters:

```
at&z0=+atdt17752842000,?????<Enter>
```

The following command enables direct connection without a callback:

```
at&z0=-atdp17755551212<Enter>
```

---

## **Setting Callback passwords**

The AT#CBN command is used to set a password for each of the Callback dial string previously defined. Passwords must be unique and 6 to 10 characters in length.

---

**NOTE:** Passwords are case-sensitive and may not include the + or - characters and must be unique.

---

### **To set a Callback password:**

After successfully logging into the modem, type **at#cbn**, followed by the memory location (0-29), **=** and the password. Press **Enter**.

Type **atz** and press **Enter** to reset the modem with the new settings.

### **Examples**

The following commands set the password for memory location 0 to 'password':

```
at#cbn0=password<Enter>
OK
atz<Enter>
OK
```

The following command sets the password for memory location 29 to 'WhOduNnIt':

```
at#cbn29=WhOduNnIt<Enter>
OK
atz<Enter>
OK
```

### **To verify the configured password:**

Type **at&v** and press **Enter**.

## **Resetting a Callback memory location**

The AT#CBR command is used to reset the dial string and password for any given memory location.

To reset a Callback memory location:

Type **at#cbx**, followed by the memory location (0-29), and press **Enter**.

Type **atz** and press **Enter** to reset the modem with the new settings.

### ***Example***

The following commands reset memory location 0:

```
at#cbr0<Enter>
OK
atz<Enter>
OK
```

## **Setting the maximum Callback attempts**

The AT#CBA command is used to set the maximum number of callback attempts the modem will make. The valid range for Callback attempts is 1 to 255. The default value is 4.

To set the maximum Call back attempts:

Type **at#cba**, followed by the maximum number of attempts and press **Enter**.

Type **atz** and press **Enter** to reset the modem with the new settings.

### ***Example***

The following command sets the maximum Callback attempts to 1:

```
at#cbal<Enter>
OK
atz<Enter>
OK
```

## **Setting the Callback delay**

The AT#CBD command is used to set the length in time the modem waits before attempting a callback. The valid range for the delay is 1 to 255 in seconds. The default value is 15.

To set the Callback delay:

Type **at#cbd**, followed by the delay (in seconds) and press **Enter**.

Type **atz** and press **Enter** to reset the modem with the new settings.

### ***Example***

The following command sets the Callback delay to 30 seconds:

```
at#cbd30<Enter>
OK
atz<Enter>
OK
```

## **Displaying Callback failed attempts counter**

The Sentry integrated Modem counts the number of failed Callback passwords attempts since a reset or power-up. The AT#CBF command is used to display this count.

---

**NOTE:** The &W command may be used with the AT#CBF command to store this number in nonvolatile memory.

---

### **To display the failed attempts counter:**

Type **at#cbf** and press **Enter**.

Type **atz** and press **Enter** to reset the modem with the new settings.

## **Resetting the Callback failed attempts counter**

The AT#CBFR command is used to reset the Callback failed attempts counter.

### **To reset the failed attempts counter:**

Type **at#cbfr** and press **Enter**.

Type **atz** and press **Enter** to reset the modem with the new settings.

## **Callback Security Calling Procedures**

### **Standard - Predefined Location Only**

Use the following steps when calling from a fixed location predefined in the Callback Security tables.

1. Using a communications program such as Hyper Terminal, dial the number of the integrated modem in the Sentry unit.
2. At the Password> prompt, enter the password for the number being connected from and press **Enter**.

When a valid password is provided, OK `Disconnecting` is displayed and the Sentry integrated modem disconnects.

3. After the specified Callback delay has elapsed, the Sentry integrated modem attempts to connect with the Callback dial string associated with the supplied password.  
**NOTE: If unable to establish a connection, the modem will retry until the maximum Callback Attempts has been reached.**
4. After the modem reconnects, at the Password> prompt, re-enter the predefined password for the number being connected from and press **Enter**.

When a valid password is provided, OK `Connecting` is displayed and access to the Sentry is granted.

You are given three attempts to enter a valid password. If all three attempts fail, the modem will automatically disconnect.

### **Dynamic Callback number entry**

Mobile users may need to use this procedure when connecting from a number different than the one stored with the password. The + option must have been used in the original configuration of the Callback dial string. See *Setting Callback dial strings* on page 66 for more information.

1. Use the standard procedure with the following deviation.
2. At the Password> prompt, enter the password for a number entry enabled number, followed by +, and the new dial string (ex: atdt7752842065). Press **Enter**.

When a valid password is provided, OK `Disconnecting` is displayed and the Sentry integrated modem disconnects.

The procedure continues as noted in #3 and 4 above.

### **Dynamic Callback extension entry**

Users may need to use this procedure an extension number must be provided for the dial string being called from. The + and ,??? options must have been used in the original configuration of the Callback dial string. See *Setting Callback dial strings* on page 66 for more information.

1. Use the standard procedure with the following deviation.
2. At the Password> prompt, enter the password for an extension entry enabled number, followed by +, and the required extension number. Press **Enter**.

When a valid password is provided, OK `Disconnecting` is displayed and the Sentry integrated modem disconnects.

The procedure continues as noted in #3 and 4 above.

### **Direct connection without Callback**

Use this procedures to make a direct connection to the integrated modem without a callback. The - option must have been used in the original configuration of the Callback dial string. See *Setting Callback dial strings* on page 66 for more information.

1. Use the standard procedure with the following deviation.
2. At the Password> prompt, enter the predefined password for the number being connected from, followed by -, and press **Enter**.

When a valid password is provided, OK `Connecting` is displayed and access to the Sentry is granted.

You are given three attempts to enter a valid password. If all three attempts fail, the modem will automatically disconnect.



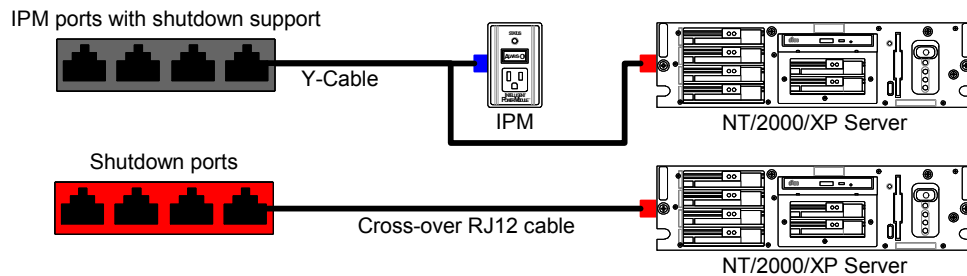
## Sentry Shutdown

Available in specific Sentry RPM models, Sentry's Shutdown feature provides the option to initiate an orderly shutdown of remote Windows NT/2000/XP servers, protecting open application files prior to the server being powered down.

**NOTE:** Sentry Shutdown also has been shown to be compatible with certain Novell Netware systems. Please contact Technical Support for more information.

### Connections

Sentry RPMs featuring this additional feature come equipped with red Shutdown ports, black external IPM (Intelligent Power Module) ports with Shutdown support or both.

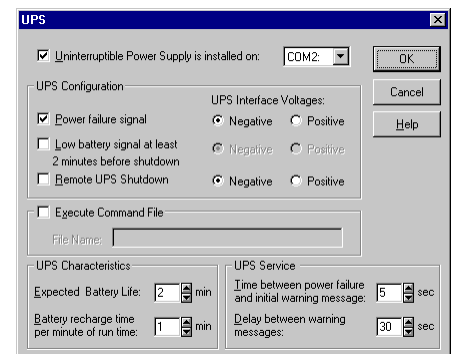
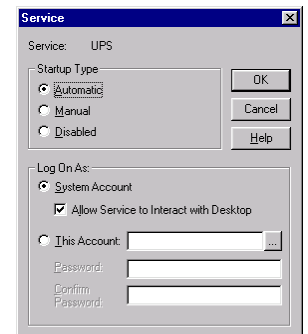
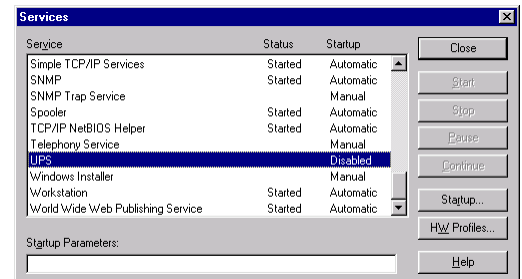


**NOTE:** Y-Cable connectors are NOT reversible. The blue RJ connects to the IPM and the red RJ, with the provided Shutdown adapter, connects to a UPS signal serial port on the Windows server.

### Configuring Windows

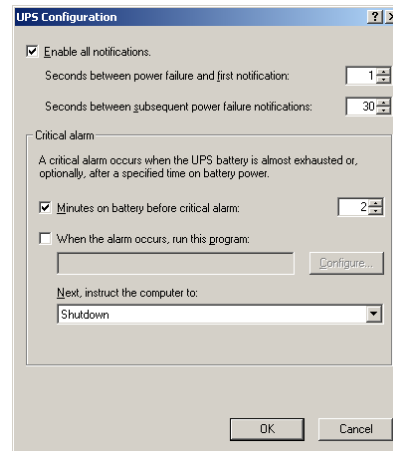
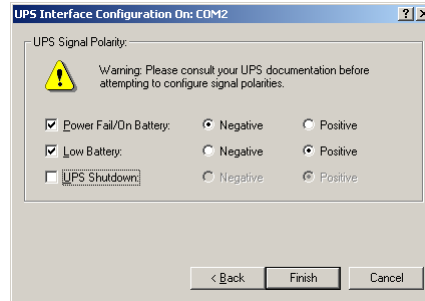
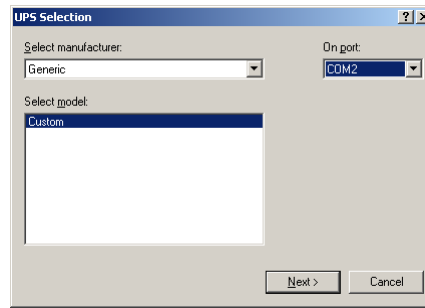
#### NT: v3.51 and later

1. Double-click **Services** from the Windows Control Panel.
2. In the Services window, select **UPS** in the Service List and press **Startup**.
3. In the Service window:
  - In the Startup Type field, select **Automatic**.
  - In the Log On As field, select **System Account** and **Allow Service to Interact with Desktop**.
  - Press **OK**.
4. In the Services window, press **Close**.
5. Double-click **UPS** from the Windows Control Panel.
6. In the UPS window:
  - Select **Uninterruptible Power Supply is installed on** and the COM port that the Shutdown signal cable is attached to.
  - In the UPS Configuration field, select **Power failure signal**. Select **Negative** for all UPS Interface Voltages.
  - Set the **Expected Battery Life** value. This value MUST be less than the Shutdown Delay value set on the Sentry Control Screen. See *Using the Control Screen* in Chapter 3: Operations for more information on setting the Shutdown delay.
  - Press **OK**.



For Windows 2000, Service Pack 1 or later is required. **NOTE:** To verify the status of Windows 2000, right-click **My Computer** from the desktop and select **Properties**. If no Service Packs are indicated, contact your system administrator or Microsoft for an update.

1. Double-click **Power Options** from the Windows Control Panel.
2. In the Power Options Properties window, select the **UPS** tab and in the Details field, press **Select...**
3. In the UPS Selection window:
  - In the Select manufacturer: field, select **Generic**.
  - In the Select model: field, select **Custom**.
  - In the On port: field, select the COM port the Shutdown signal cable is attached to.
  - Press **Next>**.
4. In the UPS Interface Configuration On window:
  - Select **Power Fail/On Battery** with a signal polarity of **Negative**.
  - Select **Low Battery** with a signal polarity of **Positive**.
  - Press **Finish**.
5. In the Power Options Properties window, select the **UPS** tab and in the Details field, press **Configuration...**
6. In the UPS Configuration window:
  - Select **Enable all notifications**.
  - Set the seconds between fields to **1** and **30**.
  - Select **Minutes on battery before critical alarm** and set value. This value **MUST** be less than the Shutdown Delay value set on the Sentry Control Screen. See *Using the Control Screen* in Chapter 3: Operations for more information on setting the Shutdown delay.
  - Press **OK**.
7. In the Power Options Properties window, press **OK**.



## **Testing the Configuration**

### **Loopback Test**

1. Remove the Shutdown signal cable from the provided adapter that is connected to the serial port on the server.
2. Insert the provided RJ12 loopback test plug into the adapter.

Insertion of the loopback test plug should initiate a UPS Service shutdown. Within 10 to 15 seconds, a Messenger Service window should appear to indicate that a power failure has occurred. The server should then begin to shutdown after the delay set in *Configuring Windows* step 6 has expired.

If a Messenger Service window does NOT appear:

- the UPS Service is configured incorrectly,
- the serial port selection is not correct, or
- the serial port is in conflict with another device.

Recheck all configuration settings/connections and test the configuration again.

---

**NOTE: DO NOT** reconnect the Shutdown signal cable or proceed to the Sentry Shutdown Test until the Loopback Test properly initiates a shutdown.

---

### **Sentry Shutdown Test**

1. Remove the loopback test plug and reattach the Shutdown signal cable.
2. Login to the Sentry Remote Power Manager.
3. At the Sentry prompt., type **show** and press **Enter**.
4. On the Control Screen, position the cursor in the Shtdwn field of the Control Status for the server's Intelligent Power Module port and press **Space**.

The x in the On field should change to an s and the Shtdwn field to Off. This indicates that the power is still on and that the UPS Service shutdown signal is being asserted.

Within 10 to 15 seconds, a Messenger Service window should appear to indicate that a power failure has occurred. The server should then begin to shutdown after the delay set in *Configuring Windows* step 6 has expired.

After the Shutdown Delay previously set at the Control Screen has expired, the Sentry will then set the Control Status for that port to Off.

## **Automatic Logon**

At boot, Windows operating systems often require a logon user and password. For remote booting this can pose a problem since a user is not present at the system to enter the appropriate logon information.

The operating system, however, can be configured to automatically logon at boot. Instructions for enabling and configuring the Windows Automatic Logon feature are available from the Microsoft Support Knowledge Base. Three Knowledge Base articles are listed below.

---

**NOTE:** All question related to the Windows Automatic Logon feature should be directed to Microsoft Support. Server Technology does not offer technical support for this feature.

---

Article Number:	Q97597
Article Title:	How to Enable Automatic Logon in Windows NT 3.x and 4.0
Applications:	Windows NT Server/Workstation 3.5/4.0, Windows 2000 Server
Article Number:	Q234562
Article Title:	How to Enable Automatic Logon in Windows 2000
Applications:	Windows 2000 Professional
Article Number:	Q315231
Article Title:	How to Enable Automatic Logon in Windows
Applications:	Windows XP Home Edition/Professional/64-Bit Edition

## SNMP

A Sentry Remote Power Manager with an internal Network Access Device supports the Simple Network Management Protocol (SNMP). This allows network management systems to use SNMP requests to retrieve information and control power for the individual ports on the Sentry. See *SNMP* in *Network Access Device* for information on enabling SNMP support.

The Network Access Device includes an SNMP v1 agent supporting standard MIB I, MIB II, and RS-232 MIB objects. A private enterprise MIB extension (Sentry MIB) is also supported to provide remote power control.

---

**NOTE:** For security, Sentry MIB extensions are disabled by default.

---

The Sentry MIB defines objects to allow query of Sentry configuration items and port status, control of port power states, and SNMP traps.

### **MIB, OID and Support**

The Sentry SNMP MIBs and OIDs are available on the Server Technology website:

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

SNMP support is available 8:30AM and 5:00 PM Pacific Time, Monday-Friday.

For SNMP Support:

Email: `mibmaster@servertech.com`

### **SNMP Support**

Sentry SNMP support must be enabled for access to Sentry2 MIB objects and generation of all Sentry2 traps. See *SNMP* in *Network Access Device* for information on enabling and configuring Sentry for SNMP support.

### **Traps**

Sentry Remote Power Managers support five types of SNMP traps.

SNMP traps are enabled at either the board (page) or port level. See *Page field* and *Port Naming and Grouping* in Chapter 3: Operations for more information on pages and ports. The following table lists and briefly describes when each trap is generated. The letter (B) indicates a board level trap and (P) indicates a port level trap.

#### **Trap Summary**

Name	Level	Description
Strt	B	Sentry startup
Temp	B	Temperature out of limit (Temperature probe equipped Sentry RPMs only)
Msta	P	Module status error or change
Csta	P	Control status change
Load	P	Device load out of limit

All traps include the Location of the Sentry RPM as defined with the Set Location command. See *Creating a location description and login banner* in Chapter 3: Operations for more information.

Sentry SNMP implementation recognizes and transmits new trap conditions immediately upon generation with limitations. These limitations are:

1. To prevent network congestion, trap conditions in a steady state (continuous error condition) only generate traps once every timer period (one minute by default). See *Setting the trap timer* for more information.
2. Traps can only be transmitted when there is no active user session or pass-through serial connection. Traps occurring during any open session are transmitted when all sessions are closed.
3. Multiple trap conditions of the same type occurring during a single open session will be transmitted with only a single trap message indication.

#### **Example**

With the Control Status trap, when a user initiates a session and turns a single port on and off several times, only one Control Status trap message will be generated indicating the change to the last control state when the session is ended.

## **Startup trap**

The Strt trap is generated whenever the Sentry RPM completes a power up. Strt traps include the Location of the Sentry RPM.

The Strt trap can only be enabled for page .a on the Sentry RPM.

## **Temperature trap**

The Temp trap is generated whenever the temperature (Celsius) on temperature probe equipped Sentry RPMs exceed preset limits. Temp traps include the reported temperature, Location of the Sentry RPM and identifier and name of the affected page. See *Setting the temperature limits* for more information on setting limits for the Temp trap.

The Temp trap can only be enabled for page .a on the Sentry RPM.

Three Temp traps can be generated:

1. Temperature out of limits high.
2. Temperature out of limits low.
3. Temperature is normal range.

Exceeding the preset limits immediately generates the out-of-limits trap and triggers the trap timer. See *Setting the trap timer* for more information. A new out-of-limits trap will be generated at the expiration of each timer period until the temperature returns to and remains within the preset limits until expiration of the timer period at which time a normal-range trap will be generated.

### ***Example***

Preset Limits: High – 100 C, Low – 80 C, Trap timer – 1 minute.

If the temperature rises to 101 C, an out-of-limits-high trap is generated. The out-of-limits-high trap is generated at the end of every timer period until the temperature falls back to and remains below 100 C until the end of a period. At this time, a normal-range trap is generated. No additional traps will be generated until the temperature exceed the preset limits again.

## **Module Status trap**

The Msta trap is generated when an error condition occurs on a port. Msta traps include the reported port Module Status, the Location of the Sentry RPM and identifier and name of the affected port.

Four Msta traps can be generated: Normal, No Response, OnS Fail, Off Fail. See *Module Status field* in Chapter 3: Operations for more information on Module Status.

Any non-Normal status generates an Msta trap and triggers the trap timer. A new non-Normal trap is generated at the end of every timer period until the Module Status returns to and remains Normal until the end of a period at which time a Normal trap will be generated.

## **Control Status Change trap**

The Csta trap is generated whenever the control state of a port is changed. Csta traps include the reported port Control Status, Location of the Sentry RPM and identifier and name of the affect port.

---

**Note:** Csta traps are not generated until an active session is ended. And for ports experiencing multiple state changes, only a single trap will be generated indicating the last control status value.

---

## **Device Load Limit Trap**

The Load trap is generated whenever the total output load on a Sentry RPM port exceeds preset limits for that port. Load traps include the reported output load, Location of the Sentry RPM and identifier and name of the particular port. See *Setting the device load limits* for more information on setting limits for the Load trap.

Three Load traps can be generated:

1. Load out of limits high.
2. Load out of limits low.
3. Load in normal range.

Exceeding the preset limits immediately generates the out-of-limits trap and triggers the trap timer. A new out-of-limits trap will be generated at the expiration of each timer period until the input load returns to and remains within the preset limits until expiration of the timer period at which time a normal-range trap will be generated.

## Commands

All Sentry SNMP commands require administrative privileges and are entered from the Sentry: prompt. The following table lists and briefly describes each command.

### Command Summary

Command	Description
List Trap	Lists current trap settings
Set Disablet	Disables a trap
Set Enablet	Enables a trap
Set Loadh	Sets the output load-sense trap high limit
Set Loadl	Sets the output load-sense trap low limit
Set Temph	Sets the temperature trap high limit
Set Templ	Sets the temperature trap low limit
Set Traptime	Sets the delay for steady state condition traps

### Enabling a trap

The Set Enablet command enables an SNMP trap to one or all boards/ports.

When the command completes successfully, the following message appears, where **x** indicates the number of pages or ports:

```
Trap Enabled/Disabled or Trap Time value set on x boards(s)/port(s)
Command Completed Successfully
```

#### To enable a trap:

At the Sentry: prompt, type **set enablet**, followed by the trap name and a page or port name. Press **Enter**, or

Type **set enablet**, followed by the trap name and a group name. Press **Enter**, or

Type **set enablet**, followed by the trap name, then **all**. Press **Enter**.

#### Examples

The following enables the Module Status trap for the fourth port using the ports' absolute name:

```
Sentry: set enablet msta .a4<Enter>
```

The following enables the Control Status Change trap for all the ports in the group named ops\_srv:

```
Sentry: set enablet csta ops_srv<Enter>
```

The following enables the Load trap for all pages:

```
Sentry: set enablet load all<Enter>
```

### Disabling a trap

The Set Disablet command disables an SNMP trap to one or all boards/ports.

When the command completes successfully, the following message appears, where **x** indicates the number of pages or ports:

```
Trap Enabled/Disabled or Trap Time value set on x boards(s)/port(s)
Command Completed Successfully
```

#### To disable a trap:

At the Sentry: prompt, type **set disablet**, followed by the trap name and a page or port name. Press **Enter**, or

Type **set disablet**, followed by the trap name and a group name. Press **Enter**, or

Type **set disablet**, followed by the trap name, then **all**. Press **Enter**.

## Examples

The following disables the Startup trap for the first page using the pages' absolute name:

```
Sentry: set disable strt .a<Enter>
```

The following disables the Module Status trap for all the ports in the group named ops\_srv:

```
Sentry: set disable msta ops_srv<Enter>
```

The following disables the Temperature Limit trap for all pages:

```
Sentry: set disable temp all<Enter>
```

## **Setting the device load limits**

The Set Loadh and Set Loadl commands set the upper and lower load limits for the Device Load Limit trap. The valid range for the load limit parameter is 0 to 240 (in amperes).

When command completes successfully, the following message appears, where x indicates the number of pages or ports:

```
Limit value set successfully on x boards(s)/port(s)  
Command Completed Successfully
```

### **To set an upper load limit:**

At the Sentry: prompt, type **set loadh**, followed by the port name and load limit. Press **Enter**, or

Type **set loadh**, followed by the load limit, then **all** and press **Enter**.

### **Example**

The following command sets the upper load limit for port A1 to 10:

```
Sentry: set loadh .a1 10<Enter>
```

### **To set a lower load limit:**

At the Sentry: prompt, type **set loadl**, followed by the port name and load limit. Press **Enter**, or

Type **set loadl**, followed by the load limit, then **all** and press **Enter**.

### **Example**

The following command sets the lower load limit for all ports to 5:

```
Sentry: set loadl all 5<Enter>
```

## **Setting the temperature limits**

The Set Temph and Set Templ commands set the upper and lower temperature limits for the Temperature trap. The valid range for the temperature limit parameter is 0 to 125 (in degrees Celsius).

When command completes successfully, the following message appears, where x indicates the number of pages or ports:

```
Limit value set successfully on x boards(s)/port(s)  
Command Completed Successfully
```

### **To set an upper temperature limit:**

At the Sentry: prompt, type **set temph**, followed by the page name and temperature limit. Press **Enter**.

### **Example**

The following command sets the upper temperature limit for page A to 100:

```
Sentry: set temph .a 100<Enter>
```

### **To set a lower temperature limit:**

At the Sentry: prompt, type **set templ**, followed by the page name and temperature limit. Press **Enter**.

### **Example**

The following command sets the lower temperature limit for page A to 50:

```
Sentry: set templ .a 50<Enter>
```

## Setting the trap timer

The Set Traptime command sets the timer period between SNMP traps in a steady state. The valid range for the timer period is 1 to 254 (in minutes).

The default value for the trap timer is 1 minute.

When the command completes successfully, the following message appears, where **x** indicates the number of pages or ports:

```
Trap Enabled/Disabled or Trap Time value set on x boards(s)/port(s)
Command Completed Successfully
```

### **To set the trap timer:**

At the Sentry: prompt, type **set traptime**, followed by the timer period and press **Enter**.

### **Example**

The following sets the timer period between steady state SNMP traps to 3 minutes:

```
Sentry: set traptime 3
```

## Displaying trap information

The List Traps command displays information about traps for one or all pages. This information includes:

- Absolute page name
- Page level traps enabled/disabled status
- Temperature and Input Load limit values
- Absolute port names associated with the page
- Port level traps enabled/disabled status
- Trap Timer value

---

**Note:** The Device Load trap and limits although displayed are NOT supported by the Sentry RPM.

---

### **To display trap information about one page:**

At the Sentry: prompt, type **list traps**, followed by the page name and press **Enter**.

### **To display trap information about all pages:**

At the Sentry: prompt, type **list traps**, then **all** and press **Enter**.

### **Examples**

The following command requests trap information about page B:

```
Sentry: list traps .b<Enter>

TRAP INFORMATION FOR BOARD: .B
Sentry Start Up Trap: N/A Temperature Trap: N/A Input Load Trap: [ ]
Temperature High Limit: 100 Deg C Temperature Low Limit: 50 Deg C
Input Load High Limit: 30 Amp(s) Input Load Low Limit: 10 Amp(s)
          .B1 .B2 .B3 .B4
Control Status Trap [X] [ ] [ ] [ ]
Module Status Trap [X] [ ] [ ] [ ]
Device Load Temp   [ ] [ ] [ ] [ ]
Load High Limit    250 250 250 250
Load Low Limit     0   0   0   0
Trap Time Value (in minutes) is 3
List Complete
```

The display indicates that page B has Temperature trap high-low limits of 100-50 degrees Celsius. For port B1, the display indicates that the Control Status and Module Status traps are enabled. Also, the Trap Timer value is set for three minutes.



The following command requests trap information about all pages:

```
Sentry: list traps all<Enter>

TRAP INFORMATION FOR BOARD: .A
Sentry Start Up Trap: [X] Temperature Trap: [X] Input Load Trap: [ ]
Temperature High Limit: 100 Deg C   Temperature Low Limit: 50 Deg C
Input Load High Limit: 240 Amp(s)   Input Load Low Limit: 0 Amp(s)
                                     .A1 .A2 .A3 .A4
Control Status Trap [X] [ ] [ ] [ ]
Module Status Trap  [X] [ ] [ ] [ ]
Device Load Temp    [X] [ ] [ ] [ ]
Load High Limit     30  250 250 250
Load Low Limit      0   0   0   0
Trap Time Value (in minutes) is 3
Press: N)ext, Q)uit:
```

The first screen of the resulting display indicates that page A has the Startup, Temperature trap enabled and Temperature trap high-low limits of 100-50 degrees Celsius. For port A1, the display indicates that the Control Status, Module Status and Device Load, with high-low limits of 30-0 amperes are enabled, traps. Also, the Trap Timer value is set for three minutes. The page ends with a prompt to continue with the display for the next page, B, or quit and return to the Sentry: prompt.

## External Intelligent Power Modules

Sentry Remote Power Managers are able to perform the advanced power management functions by communicating to Intelligent Power Modules (IPMs). IPMs contain all hardware and logic required to control the power output connector on the IPM as well as monitor and report port operating states.

Sentry RPMs have either integrated IPMs, support for external IPMs or a combination of both.

External IPMs are designed for in-line connection between the power source and the device to be powered and they are controlled by the Sentry RPM using a supplied RJ12 crossover cable. External IPMs also feature an LED for IPM power status. See *Port Status* in 0Technical Specifications for more information on the port status LED.

### Standard Models

Model	Voltage	Features	Inlet	Outlet
IPM3-0-3	100-120V AC 50/60 Hz	10 Amp	IEC 60320 C14	IEC 60320 C13
IPM3-R-3	100-120V AC 50/60 Hz	10 Amp w/ retainer clips	IEC 60320 C14	IEC 60320 C13
IPM5-0-2	208-240V AC 50/60 Hz	6 Amp	IEC 60320 C14	IEC 60320 C13
IPM5-0-2	208-240V AC 50/60 Hz	6 Amp, w/ retainer clips	IEC 60320 C14	IEC 60320 C13
PM20-0-1	100-120V AC 50/60 Hz	16 Amp, w/ retainer clips	IEC 60320 C14	IEC 60320 C20
PM20-0-2	208-240V AC 50/60 Hz	16 Amp, w/ retainer clips	IEC 60320 C20	IEC 60320 C19
PM48-0-1	-48V DC	20 Amp	Screw down terminal	Screw down terminal

**NOTE:**

1. IPM rack mounting kits are available. Contact your Server Technology Sales Representative for more information.
2. For more information regarding inlet/outlet specifications, please go to Panel Components at [www.panelcomponents.com](http://www.panelcomponents.com).

## R480-0-x

The Sentry Commander model R480-0-x is a unique model in the Sentry product family of Remote Power Managers. It features two serial access communication paths, two serial pass-through communication ports, 2 internal power outputs and support for two external IPMs. It is also offered with optional support for out-of-band access with an integrated modem.

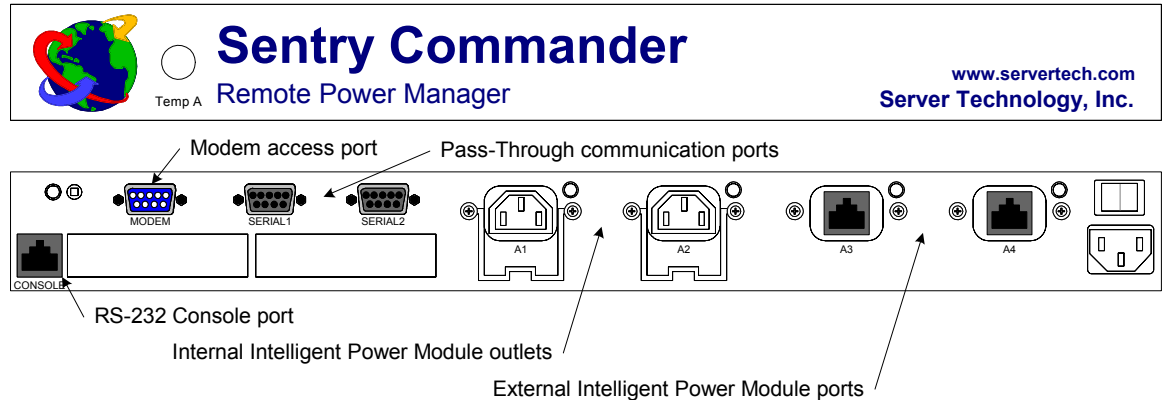
---

**NOTE:** The R480-0-x does NOT support an optional integrated Ethernet solution.

---

The R480-0-x is nearly functionally identical to the rest of the Sentry RPM family, however there are some physical and operational differences.

### Equipment Overview



The temperature probe connector optionally available is located on the front panel. The remainder of all connection points and status LEDs are located on the back panel.

### Operations Commands

#### Connecting to a serial device

The R480-0-x uses a variation of the Connect command to allow pass-through serial connection to devices attached to either the Serial1 or Serial2 ports..

#### To connect to a serial device attached to an R480-0-x:

At the Sentry: prompt, type **connect**, **serial1** or **serial2** and press **Enter**.

#### Examples

The following command connects to the serial device attached to Serial1:v

```
Sentry: connect serial1<Enter>
```

The following command connects to the serial device attached the port named ops\_2:

```
Sentry: connect ops_2<Enter>
```

The port name was previously defined at the Sentry RPM command line.

#### To disconnect from a serial device:

Type **!\*login** and press **Enter**.

---

**NOTE:** Disconnecting from a pass-through communication session returns the user to the login prompt.

---

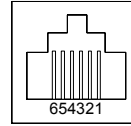
## Technical Specifications

### Data Connections

#### Console Port

The R480-0-x is equipped standard with an RJ12 RS-232 DTE Console serial port. This connector is typically used for direct local access, but may also be used for connection to other serial devices such as a terminal server. An RJ12 crossover cable and an adapter are provided for connection to a PC DB9-male DTE serial port.

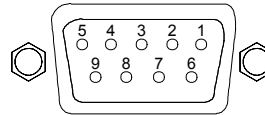
Pin	DTE Signal Name	Input/Output	
1	Signal Ground		
2	Data Set Ready	DSR	Input
3	Data Receive		Input
4	Data Transmit		Output
5	Data Terminal Ready	DTR	Output
6			



#### Serial1 and Serial2 Ports

The R480-0-x is equipped standard with two DB9-female DCE serial pass-through port for connection to serial devices. DB9-male to DB9-female straight-thru serial cables are provided for connection to standard RS-232C 9 pin DTE serial ports.

Pin	DCE Signal Name	Input/Output	
1	Data Carrier Detect	DCD	Output
2	Receive Data	RD	Output
3	Transmit Data	TD	Input
4	Data Terminal Ready	DTR	Input
5	Signal Ground		
6	Data Set Ready	DSR	Output
7	Request to Send	RTS	Input
8	Clear to Send	CTS	Output



## Sentry Any-to-Any Pass Through Switch

Server Technology offers a family of add-on equipment supporting asynchronous communication for console port access to attached serial devices, one device at a time. This family is referred to as the Sentry Any-to-Any Pass Through Switch (ATA Switch). The ATA Switch effectively expands the ability of a standard Sentry RPM to serially connect to a maximum of fifteen additional devices.

### Standard Models

Model	Voltage	Pass-through ports	Additional Features
R484-0-1	100-120V, 50/60 Hz	4	2 unswitched NEMA 5-15 receptacles
R488-0-1	100-120V, 50/60 Hz	8	2 unswitched NEMA 5-15 receptacles
R496-0-1	100-120V, 50/60 Hz	16	2 unswitched NEMA 5-15 receptacles
R484-0-2	208-240V, 50/60 Hz	4	
R488-0-2	208-240V, 50/60 Hz	8	
R496-0-2	208-240V, 50/60 Hz	16	

The ATA Switch is available in a 1U rack-mount enclosure for installation in standard 19" racks. Once installed and powered, serial communication through any of the ATA Switch's ports is enabled and access is granted through the Sentry RPM interface.

**For pricing and availability contact your Server Technology Sales Representative.**

### Commands

The following table lists and briefly describes each command used with the ATA Switch. The 'Type' letter (A) indicates an administration command and (O) indicates an operations command.

#### Any-to-Any Pass Through Switch Command Summary

Command	Type	Description
Add Sname	A	Adds a descriptive name to a port
Del Sname	A	Deletes a descriptive name from a port
Connect	O	Connects to a serial device
Set Connect Link	A	Enables or disables active signal checking for serial connections
Show Connect Link	O	Displays the on/off status of active signal checking for serial ports

### Adding or deleting a port name

ATA Switch ports may be assigned a descriptive name in addition to its absolute name. The Add Sname command is used to assign this descriptive name. See *Creating a serial pass-through port name* in Chapter 3: Operations for more information on the Add Sname command.

**NOTE:** Serial pass-through port names assigned with the Add Sname command are NOT bound by port privilege security unlike Port Names assigned from the Control Screen. See *Port Name field* on page 30 for additional information.

### Connecting to a serial device

The ATA Switch uses a variation of the Connect command to allow pass-through serial connection to device attached to the blue serial ports.

#### To connect to a serial device attached to an ATA Switch:

At the Sentry: prompt, type **connect**, followed by the port name and press **Enter**.

#### Examples

The following command connects to the serial device attached to port 4 on an R484-0-1:

```
Sentry: connect 4<Enter>
```

The following command connects to the serial device attached the port named ops\_2:

```
Sentry: connect ops_2<Enter>
```

The port name was previously defined at the Sentry RPM command line.

#### To disconnect from a serial device:

Type **!\*login** and press **Enter**.

**NOTE:** Disconnecting from a pass-through communication session returns the user to the login prompt.

## **Enabling and disabling active signal checking for ATA Switch connections**

By default the DSR signal checking is enabled for serial connections through the ATA switch. For attached devices that do not support DSR signal checking, the Set Connect Link command is used to enable and disable the Sentry RPMs signal checking settings. See *Enabling and disabling active signal checking for serial connections* in Chapter 3: Operations for more information on the Set Connect command.

---

**NOTE:** The Set Connect Link command applies the setting to ALL ATA Switch connections. It is not possible to set individual ports with different signal checking states.

---

## **Displaying ATA Switch serial port information**

The Show Connect Link command displays the active signal checking status for all ATA Switch ports. See *Displaying serial port information* in Chapter 3: Operations for more information on the Show Connect command.

## **Data Connections**

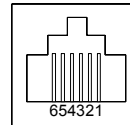
### **Link Port**

ATA Switches are equipped standard with a DB9-male RS 232C DCE Link serial port for connection ONLY to a Sentry RPM. A DB9-M to DB9-F straight-thru serial cable is provided for connection.

### **Pass-through Port**

ATA Switches are equipped with 4, 8 or 16 blue RJ12 Pass-through ports for connection to serial devices. RJ12 crossover cables are provided for connection along with adapters for connection to standard RS 232C 9 and 25 pin, DTE and DCE serial ports.

<b>Pin</b>	<b>DTE Signal Name</b>	<b>Input/Output</b>	
1	Signal Ground		
2	Data Set Ready	DSR	Input
3	Data Receive		Input
4	Data Transmit		Output
5	Data Terminal Ready	DTR	Output
6	Signal Ground		



## Warranty, Product Registration and Support

### Warranty and Limitation of Liability

Server Technology, Inc. agrees to repair or replace Products that fail due to a defect within twelve (12) months after the shipment date of each Product unit to Buyer ("Warranty Period"). For purposes of this Agreement the term "defect" shall mean the Product fails to operate or fails to conform to its applicable specifications. Any claim made pursuant to this Agreement shall be asserted or made in writing only by Buyer. Buyer shall comply with Server Technology's Standard Return Merchandise Authorization ("RMA") procedure for all warranty claims as set forth in Server Technology's operation manual.

**Buyer must return Products in original packaging and in good condition.** This limited warranty does not include labor, transportation, or other expenses to repair or reinstall warranted Products on site or at Buyer's premises.

Server Technology reserves the right to investigate any warranty claims to promptly resolve the problem or to determine whether such claims are proper. In the event that after repeated efforts Server Technology is unable to repair or replace a defective Product, then Buyer's exclusive remedy and Server Technology's entire liability in contract, tort, or otherwise shall be the payment by Server Technology of Buyer's actual damages after mitigation, but shall not exceed the purchase price actually paid by Buyer for the defective Product.

Server Technology shall have no responsibility or liability for any Product, or part thereof, that (a) has had the Serial Number, Model Number, or other identification markings altered, removed or rendered illegible; (b) has been damaged by or subject to improper installation or operation, misuse, accident, neglect and/or has been used in any way other than in strict compliance with Server Technology's operation and installation manual; (c) has become defective or inoperative due to its integration or assembly with any equipment or products not supplied by Server Technology; (d) has been repaired, modified or otherwise altered by anyone other than Server Technology and/or has been subject to the opening of any sealed cabinet boxes without Server Technology's prior written consent. If any warranty claim by Buyer falls within any of the foregoing exceptions, Buyer shall pay Server Technology its then current rates and charges for such services.

THE ABOVE WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. SERVER SHALL NOT BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR EXEMPLARY DAMAGES; EVEN OF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

### Product Registration

Registration is your key to special offers and services reserved for Registered Users.

- Excellent Technical Support Services
- Special Update and Upgrade Programs
- Warranty Protection
- Extended Warranty Service
- New Product Information

Register your products online today!

[www.servertech.com](http://www.servertech.com)

### Technical Support

Server Technology understands that there are often questions when installing and/or using a new product. Free Technical Support is provided from 8:30 AM to 5:00 PM, Monday-Friday, Pacific Time.

For Technical Support:

Server Technology, Inc.

1040 Sandhill Drive

Reno, Nevada 89521 USA

Tel: 775.284.2000

Fax: 775.284.2065

Web: [www.servertech.com](http://www.servertech.com)

Email: [support@servertech.com](mailto:support@servertech.com)

## **Return Merchandise Authorization**

If you have a unit that is not functioning properly and is in need of technical assistance or repair:

Submit a request for support by phone at the above number, or via the web at [www.servertech.com/forms/techrequest.htm](http://www.servertech.com/forms/techrequest.htm).

Be ready to provide:

- Company Name
- Contact Name, Phone Number, and Email address
- Model or Part Number (from the label on the equipment)
- Server Technology Serial Number
- Version of code (type 'vers' at the Sentry: prompt)
- Description of problem

1. Technical Support will work to diagnose/resolve the problem remotely, if possible. If the problem cannot be resolved, Technical Support will then issue an RMA# for the return/repair of the equipment in question. RMA#'s are valid for 30 days only from the issue date.
2. Shipping charges for the return of the equipment to Server Technology shall be the responsibility of the customer. For warranty repairs, Server Technology shall assume return shipping charges but for non-warranty repairs, the shipping charges shall be billed.
3. The RMA# shall be placed conspicuously on all shipping documentation, associated correspondence, and the shipping container.
4. Equipment must be returned in proper/original packaging to protect the equipment in transit. The customer shall be financially responsible for any damage/destruction of the equipment due to improper packaging.
5. Equipment shall typically be turned around within 48-72 hours of receipt at Server Technology. Equipment under warranty shall be repaired at no cost. Equipment NOT under warranty shall be repaired at the standard labor rate plus parts. Upon diagnosis of the equipment, the customer shall be notified of estimated charges prior to repair.
6. For non-warranty repairs, return of the equipment will be expedited with the inclusion of a Purchase Order or credit card number for incurred charges.





# Server Technology, Inc.

1040 Sandhill Drive, Reno, Nevada 89521 • (775) 284-2000 • Fax: (775) 284-2065  
E-mail: [sales@servertech.com](mailto:sales@servertech.com) • World Wide Web: [www.servertech.com](http://www.servertech.com)

Sentry and Intelligent Power Modules are trademarks of Server Technology, Inc.

301-0150-1 Rev. B (060303)

© 2003 Server Technology, Inc. All rights reserved.