



**Server Technology**

Solutions for the Data Center Equipment Cabinet

# Sentry

## Commander

- PT40

### 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.

**Please Recycle**

Shipping materials are recyclable. Please save them for later use, or dispose of them appropriately.

**Notices**

Copyright © 2004-2005 Server Technology, Inc. All rights reserved  
1040 Sandhill Drive  
Reno, Nevada 89521 USA

**All Rights Reserved**

This publication is protected by copyright and all rights are reserved. No part of it may be reproduced or transmitted by any means or in any form, without prior consent in writing from Server Technology.

The information in this document has been carefully checked and is believed to be accurate. However, changes are made periodically. These changes are incorporated in newer publication editions. Server Technology may improve and/or change products described in this publication at any time. Due to continuing system improvements, Server Technology is not responsible for inaccurate information which may appear in this manual. For the latest product updates, consult the Server Technology web site at [www.servertech.com](http://www.servertech.com). In no event will Server Technology be liable for direct, indirect, special, exemplary, incidental or consequential damages resulting from any defect or omission in this document, even if advised of the possibility of such damages.

In the interest of continued product development, Server Technology reserves the right to make improvements in this document and the products it describes at any time, without notices or obligation.

# Table of Contents

<b>CHAPTER 1: INTRODUCTION</b>	<b>4</b>
Quick Start Guide.....	4
Technical Support .....	4
Equipment Overview.....	5
<b>CHAPTER 2: INSTALLATION</b>	<b>6</b>
Standard Accessories.....	6
Additional Required Items .....	6
Safety Precautions .....	6
Installing the Power Input Retention Bracket.....	7
Mounting .....	7
Connecting to the Power Source .....	7
Connecting Devices.....	7
Connecting to the Unit .....	8
<b>CHAPTER 3: OPERATIONS</b>	<b>9</b>
Interfaces .....	10
HTML Interface .....	11
Command Line Interface.....	22
<b>CHAPTER 4: ADVANCED OPERATIONS</b>	<b>43</b>
SSL .....	44
SSH .....	45
SNMP.....	46
LDAP .....	52
TACACS+.....	61
<b>CHAPTER 5: APPENDICES</b>	<b>66</b>
Appendix A: Resetting to Factory Defaults .....	66
Appendix B: Uploading Firmware .....	66
Appendix C: Technical Specifications .....	67
Appendix D: Warranty, Product Registration and Support.....	71

# Chapter 1: Introduction

## Quick Start Guide

The following instructions will help you quickly install and configure your Commander for use in your data center equipment cabinet. For detailed information on each step, go to the page number listed to the right.

1. Mount the Commander.....6
2. Connect to the power source .....7
3. Connect the devices.....7
4. Connect to the Commander .....8
5. Configure the Commander .....9
  - Login as the predefined Administrator (adm/admn) .....10
  - Configure the network settings .....13
  - Create new administrative user account.....15
  - Configure location and Commander names .....13
  - Configure new user account(s) .....15
  - Remove the predefined Administrator .....16
6. Connect the Commander to the network.

## 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.

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)

## Equipment Overview

1. The power inlet/cord(s) connects the Commander to the electrical power source.
2. One RJ12 Aux connector for connection to an optional Environmental Monitor.
3. RJ12 Pass-Thru console communication ports.
4. One DB9 Modem connector for connection to an external modem.
5. Two RJ45 connectors for Serial (RS-232) and Ethernet connection.

A number is printed above each Commander outlet. These numbers may be used in commands that require an outlet name.

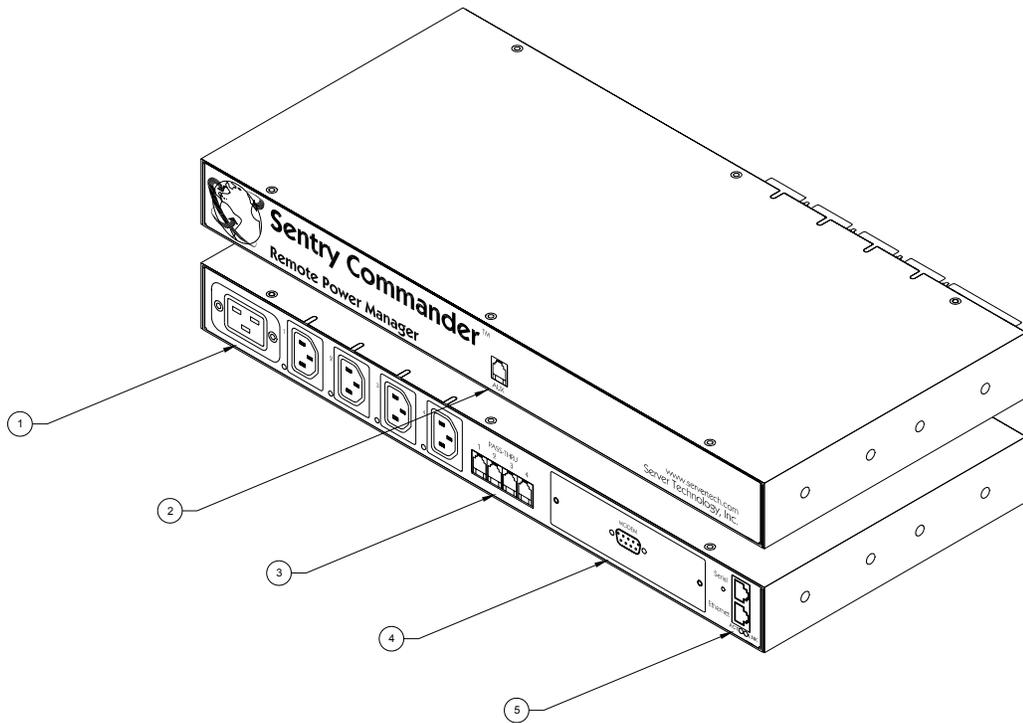


Figure 1.1 PT40 Commander Views

## Chapter 2: Installation

Before installing your Sentry Commander, refer to the following lists to ensure that you have all the items shipped with the unit as well as all other items required for proper installation.

### Standard Accessories

- Mounting bracket hardware: two mounting brackets and four screws
- RJ45 to RJ45 crossover cable
- RJ45 to DB9F serial port adapter (for connection to standard DB9M DTE serial port)
- DB9F to DB25M modem cable
- Pass-Thru cable/adapter kit
  - Four RJ12 to RJ12 crossover cables
  - RJ12 to DB25F adapter
  - RJ12 to DB25M adapter
  - RJ12 to DB9F adapter
  - RJ12 to DB9M adapter
- Separate power input cord
- Power input retention bracket hardware: Two removable T-brackets with two 40mm screws.
- Outlet retention clips (208-240V models)

### Additional Required Items

- Flathead and Phillip screwdrivers
- Screws, washers and nuts to attach the Commander to your rack

### Safety Precautions

This section contains important safety and regulatory information that should be reviewed before installing and using the Sentry Commander. For input and output current ratings, see *Power Ratings* in Appendix C: Technical Specifications.

	Only for installation and use in a Service Access Location in accordance with the following installation and use instructions.	<i>Destiné à l'installation et l'utilisation dans le cadre de Service Access Location selon les instructions d'installation et d'utilisation.</i>	Nur für Installation und Gebrauch an Anschlusszugriffspunkten gemäß der folgenden Installations- und Gebrauchsanweisungen.
	This equipment is designed to be installed on a dedicated circuit.	<i>Cet équipement est conçu à être installé sur un circuit spécialisé.</i>	Diese Ausrüstung ist zur Installation in einem festen Stromkreis vorgesehen.
	Dedicated circuit must have circuit breaker or fuse protection. Commanders have been designed without a master circuit breaker or fuse to avoid becoming a single point of failure. It is the customer's responsibility to provide adequate protection for the dedicated power circuit. Protection of capacity equal to the current rating of the Commander must be provided and must meet all applicable codes and regulations. In North American, protection must have a 10,000A interrupt capacity.	<i>Le circuit spécialisé doit avoir un disjoncteur ou une protection de fusible. Commanders ont été conçus sans disjoncteur général ni fusible pour éviter que cela devient un seul endroit de panne. C'est la responsabilité du client de fournir une protection adéquate pour le circuit-alimentation spécialisé. Protection de capacité équivalent à la puissance de l'équipement, et respectant tous les codes et normes applicables. Les disjoncteurs ou fusibles destinés à l'installation en Amérique du Nord doivent avoir une capacité d'interruption de 10.000 A.</i>	Der feste Stromkreis muss mit einem Schutzschalter oder einem Sicherungsschutz versehen sein. Commanders verfügt über keinen Hauptschutzschalter bzw. über keine Sicherung, damit kein einzelner Fehlerpunkt entstehen kann. Der Kunde ist dafür verantwortlich, den Stromkreis sachgemäß zu schützen. Der Kapazitätsschutz entspricht der aktuellen Stromstärke der Geräte und muss alle relevanten Codes und Bestimmungen erfüllen. Für Installation in Nordamerika müssen Ausschalter bzw. Sicherung über 10.000 A Unterbrechungskapazität verfügen.
	The plug on the power supply cord shall be installed near the equipment and shall be easily accessible.	<i>La prise sur le cordon d'alimentation sera installée près de l'équipement et sera facilement disponible.</i>	Der Stecker des Netzkabels muss in der Nähe der Ausrüstung installiert werden und leicht zugänglich sein.
	Always disconnect the power supply cord before opening to avoid electrical shock.	<i>Toujours déconnecter le cordon d'alimentation avant d'ouvrir pour éviter un choque électrique.</i>	Ziehen Sie vor dem Öffnen immer das Netzkabel heraus, um die Gefahr eines elektrischen Schlags zu vermeiden.
	<b>WARNING!</b> High leakage current! Earth connection is essential before connecting supply!	<b>ATTENTION !</b> <i>Haut fuite très possible ! Une connection de masse est essentielle avant de connecter l'alimentation !</i>	<b>ACHTUNG!</b> Hoher Ableitstrom! Ein Erdungsanschluss ist vor dem Einschalten der Stromzufuhr erforderlich!

## Installing the Power Input Retention Bracket

### To install the power input retention bracket:

1. Remove the two screws attaching the IEC 60320 C19 inlet to the enclosure.
2. Assemble and attach the retention bracket to the enclosure as shown.

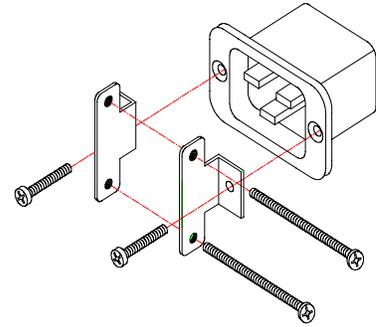


Figure 2.1 Retention Bracket assembly

## Mounting

1. Select the appropriate bracket mounting points for proper mounting depth within the rack.
2. Attach the brackets to these mounting points with two screws for each bracket.
3. 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:** A mounting bracket kit for 23" wide racks or cabinets is available. Contact your Server Technology Sales Representative for more information.

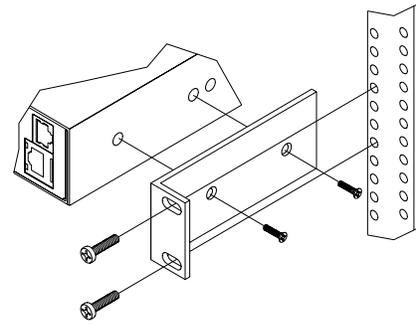


Figure 2.2 Mounting

## Connecting to the Power Source

The input power cord must first be attached to the unit before connecting the unit to the power source. Each outlet powers up sequentially, eliminating a potential blown primary fuse or circuit breaker from excessive in-rush current.

### To attach the power cord to the unit:

1. Plug the female end of the power cord firmly into its connector at the base.
2. Use a screwdriver to tighten the two screws on the retention bracket.

### To connect to the power source:

Plug the male end of the power cord into the AC power source.

## Connecting Devices

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

1. Keep the device's on/off switch in the off position until after it is plugged into the outlet.
2. Connect devices to the Commander outlets.

**NOTE:** Server Technology recommends even distribution of attached devices across all available outlets to avoid exceeding the outlet, branch or phase limitations. See *Power Ratings* on page 67 for more information.



Always disconnect both power supply cords before opening to avoid electrical shock.

Afin d'éviter les chocs électriques, débranchez les câbles électrique avant d'ouvrir.

Immer beiden Netzleitungen auskuppeln vor den Aufmachen um elektrischen Schlag zu vermeiden.

3. Connect devices to the Pass-Thru ports. See *Power Ratings* on page 67 for more information on the Pass-Thru port.

## Connecting to the Unit

### **Serial (RS232) port**

The Commander is equipped with an RJ45 Serial RS-232 port for attachment to a PC or networked terminal server using the supplied RJ45 to RJ45 crossover cable and RJ45 to DB9F serial port adapter as required. See *Power Ratings* in Appendix C: Technical Specifications for more information on the Serial RS-232 port.

### **Ethernet port**

The Commander is equipped with an RJ45 10/100Base-T Ethernet port for attachment to an existing network. This connection allows access to the Switched Commander via Telnet or HTML.

The Commander is configured with the following network defaults to allow unit configuration out-of-the-box through either Telnet or HTML:

- IP address: 192.168.1.254
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.1.1

The local PC network connection must be configured as noted below:

---

**NOTE:** Contact your system administrator for instructions in reconfiguring the network connection. Reconfiguration of your network connection may require a restart to take effect.

---

- IP address: 192.168.1.x (where x is 2-253)
- Subnet Mask: 255.255.255.0

### **Modem port**

The Commander is equipped with a DB9 male Modem serial port for connection to an external modem using the supplied DB9 female to DB25 male serial cable. See *Power Ratings* in Appendix C: Technical Specifications more information on the Modem port.

# Chapter 3: Operations

<b>INTERFACES</b>	<b>10</b>
Outlet Naming and Grouping	10
Usernames and Passwords	10
<b>HTML INTERFACE</b>	<b>11</b>
Logging In	11
Outlet Control	12
<i>Individual</i> .....	12
<i>Group</i> .....	12
Environmental Monitoring	12
<i>Input Load</i> .....	12
Configuration	13
<i>System</i> .....	13
<i>Network</i> .....	13
<i>Telnet/SSH</i> .....	14
<i>HTTP/SSL</i> .....	14
<i>Serial Ports</i> .....	15
<i>Outlets</i> .....	16
<i>Groups</i> .....	16
<i>Users</i> .....	16
<i>FTP</i> .....	17
<i>SNTP</i> .....	18
<i>SNMP</i> .....	18
<i>LDAP</i> .....	18
<i>TACACS+</i> .....	20
Tools	21
<i>Restart</i> .....	21
<i>Ping</i> .....	21
<b>COMMAND LINE INTERFACE</b>	<b>22</b>
Logging In	22
Operations Commands	24
Administration Commands	28
<i>User Administration</i> .....	28
<i>Outlet Administration</i> .....	31
<i>Group Administration</i> .....	33
<i>Serial Port Administration</i> .....	34
<i>System Administration</i> .....	36
<i>TCP/IP Administration</i> .....	38
<i>HTTP Administration</i> .....	40
<i>Telnet Administration</i> .....	40
<i>FTP Administration</i> .....	41
<i>SNTP Administration</i> .....	42

## Interfaces

The Commander has two interfaces: the HTML interface accessed via the HTTP enabled Ethernet connections and the command line for serial and Telnet connections.

### **Outlet Naming and Grouping**

For commands requiring an outlet name, you may specify it in one of two ways: a predefined absolute name or a descriptive name assigned by an administrator.

Absolute names are specified by a period (.) followed by a tower letter and outlet number.

Outlets may also be included in one or more named groups of outlets, enabling you to issue a command that affects all outlets in a named group.

### **Usernames and Passwords**

The Commander has one predefined administrative user account (username/password: admn/admn) and supports a maximum of 128 defined user accounts

---

**NOTE:** For security, Server Technology recommends removal of the predefined administrative user account after a new account with administrative rights has been created.

---

Only an administrative-level user may perform operations such as creating/removing user accounts and command privileges, changing passwords and displaying user information. An administrator may also view the status of all sensors and power inputs.

Usernames may contain from 1-16 characters and are not case sensitive; spaces are not allowed. Passwords may contain up to 16 characters, and are case sensitive.

## HTML Interface

The HTML interface is constructed of three major components: the System Location bar, the User/Navigation bar and the Control Screen. The System Location bar displays the Sentry's location and IP address as well as the current Control Screen title. The User/Navigation bar displays the current user and privilege level and provides access to all HTML pages. And the Control Screen is used to display current data and allow changes to outlet states or system configuration.

The following sections describe each interface section/page and their use.

The screenshot shows the Sentry Power Distribution Unit interface in a Microsoft Internet Explorer browser window. The browser title is "Sentry Power Distribution Unit - Microsoft Internet Explorer" and the address bar shows "http://64.42.31.200/". The interface features a blue header with the Sentry logo and "Power Distribution Unit" text. A navigation bar on the left shows the user "ADMN" with "Admin" access and a menu with "Environmental Monitoring", "Configuration", and "Tools". The main content area displays "Environmental Monitoring - Input Feeds" and a table of input feeds.

Input Feed ID	Input Feed Name	Input Status	Input Load
AA	TowerA_InfeedA	On	0.00 Amps
AB	TowerA_InfeedB	On	0.00 Amps
AC	TowerA_InfeedC	On	0.00 Amps
BA	TowerB_InfeedA	On	0.00 Amps
BB	TowerB_InfeedB	On	0.00 Amps
BC	TowerB_InfeedC	On	0.25 Amps

Figure 3.1 Example HTML page

### Logging In

Logging in through HTML requires directing the HTML client to the configured IP address of the unit.

#### To log in by HTML:

In the login window, enter a valid username and password and press **OK**.

If you enter an invalid username or password, you will be prompted again.

You are given three attempts to enter a valid username and password combination. If all three fail, the session ends and a protected page will be displayed.

**NOTE:** The default Sentry username/password is `adm/admn`.

## **Outlet Control**

The Outlet Control section offers access to the Individual and Group outlet control pages. From the Individual and Group pages, the user can review and manipulate power control functions for all outlets and groups assigned to the current user. Both pages include the outlets absolute and descriptive names, the Outlet Status reported to the Sentry by the outlet, the current Control State being applied by the Sentry and the outlet load in amperes.

Available outlet and group power states may be set to on, off or reboot.

### **Individual**

The Individual outlet control page displays all outlets assigned to the current user. The user may apply on, off or reboot actions to individual, multiple or all accessible outlets.

#### **To apply actions to individual or multiple outlets:**

In the Individual Outlet Control section, select the desired action from the Control Action drop-down menu for each individual outlet to be changed and press **Apply**.

#### **To apply an action to all outlets:**

In the Global Control section, select the desired action from the Control Action drop-down menu and press **Apply**.

### **Group**

The Group outlet control page displays all groups assigned to the current user as well as the outlets for each group.

#### **To select a group:**

Select the group name from the drop-down menu and press **Select**. The page will refresh to display all outlets associated to the selected group name.

#### **To apply an action to a group:**

Select the desired action from the drop-down menu and press **Apply**.

#### **Outlet State/Control State Field Values**

<b>Outlet State</b>	<b>Control State</b>	<b>Description</b>
On	On	Outlet is on
Off	Off	Outlet is off
Off	Pend On	Outlet is off and about to turn on in response to a sequence timer
Off	Reboot	Outlet is off and a Reboot action has been initiated
On	Idle On	A restart has occurred – Last Control State has been maintained
Off	Idle Off	A restart has occurred – Last Control State has been maintained
On	Wake On	A power-loss has occurred – Wakeup State has been applied
Off	Wake Off	A power-loss has occurred – Wakeup State has been applied
On/Wait	Off	Outlet state in transition – Requery of outlet status required
Off/Wait	On	Outlet state in transition – Requery of outlet status required
On/Error	varies	Error State – Outlet should be off but current is sensed at the outlet
Off/Error	varies	Error State – Outlet should be on but no current is sensed at the outlet
No Comm	varies	Communication to the outlet has been lost*

\* Control State will be applied when communication is re-established

## **Environmental Monitoring**

### **Input Load**

The Input Load page displays the tower(s) absolute and descriptive name and the cumulative input load in amperes of all devices attached to the Sentry at the time the page was loaded. This page will refresh automatically every 10 seconds

## **Configuration**

The Configuration section offers access to all unit configuration options including Network, Telnet/SSH, HTTP/SSL, Serial Ports, Users, FTP, Proxy/SNTP and SNMP. This section is available to administrative level users only.

## **System**

The System configuration page is used for reference of system information such as Ethernet NIC Serial Number, Ethernet MAC address and system firmware and hardware revisions as well as assignment and maintenance of the system location and tower descriptive names.

For description names, up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal – spaces are not allowed) are allowed.

---

**NOTE:** Spaces may be used for the location description only.

---

### **Creating a descriptive system location name:**

Enter a descriptive name and press **Apply**.

### **Configuring the Input Current LED display orientation:**

Select **Normal** or **Inverted** from the drop-down menu and press **Apply**.

### **Creating a descriptive unit name:**

Click on the **Tower Names** link.

On the subsequent Tower Names page, enter a descriptive name and press **Apply**.

### **Creating a descriptive input feed name:**

Click on the **Input Feed Names** link.

On the subsequent Input Feed Names page, enter a descriptive name and press **Apply**.

### **Creating a descriptive outlet name:**

Click on the **Outlet Names** link which will open the Outlets configuration page. See *Outlets* on page 16 for additional information on creating descriptive outlet names.

### **Creating a descriptive serial port/Pass-Thru name:**

Click on the **Serial Port Names** link which will open the Serial Ports configuration page. See *Serial Ports* on page 15 for additional information on creating descriptive serial port names.

## **Network**

The Network configuration page is used for maintenance of the network interface. From this page an administrator may configure the IP address, subnet mask, gateway address, DNS addresses as well as view the link status, speed and duplex value.

The Sentry is configured with the following network defaults to allow unit configuration out-of-the-box through either Telnet or HTML:

- IP address: 192.168.1.254
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.1.1

The initial local PC network connection must be configured as noted below:

---

**NOTE:** Contact your system administrator for instructions in reconfiguring the network connection. Reconfiguration of your network connection may require a restart to take effect.

---

- IP address: 192.168.1.x (where x is 2-253)
- Subnet Mask: 255.255.255.0

---

**NOTE:** The unit must be restarted after network configuration changes. See *Performing a warm boot:* on page 21.

---

### **Setting the IP address, subnet mask, gateway or DNS address:**

In the appropriate field, enter the IP address, subnet mask, gateway address or DNS address and press **Apply**.

## **Telnet/SSH**

The Telnet/SSH configuration page used to enable or disable Telnet and SSH support and configure the port number that the Telnet or SSH server watches. For more information on SSH see page 45 in Chapter 4: Advanced Operations.

### **Enabling or disabling Telnet or SSH support:**

Select **Enabled** or **Disabled** from the appropriate Server drop-down menu and press **Apply**.

### **Changing the Telnet or SSH server port number:**

In the appropriate Port field, enter the port number and press **Apply**.

## **HTTP/SSL**

The HTTP/SSL configuration page used to enable or disable HTTP and SSL support, configure the port number that the HTTP server watches and responds to, selection of the method of authentication used and SSL access level. For more information on SSL see page 43 in Chapter 4: Advanced Operations.

### **Enabling or disabling HTTP or SSL support:**

Select **Enabled** or **Disabled** from the appropriate Server drop-down menu and press **Apply**.

### **Changing the HTTP server port number:**

In the HTTP Port field, enter the port number and press **Apply**.

### **Setting the HTTP authentication method:**

The Sentry HTTP server supports two authentication methods for security and validation of the username-password – Basic and MD5 digest.

The Basic method utilizes Base64 encoding to encode and deliver the username-password over the network to the HTTP server for decoding and authentication. This basic method is supported by all web browsers and offers a minimum level of security.

---

**NOTE:** The Base64 algorithm is widely-known and susceptible to packet-sniffer attack for acquisition of the encoded username-password string.

---

The MD5 digest method provides stronger protection utilizing one-way encoded hash numbers, never placing the username-password on the network. Instead, the sending browser creates a challenge code based on the hash algorithm, provided username-password and unique items such as the device IP address and timestamp, which is compared against the HTTP server internal user database of valid challenge codes. The MD5 digest method offers a higher level of security than the Basic method but at present is not supported by all browsers.

---

**NOTE:** MD5 is known to be fully supported by Internet Explorer 5.0+

---

Select **Basic** or **MD5** from the Authentication drop-down menu and press **Apply**.

### **Setting SSL access level**

Sentry SSL supports configuration of SSL connections as being either optional or required. The default access level is set to optional.

- Optional –Both non-secure (HTTP) and SSL encrypted connections (HTTPS) are allowed access.
- Required – ONLY SSL encrypted connections (HTTPS) are allowed access.

Select **Optional** or **Required** from the Secure Access drop-down menu and press **Apply**.

## Serial Ports

The Serial Ports configuration page is used for maintenance of all serial/Pass-Thru ports.

---

**NOTE:** Pass-Thru connections may only be initiated from the command line interface via a direct serial or Telnet session.

---

### Setting the data-rate for all serial/Pass-Thru ports:

Select the serial/Pass-Thru port data-rate from the drop-down menu and press **Apply**.

### Setting the serial/Pass-Thru port timeout value:

Enter the timeout value (in minutes) in the Connection Timeout field and press **Apply**.

### Creating a descriptive serial/Pass-Thru port name:

Click on the **Edit** link in the Action column next to the port to be configured.

On the subsequent Serial Port Edit page, enter the descriptive name. Up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal, spaces and colon characters are not allowed) are allowed. Press **Apply**.

---

**NOTE:** Port names '1' thru '64', 'CONSOLE' and 'MODEM' are reserved system names and may not be used.

---

### Enabling or disabling serial/Pass-Thru port active signal checking:

Click on the **Edit** link in the Action column next to the port to be configured.

On the subsequent Serial Port Edit page, select **On** or **Off** from the DSR Check drop-down menu and press **Apply**.

### Enabling or disabling modem initialization strings:

By default, the Sentry assumes an external modem is attached to the Modem port and sends initialization strings to that modem as necessary. The Sentry sends the initialization strings under the following conditions:

- System start – DSR is high and DCD is low
- Normal operations – If DSR transitions from low to high and DCD is low
- Normal operations – After a session initiated from the Modem port ends
- Normal operations – After a Pass-Thru connection to the Modem port is disconnected

Click on the **Edit** link in the Modem port Action column.

On the subsequent Serial Port Edit page, select **On** or **Off** from the Modem Initializations drop-down menu and press **Apply**.

### Editing modem initialization strings:

Click on the **Edit** link in the Modem port Action column.

On the subsequent Serial Port Edit page, enter the initialization string in the appropriate field and press **Apply**.

The Init1 and Init2 strings may be up to 48 characters. The Attention and Hang-up strings may be up to 16 characters.

### Predefined Modem Initialization Strings

String Type	String	Description
Init 1	AT	Gets modem attention
Init 2	AT E0 Q1 S0=1 S2=64 S12=50 &C1 &D2	Initializes default settings required
Attention	@@@	Switches the modem to command mode
Hang-up	ATH	Forces a hang-up of an active connection

---

**NOTE:** Sentry Remote Power Managers do NOT support *variable data-rate mode* modems. The modem operating mode must be set to *fixed data-rate mode* to avoid the data-rate being changed after initialization.

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.

---

## Outlets

The Outlets configuration page is used for assignment and/or editing of outlet sequence and reboot timers, descriptive names and wakeup states.

### **Setting the outlet sequencing interval:**

Enter the sequencing interval (in seconds) in the Sequence Interval field and press **Apply**.

### **Setting the outlet reboot delay:**

Enter the reboot interval (in seconds) in the Reboot Delay field and press **Apply**.

### **Editing the outlet descriptive name:**

Click on the **Edit** link in the Action column next to the outlet to be configured.

On the subsequent Outlet Edit page, enter the descriptive name. Up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal, spaces are not allowed) are allowed. Press **Apply**.

### **Changing the outlet wakeup state:**

Click on the **Edit** link in the Action column next to the outlet to be configured.

On the subsequent Outlet Edit page, select **On**, **Off** or **Last** from the Wakeup State drop-down menu and press **Apply**.

### **Setting the outlet Post-On delay:**

Click on the **Edit** link in the Action column next to the outlet to be configured.

On the subsequent Outlet Edit page, enter the outlet Post-On delay (in seconds) in the Post-On Delay field and press **Apply**.

## Groups

The Groups configuration page is used for creation and deletion of group and assignment of outlets to groups.

### **Creating a group:**

Enter a descriptive group name in the Group Name field. Up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal, spaces are not allowed) are allowed. Press **Apply**.

### **Removing a group:**

Click on the **Remove** link in the Action column for the group to be removed and press **Yes** on the subsequent confirmation window.

### **Adding and Deleting outlets from a group:**

Press the **Edit** link in the Action column for the associated group.

On the subsequent Group Edit page, select or deselect outlets to be included in that group. Press **Apply**.

## Users

The Users configuration page is used for creation and removal of usernames, assignment of accessible outlets and group, assignment of privilege levels and the changing of user passwords.

### **Creating a new user:**

Enter a user name in the Username field. Up to 16 alphanumeric and other typeable characters (ASCII 33 to 126 decimal, spaces are not allowed) are allowed.

Enter a password for the new user and verify in the Password and Verify Password fields. For security, password characters are not displayed. Press **Apply**.

### **Removing a user:**

Click on the **Remove** link in the Action column for the user to be removed and press **Yes** on the subsequent confirmation window.

### Changing a user password:

Click on the **Edit** link in the Action column for the associated user.

On the subsequent User Edit page, enter a password and verify the new password for the new user in the Password and Verify Password fields. For security, password characters are not displayed. Press **Apply**.

### Changing a user's access privilege level:

The Sentry has four defined access privilege levels; Admin, User, On-Only and View-Only:

- Admin: Full-access for all configuration, control (On, Off, Reboot), status and Pass-Thru.
- User: Partial-access for control (On, Off, Reboot), status and Pass-Thru of assigned outlets, groups and serial/Pass-Thru ports.
- On-Only: Partial-access for control (On), status and Pass-Thru of assigned outlets, groups and serial/Pass-Thru ports.
- View-Only: Partial-access for status and Pass-Thru of assigned outlets, groups and serial/Pass-Thru ports.

The administrator may also grant administrative privileges to other user accounts allowing the Sentry to have more than one administrative-level user.

---

**NOTE:** You cannot remove administrative privileges from the Admn user unless another user has already been given administrative access level privileges created.

---

Click on the **Edit** link in the Action column for the associated user.

On the subsequent User Edit page, select **Admin**, **User**, **On-only** or **View-only** from the Access Level drop-down menu and press **Apply**.

### Granting or removing Environmental Monitoring viewing privileges:

Click on the **Edit** link in the Action column for the associated user.

On the subsequent User Edit page, select **Yes** or **No** from the Environmental Monitoring drop-down menu and press **Apply**.

---

**NOTE:** This also grants or removes viewing privileges for the optional Equipment Cabinet Environmental Manager. See the Equipment Cabinet Environmental Manager Installation and Operations manual for more information.

---

### Adding and Deleting outlet access:

Click on the **Outlets** link in the Access column for the associated user.

On the subsequent User Outlets page, select or deselect outlets to be accessed by the user and press **Apply**.

### Adding and Deleting group access:

Click on the **Groups** link in the Access column for the associated user.

On the subsequent User Groups page, select or deselect group to be accessed by the user and press **Apply**.

### Adding and Deleting serial/Pass-Thru port access:

Click on the **Ports** link in the Access column for the associated user.

On the subsequent User Ports page, select or deselect ports to be accessed by the user and press **Apply**.

## FTP

The FTP configuration page is used for setup and maintenance of all settings required to perform an FTP firmware upload. See Appendix B: Uploading Firmware for more information on uploading firmware.

### Setting the FTP Host IP Address:

Enter the IP address in the Host IP Address field and press **Apply**.

### Setting the FTP username:

Enter the FTP server username in the Username field, and press **Apply**.

### Setting the FTP password:

Enter the FTP server password in the Password field, and press **Apply**.

### Setting the filepath:

Enter the path of the file to be uploaded in the Directory field, and press **Apply**.

### Setting the filename for upload:

Enter the filename of the file to be uploaded in the Filename field, and press **Apply**.

### Testing the FTP upload configuration:

This test validates that the unit is able to contact and log onto the specified FTP server, download the firmware file and verify that the firmware file is valid for this unit.

Press **Test**.

## SNTP

The SNTP configuration page is used for setup and maintenance of SNTP support.

### Setting the SNTP Server Address:

Enter the IP address in the primary and/or secondary address field and press **Apply**.

## SNMP

The SNMP configuration page is used for setup and maintenance of all settings required to enable SNMP support as well as access to the trap configuration pages. For additional information on SNMP support and detailed descriptions of available traps, see *SNMP* on page 46.

---

**NOTE:** Traps are generated according to a hierarchical architecture; i.e. if a Tower Status enters a trap condition, only the Tower Status trap is generated. Infeed and Outlet Status traps are suppressed until the Tower Status returns to Normal.

---

### Enabling or disabling SNMP support:

Select **Enabled** or **Disabled** from the drop-down menu and press **Apply**.

### Setting the community strings:

Enter the community string in the appropriate field and press **Apply**.

Community strings may be 1 to 24 characters

### Setting the trap timer:

Enter a trap timer value in the Error Trap Repeat Time field and press **Apply**.

The Error Trap Repeat Time value may be 1 to 65535 (in seconds).

### Setting trap destinations:

Enter an IP address in the appropriate Trap Destination field and press **Apply**.

### Enabling or disabling tower traps:

Click on the **Tower Traps** link.

On the subsequent Tower Traps page, select or deselect the desired traps and press **Apply**.

### Configuring input feed traps:

Click on the **Input Feed Traps** link.

On the subsequent Input Feed Traps page, select or deselect the desired traps and press **Apply**.

For Load traps, enter a maximum load value for the infeed in the High Load Threshold field and press **Apply**.

The High Load Threshold value may be 0 to 255 (in amperes).

### Configuring outlet traps:

Click on the **Outlet Traps** link.

On the subsequent Outlet Traps page, select or deselect the desired traps and press **Apply**.

## LDAP

The LDAP configuration page is used for setup and maintenance of all settings required to enable LDAP support. For additional information and configuration requirements, see *LDAP* on page 52.

### Enabling or disabling LDAP support:

Select **Enabled** or **Disabled** from the LDAP drop-down menu and press **Apply**.

**Setting the LDAP server IP address:**

Enter the IP address in the Host IP1 and/or Host IP2 address field and press **Apply**.

**Changing the LDAP server port:**

Enter the port number in the LDAP Port field and press **Apply**.

**Setting the LDAP bind password type:**

Select **Simple** or **MD5** from the drop-down menu and press **Apply**.

For more information on LDAP bind password types, see *Setting the LDAP bind password type* on page 53.

**Setting the search bind Distinguished Name (DN):**

Enter the fully-qualified distinguished name (FQDN) in the Search Bind field and press **Apply**.

**Setting the search bind password for Distinguished Name (DN):**

Enter the Search Bind Password in the Search Bind Password field and press **Apply**.

**Setting the group membership attribute:**

Enter the group membership attribute in the Group Membership Attribute Field and press **Apply**.

**Setting the group membership value type:**

Select the appropriate value from the drop-down menu and press **Apply**.

**Setting the user search base Distinguished Name (DN):**

Enter the User Search Base DN in the User Search Base DN field and press **Apply**.

**Setting the user search filter:**

Enter the User Search Filter in the User Search Filter field and press **Apply**.

**Setting the DNS IP address:**

See *Network* on page 13 for information on how to set the DNS IP address.

**Configuring the authentication order:**

Select **Remote -> Local** or **Remote Only** from the drop-down menu and press **Apply**.

For more information on remote authentication order, see *Setting the authentication order* on page 55.

---

**NOTE:** Server Technology recommends NOT setting the authentication order to Remote Only until the LDAP has been fully configured and tested.

---

**Configuring LDAP groups:**

Click on the **LDAP Groups** link at the bottom of the page.

***Creating an LDAP group:***

Enter a descriptive group name in the LDAP Group Name field. Up to 24 alphanumeric and other typeable character (ASCII 33 to 126 decimal, spaces are not allowed) are allowed. Press **Apply**.

***Removing an LDAP group:***

Click on the **Remove** link in the Action column for the group to be removed and press **OK** on the subsequent confirmation window.

***Changing an LDAP group's access privilege level:***

Click on the **Edit** link in the Action column for the associated LDAP Group.

On the subsequent LDAP Group - Edit page, select **Admin**, **User**, **On-only** or **View-only** from the Access Level drop-down menu and press **Apply**.

For more information on access privilege levels, see *Changing a user's access privilege level:* on page 17.

### ***Granting or removing Environmental Monitoring viewing privileges:***

Click on the **Edit** link in the Action column for the associated LDAP Group.

On the subsequent LDAP Group - Edit page, select **Yes** or **No** from the Environmental Monitoring drop-down menu and press **Apply**.

### ***Adding and Deleting outlet access:***

Click on the **Outlets** link in the Access column for the associated LDAP Group.

On the subsequent LDAP Group - Outlets page, select or deselect outlets to be accessed by the LDAP Group and press **Apply**.

### ***Adding and Deleting outlet group access:***

Click on the **Groups** link in the Access column for the associated LDAP Group.

On the subsequent LDAP Group - Groups page, select or deselect outlet groups to be accessed by the LDAP Group and press **Apply**.

### ***Adding and Deleting serial port access:***

Click on the **Ports** link in the Access column for the associated LDAP Group.

On the subsequent LDAP Group - Ports page, select or deselect ports to be accessed by the LDAP Group and press **Apply**.

## **TACACS+**

The TACACS+ configuration page is used for setup and maintenance of all settings required to enable TACACS+ support. For additional information and configuration requirements, see *TACACS+* on page 61.

### **Enabling or disabling TACACS+ support:**

Select **Enabled** or **Disabled** from the TACACS+ drop-down menu and press **Apply**.

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

Enter the IP address in the Host IP1 and/or Host IP2 address field and press **Apply**.

### **Setting the TACACS+ encryption key:**

Enter a key and verify the new key the Encryption Key and Verify Encryption Key fields. Press **Apply**.

For security, key characters are not displayed.

### **Configuring the authentication order:**

Select **Remote** -> **Local** or **Remote Only** from the drop-down menu and press **Apply**.

For more information on remote authentication order, see *Setting the authentication order* on page 62.

---

**NOTE:** Server Technology recommends NOT setting the authentication order to Remote Only until the LDAP has been fully configured and tested.

---

### **Configuring TACACS+ privilege levels:**

Click on the **TACACS+ Privilege Levels** link at the bottom of the page.

#### ***Changing an TACACS+ Privilege Level's access privilege level:***

Click on the **Edit** link in the Action column for the associated TACACS+ Privilege Level.

On the subsequent TACACS+ Privilege Level - Edit page, select **Admin**, **User**, **On-only** or **View-only** from the Access Level drop-down menu and press **Apply**.

For more information on access levels, see *Changing a user's access privilege level:* on page 17.

#### ***Granting or removing Environmental Monitoring viewing privileges:***

Click on the **Edit** link in the Action column for the associated TACACS+ privilege level.

On the subsequent TACACS+ Privilege Level - Edit page, select **Yes** or **No** from the Environmental Monitoring drop-down menu and press **Apply**.

### ***Adding and Deleting outlet access:***

Click on the **Outlets** link in the Access column for the associated TACACS+ Privilege Level.

On the subsequent LDAP Group - Outlets page, select or deselect outlets to be accessed by the TACACS+ Privilege Level and press **Apply**.

### ***Adding and Deleting outlet group access:***

Click on the **Groups** link in the Access column for the associated TACACS+ Privilege Level.

On the subsequent LDAP Group - Groups page, select or deselect outlet groups to be accessed by the TACACS+ Privilege Level and press **Apply**.

### ***Adding and Deleting serial port access:***

Click on the **Ports** link in the Access column for the associated TACACS+ Privilege Level.

On the subsequent LDAP Group - Ports page, select or deselect ports to be accessed by the TACACS+ Privilege Level and press **Apply**.

## **Tools**

The Tools section contains access to rebooting the unit, uploading new firmware as well as resetting the unit to factory defaults. This section is available to administrative level users only.

### **Restart**

#### **Performing a warm boot:**

Select the **Restart** from the Action drop-down menu and press **Apply**.

---

**Note:** System user/outlet/group configuration or outlet states are NOT changed or reset with this command.

---

#### **Resetting to factory defaults:**

See Chapter 5: for more information on resetting a Sentry to factory defaults from the HTML interface.

#### **Uploading new firmware:**

See Appendix B: for more information on uploading new firmware from the HTML interface.

### **Ping**

The Ping feature may be used to test the Sentry's ability to contact another Ethernet enabled device's IP address. For LDAP support, it may also be used to test the configuration of the Domain Name server IP address by testing for proper name resolution.

## Command Line Interface

### Logging In

Logging in through Telnet requires directing the Telnet client to the configured IP address of the unit.

Logging in through the Console (RS232) port requires the use of a terminal or terminal emulation software configured to support ANSI or VT100 and a supported data rate (300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200 BPS) - 8 data bits-no parity-one stop bit and Device Ready output signal (DTR or DSR).

#### To log in by RS-232 or Telnet:

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

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

---

**NOTE:** Logging in by Telnet will automatically open a session. It is not necessary to press Enter.

---

2. At the Username: and Password: prompts, enter a valid username and password. And press **Enter**.

You are given three attempts to enter a valid username and password combination. If all three fail, the session ends.

---

**NOTE:** The default Sentry username/password is `admn/admn`.

---

When you enter a valid username and password, the command prompt (Sentry:) appears. If a location identifier was defined, it will be displayed before the Sentry: prompt. See *Creating a location description* on page 36 for more information.

Commands may be entered in any combination of uppercase and lowercase. All command characters must be entered correctly; there are no command abbreviations. A user must have administrative privileges to use the administration commands. The following tables list and briefly describe each command.

#### Operations Command Summary

Command	Description
On	Turns one or more outlets on
Off	Turns one or more outlets off
Reboot	Reboots one or more outlets
Status	Displays the on/off status of one or more outlets
lLoad	Displays the total cumulative input load
lstat	Displays the status of the infeeds
Connect	Connects to a serial/Pass-Thru port
Login	Ends the current session and brings up the Username: prompt
Logout	Ends a session
Quit	Ends a session
List Outlets	Lists all accessible outlets for the current user
List Ports	Lists all accessible serial/Pass-Thru ports for the current user
List Group	Lists all assigned outlets for a group name
List Groups	Lists all accessible groups for the current user

#### Administrative Command Summary

Add Grouptouser	Grants a user access to one or more groups
Add Outlettogroup	Adds an outlet to a group name
Add Outlettouser	Grants a user access to one or all outlets
Add Porttouser	Grants a user access to one or all serial/Pass-Thru ports
Create Group	Adds a group name
Create User	Adds a user account
Delete Groupfromuser	Removes access to one or more groups for a user
Delete Outletfromgroup	Deletes an outlet from a group name
Delete Outletfromuser	Removes access to one or all outlets for a user
Delete Portfromuser	Removes access to one or all serial/Pass-Thru ports

## Administrative Command Summary (continued)

List User	Displays all accessible outlets/groups/ports for a user
List Users	Displays privilege levels for all users
Remove Group	Deletes a group name
Remove User	Deletes a user account
Restart	Performs a warm boot
Set DNS	Sets the IP address of the Domain Name server
Set Display	Sets the LED orientation for external Current displays
Set FTP Filename	Specifies the file to be uploaded via FTP
Set FTP Filepath	Specifies the filepath for the file to be uploaded
Set FTP Host	Sets the FTP Host IP address
Set FTP Password	Sets the password for the FTP Host
Set FTP Username	Sets the username for the FTP Host
Set Gateway	Sets the Gateway
Set HTTP	Enables or disables HTTP access
Set HTTP Port	Specifies the target port for HTTP access
Set HTTP Security	Specifies the HTTP server authentication method
Set Infeed Name	Specifies a descriptive field for the infeed
Set Ipaddress	Sets the IP address
Set Location	Specifies a descriptive field for the HTML control screen and login banner
Set Modem Inits	Enables or disables Modem port initialization strings
Set Modem	Specifies Modem port initialization strings
Set Outlet Name	Specifies a descriptive field for a device attached to an outlet
Set Outlet PostOnDelay	Sets the Post-On delay for an outlet
Set Outlet RebootDelay	Sets the reboot delay for all outlets
Set Outlet SeqInterval	Sets the sequencing interval for all outlets
Set Outlet Wakeup	Sets the wakeup state for an outlet
Set Subnet Mask	Sets the Subnet Mask
Set Telnet Port	Sets the Telnet server port number
Set Telnet	Enables or disables Telnet access
Set Tower Name	Specifies a descriptive field for the Sentry
Set User Access	Sets the access level for a user
Set User Envmon	Grants or removes privileges to view input and environmental monitoring status
Set User Password	Changes the password for a user
Set Port Name	Specifies a descriptive field for a serial/Pass-Thru port
Set Port Dsrchk	Sets the DSR active signal checking for a serial/Pass-Thru port
Set Port Speed	Set the connection speed for all serial/Pass-Thru ports
Set Port Timeout	Sets the inactivity timer for Pass-Thru sessions
Show FTP	Displays FTP configuration information
Show Infeeds	Displays infeed configuration information
Show Network	Display network configuration information
Show Outlets	Displays configuration information for all outlets
Show Ports	Displays serial/Pass-Thru port configuration information
Show System	Displays system configuration information
Show Towers	Displays tower configuration information
Version	Displays the Sentry firmware version

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

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

## **Operations Commands**

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

### **Turning outlets on**

The On command turns on one or more outlets. When the command completes, a display indicating all outlets affected and their current states will be displayed.

#### ***To turn outlets on:***

At the Sentry: prompt, type **on**, followed by an outlet name, 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 outlet on, using the outlet's absolute name:

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

The following command turns on all the outlets in the group named ServerGroup\_1:

```
Sentry: on ServerGroup_1<Enter>
```

### **Turning outlets off**

The Off command turns off one or more outlets. When the command completes, a display indicating all outlets affected and their current states will be displayed.

#### ***To turn outlets off:***

At the Sentry: prompt, type **off**, followed by an outlet name, 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 off the outlet named FileServer\_1:

```
Sentry: off FileServer_1<Enter>
```

The following command turns off all outlets:

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

### **Rebooting outlets**

The Reboot command reboots one or more outlets. This operation turns the outlet(s) off, delays for a user configurable period and then turns the outlet(s) on. When the command completes, a display indicating all outlets affected and their current states will be displayed.

---

**NOTE:** It is necessary to reissue the Status command to verify that the outlets have rebooted. See *Displaying outlet status for more information*.

---

#### ***To reboot one or more outlets:***

At the Sentry: prompt, type **reboot**, followed by an outlet name, and press **Enter**, or

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

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

#### **Example**

The following command reboots all the outlets in the group named ServerGroup\_1:

```
Sentry: reboot ServerGroup_1<Enter>
```

## Displaying outlet status

The Status command displays the on/off status of one or more outlets. The command displays the status of only those outlets for which the current username has power control access.

This display includes the outlet absolute and descriptive names, the Outlet State reported to the Sentry by the outlet and the current Control State being applied by the Sentry. If you do not specify any parameter with this command, the status of all accessible outlets is displayed.

---

**NOTE:** If the user has access to more than 16 total outlets, the Status command will display the first 16 outlets with a prompt to view the remaining outlets.

---

For more information on outlet and control state values, see *Outlet Control* on page 12.

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

At the Sentry: prompt, type **status**, followed by an outlet name, and press **Enter**, or

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

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

### **Examples**

The following command displays the on/off status of the outlet named FileServer\_1:

```
Sentry: status FileServer_1<Enter>
      Outlet  Outlet                Outlet  Control
      ID      Name                  State   State
      .A3     FileServer_1           On      On
```

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

```
Sentry: status<Enter>
      Outlet  Outlet                Outlet  Control
      ID      Name                  State   State
      .A1     DataServer_1         On      On
      .A2     WebServer_1         On      On
      .A3     FileServer_1         On      On
      .A4
```

The following command displays the on/off status for outlets in the group ServerGroup\_1:

```
Sentry: status ServerGroup_1<Enter>
Group: ServerGroup_1
      Outlet  Outlet                Outlet  Control
      ID      Name                  State   State
      .A1     DataServer_1         On      On
      .A2     WebServer_1         On      On
      .A3     FileServer_1         On      On
```

## Displaying accessible outlets

The List Outlets command displays accessible outlets for the current user. The display includes the absolute and descriptive name of all outlets assigned to the current user.

### *To display accessible outlets:*

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

### **Example**

The follow command displays all accessible outlets for the current user:

```
Sentry: list outlets<Enter>
      Outlet  Outlet
      ID      Name
      .A1     DataServer_1
      .A2     WebServer_1
```

## Displaying accessible groups

The List Groups command displays accessible groups for the current user.

### *To display accessible groups:*

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

### **Example**

The follow command displays all accessible groups for the current user:

```
Sentry: list groups<Enter>
Groups:
  ServerGroup_1
  RouterGroup_1
```

## Displaying outlets assigned to a group

The List Group command displays outlets assigned to the specified group name.

### *To display outlets assigned to a group:*

At the Sentry: prompt, type **list group**, followed by the group name and press **Enter**.

### **Example**

The follow command displays the outlets assigned to the group ServerGroup\_1:

```
Sentry: list group ServerGroup_1<Enter>
Group: ServerGroup_1
      Outlet  Outlet
      ID      Name
      .A1     DataServer_1
      .A2     WebServer_1
      .A3     FileServer_1
```

## Displaying accessible serial/Pass-Thru ports

The List Ports command displays accessible serial/Pass-Thru ports for the current user.

### *To display accessible serial/Pass-Thru ports:*

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

### **Example**

The follow command displays all accessible serial/Pass-Thru ports for the current user:

```
Sentry: list ports<Enter>
      Port    Port
      ID      Name
      Console Console
      Modem   Modem
      1       router1
```

## Displaying infeed status

The Istat or Iload command displays the status of one or more infeed.

This display includes the infeed absolute and descriptive names and the Input Status and current Load reported to the Sentry by the infeed.

### *To display status of one or more infeeds:*

Type **istat** and press **Enter**, or

Type **iload** and press **Enter**.

### *Examples*

The following command displays the infeed status:

```
Sentry: istat
```

Input Feed ID	Input Feed Name	Input Status	Input Load
.AA	HQ_1_Infeed_A	On	10.5 Amps

## Connecting to a serial device

The Connect command allows Pass-Thru serial connection to devices attached to one of the two standard serial ports (Console, Modem) or a Pass-Thru port.

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

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

### *Examples*

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

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

The follow command connects to the serial device connected to the Pass-Thru port 1:

```
Sentry: connect 1<Enter>
```

The follow command connects to the serial device connected to the Pass-Thru port named router1:

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

The port name was previously defined.

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

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

## 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

The Quit or Logout commands ends a session. A session ends automatically when no activity is detected for five minutes, or upon loss of connection.

### *To end a session:*

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

Type **logout** and press **Enter**.

## **Administration Commands**

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 Set User Admnpriv command.

### **User Administration**

#### **Creating a user account**

The Create User command creates a user account with the specified username and password. See *Usernames and Passwords* in this chapter for more information.

##### ***To create a user account:***

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

At the Password: prompt, type a password of 1-16 alphanumeric and other typeable characters (ASCII 32 to 126 decimal). Passwords are case sensitive. Press **Enter**.

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

##### ***Example***

The following command creates the user account JaneDoe:

```
Sentry: create user JaneDoe<Enter>
Password: <Enter>
Verify New Password: <Enter>
```

For security, password characters are not displayed.

#### **Removing a user account**

The Remove User command removes a user account.

---

**NOTE:** You may remove the predefined user account Admn only if another user account has been granted administrative privileges using the Set User Admnpriv command.

---

##### ***To remove a user account:***

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

#### **Changing a password**

The Set User Password command changes a user's password. For security, when you type a password, the characters are not displayed on the screen. See *Usernames and Passwords* for more information.

##### ***To change a password:***

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

At the Password: prompt, type the new password and press **Enter**. Passwords may contain 1-16 characters.

At the Verify Password: prompt, retype the new password and press **Enter**.

##### ***Example***

The following command changes the password for the user JohnDoe:

```
Sentry: set user password johndoe<Enter>
Password: <Enter>
Verify Password: <Enter>
```

For security, password characters are not displayed.

## Setting user access level privileges

The Set User Access command sets the access level privileges for a user. The Sentry has four defined access privilege levels; Admin, User, On-Only and View-Only. For more information on user access levels, see *Changing a user's access privilege level*: on page 17.

The administrator may also grant administrative privileges to other user accounts allowing the Sentry to have more than one administrative-level user.

---

**NOTE:** You cannot remove administrative privileges from the Admn user unless another user has already been given administrative access level privileges created.

---

### *To set the access level privilege for a user:*

At the Sentry: prompt, type **set user access**, followed by **admin** or **user**, optionally followed by a username and press **Enter**.

### **Examples**

The following command sets the user access level for JohnDoe to Admin:

```
Sentry: set user access admin johndoe<Enter>
```

The following command sets the user access level for JaneDoe to User:

```
Sentry: set user access user janedoe<Enter>
```

## Granting and removing input load viewing privileges

The Set User Envmon command grants or removes input load viewing privileges to/from a general or view-only user.

---

**NOTE:** This command also grants or removes viewing privileges for the status of the optional Equipment Cabinet Environmental Manager and attached sensors. See the *Equipment Cabinet Environmental Manager Installation and Operations manual* for more information.

---

### *To grant or remove input load viewing privileges for a user:*

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

### **Example**

The following command grants input load privileges to the user JohnDoe:

```
Sentry: set user envmon on johndoe<Enter>
```

## Displaying the access privilege levels

The List Users command displays all defined users with their access privilege level.

### *To display user access privilege levels:*

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

### **Example**

The following command displays all users with their access privilege level:

```
Sentry: list users<Enter>
```

User Name	Privilege Level	Environmental Monitoring
JOHNDOE	Admin	Allowed
JANEDOE	User	Allowed
JOSEYDOE	On-Only	Not Allowed
JOEDOE	View-Only	Not Allowed

## Adding outlet access to a user

The Add OutletToUser command grants a user access to one or all outlets. To grant access for more than one outlet, but not all outlets, you must use multiple Add OutletToUser commands.

### *To grant outlet access to a user:*

At the Sentry: prompt, type **add outlettouser**, optionally followed by an outlet name and a username. Press **Enter**, or

Type **add outlettouser all**, followed by a username and press **Enter**.

### **Examples**

The following commands grant the user JaneDoe access to outlets A1 and Webserver\_1:

```
Sentry:add outlettouser .a1 janedoe<Enter>
Sentry:add outlettouser WebServer_1 janedoe<Enter>
```

## Deleting outlet access for a user

The Delete OutletFromUser command removes a user's access to one or all outlets. You cannot remove access to any outlet for an administrative level user.

### *To delete outlet access for a user:*

At the Sentry: prompt, type **delete outletfromuser**, optionally followed by an outlet name and a username. Press **Enter**, or

Type **delete outletfromuser all**, followed by a username and press **Enter**.

## Adding group access to a user

The Add GroupToUser command grants a user access to a group. To grant access for more than one group, you must use multiple Add GroupToUser commands.

### *To grant group access to a user:*

At the Sentry: prompt, type **add grouptouser**, optionally followed by a group name and a username. Press **Enter**.

### **Examples**

The following commands grants to user JaneDoe access to the groups ServerGroup\_1 and ServerGroup\_2:

```
Sentry:add GroupToUser ServerGroup_1 janedoe<Enter>
Sentry:add GroupToUser ServerGroup_2 janedoe<Enter>
```

## Deleting group access for a user

The Delete GroupFromUser command removes a user's access to a group. You cannot remove access to any group for an administrative level user.

### *To delete group access for a user:*

At the Sentry: prompt, type **delete GroupFromUser**, optionally followed by a group name and a username. Press **Enter**.

## Adding serial/Pass-Thru port access to a user

The Add PortToUser command grants a user access to a serial/Pass-Thru port. To grant access for more than one port, you must use multiple Add PortToUser commands.

### *To grant serial/Pass-Thru port access to a user:*

At the Sentry: prompt, type **add porttouser**, optionally followed by a Port name and a username. Press **Enter**.

### **Examples**

The following commands grants to user JaneDoe access to the Modem port:

```
Sentry:add PortToUser modem janedoe<Enter>
```

## Deleting serial/Pass-Thru port access for a user

The Delete PortFromUser command removes a user's access to a serial/Pass-Thru port. You cannot remove access to any serial/Pass-Thru port for an administrative level user.

### *To delete serial/Pass-Thru port access for a user:*

At the Sentry: prompt, type **delete portfromuser**, optionally followed by a Port name and a username. Press **Enter**.

## Displaying user outlet, group and serial/Pass-Thru port access

The List User command displays all accessible outlets, groups and serial/Pass-Thru ports for a user.

### *To display user outlet, group and serial/Pass-Thru port access:*

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

### **Example**

The following command displays information about the user JaneDoe:

```
Sentry: list user janedoe<Enter>
Username: JANEDOE
Outlet   Outlet
ID       Name
.A1     DataServer_1
.A2     WebServer_1
Groups:
  ServerGroup_1
  ServerGroup_2
More (Y/es N/o): Y
Ports:
Port     Port
ID       Name
Console  Console
Modem    Modem
1        router1
```

JaneDoe may access the following outlets, groups and serial ports: outlet A1 which has a descriptive name of DataServer\_1, outlet A2 which has a descriptive name of WebServer\_1, group ServerGroup\_1 group ServerGroup\_2, Console serial port and Modem serial port.

## **Outlet Administration**

### **Setting the sequencing interval**

The Set Outlet SeqInterval commands sets the power on sequencing interval for all outlets.

#### *To set the sequencing interval:*

At the Sentry: prompt, type **set outlet seqinterval all**, followed by a value from 2 to 15 (in seconds) and press Enter.

### **Setting the reboot delay**

The Set Outlet RebootDelay commands sets the reboot delay for all outlets.

#### *To set the sequencing interval:*

At the Sentry: prompt, type **set outlet rebootdelay all**, followed by a value from 5 to 60 (in seconds) and press Enter.

## Creating a descriptive outlet name

The Set Outlet Name command assigns a descriptive name to an outlet. You may use this name in commands that require an outlet name as an alternative to using the outlet's absolute name.

### *To create an outlet name:*

At the Sentry: prompt, type **set outlet name**, followed by the absolute outlet name and a descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal - spaces are not allowed). Outlet names are not case sensitive. Press **Enter**.

### **Example**

The following command adds the descriptive name DataServer\_1 to outlet .a1:

```
Sentry: set outlet name .a1 DataServer_1<Enter>
```

## Setting the outlet wakeup state

The Set Outlet Wakeup command set the default wakeup state for that outlet. In the event of a system-wide power loss, this state will be applied to the outlet when power is restored.

The wakeup state may be set to On, Off or Last. Upon restoration of system power; If set to On, the Sentry will apply power to that outlet. If set to Off, the Sentry will not apply power to that outlet. If set to Last, the Sentry will apply the last known power state.

### *To set the wakeup state:*

At the Sentry: prompt, type **set outlet wakeup**, followed by **on**, **off** or **last** and the outlet name. Press **Enter**.

### **Example**

The following command sets the wakeup state for outlet .a1 to off:

```
Sentry: set outlet wakeup off .a1<Enter>
```

## Setting the outlet Post-On delay

The Set Outlet PostOnDelay command is used set the Post-On delay for an outlet. This feature allows the administrator to manage boot dependencies during power-on sequencing or group commands by delaying the sequencing of subsequent outlets after an outlet has been powered on.

---

**NOTE:** This delay is applied *in addition* to the general sequencing interval.

---

### *To set the outlet Post-On delay*

At the Sentry: prompt, type **set outlet postondelay**, followed by a value from 0 to 900 (in seconds) and press **Enter**.

### **Example**

The following command set the Post-On delay for outlet .a4 to 90 seconds:

```
Sentry: set outlet postondelay .a4 90<Enter>
```

## Displaying outlet information

The Show Outlets command displays information about all outlets. This information includes:

- Sequencing and reboot timer values
- Descriptive outlet name, if applicable
- Outlet wakeup state and Post-On settings

### *To display outlet information:*

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

### **Example**

The following command displays all outlet information:

```
Sentry: show outlets<Enter>
Outlet      Outlet      Wakeup      Post-On
ID          Name          State        Delay (seconds)
.A1         TowerA_Outlet1  On           0
.A2         TowerA_Outlet2  On           0
.A3         FileServer_1    On           0
.A4         .A4             On           90

Outlet Options:
Sequence Interval:  2 seconds
Reboot Delay:      15 seconds
```

## Group Administration

### **Creating a group name**

The Create Group command creates a new group name.

### *To create a group name:*

At the Sentry: prompt, type **create group**, optionally followed by a descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal - spaces are not allowed. Group names are not case sensitive). Press **Enter**.

### **Example**

The following command creates group name ServerGroup\_1:

```
Sentry: create group ServerGroup_1<Enter>
```

### **Removing a group name**

The Remove Group command removes a group name.

### *To remove a group name:*

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

### **Example**

The following command removes group name ServerGroup\_1:

```
Sentry: remove group ServerGroup_1<Enter>
```

## Adding an outlet to a group

The Add OutletToGroup command adds an outlet to a group. To add more than one outlet, but not all outlets, you must use multiple Add OutletToGroup commands.

### *To add an outlet to a group:*

At the Sentry: prompt, type **add outlettogroup**, optionally followed by an outlet name and group name. Press **Enter**, or

Type **add OutletToGroup**, followed by **all** and the group name. Press **Enter**.

### **Examples**

The following commands uses absolute outlet names to add outlets A1 and A2 to group name ServerGroup\_1:

```
Sentry:add OutletToGroup .a1 ServerGroup_1<Enter>
Sentry:add OutletToGroup .a2 ServerGroup_1<Enter>
```

The following commands use the outlets' descriptive names to add outlets DataServer\_1 and WebServer\_1 to group name ServerGroup\_1:

```
Sentry:add OutletToGroup DataServer_1 ServerGroup_1<Enter>
Sentry:add OutletToGroup WebServer_1 ServerGroup_1<Enter>
```

The following command add all outlets to group name ServerGroup\_1:

```
Sentry: add OutletToGroup<Enter>
Outletname: all<Enter>
Groupname: ServerGroup_1<Enter>
```

## Deleting an outlet from a group

The Delete OutletFromGroup command deletes an outlet from a group. To delete more than one outlet, but not all outlets, you must use multiple Delete OutletToGroup commands.

### *To delete an outlet from a group:*

At the Sentry: prompt, type **delete outletfromgroup**, optionally followed by an outlet name and a group name. Press **Enter**, or

Type **delete outletfromgroup**, followed by **all** then the group name. Press **Enter**.

## Serial Port Administration

### Creating a descriptive serial port name

The Set Port Name command assigns a descriptive name to a serial port. You may use this name in commands that require a port name as an alternative to using the port's absolute name.

#### *To create an port name:*

At the Sentry: prompt, type **set port name**, followed by the absolute outlet name and a descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal - spaces are not allowed). Port names are not case sensitive. Press **Enter**.

#### **Example**

The following command adds the descriptive name Rack1 to Console port:

```
Sentry: set port name console Rack1<Enter>
```

### Setting the serial ports data-rate

The Set Port Speed command sets the default data-rate for the serial port. Valid data-rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600 and 115200.

#### *To set the serial port data-rate:*

At the Sentry: prompt, type **set port speed**, follow by the data-rate and press **Enter**.

#### **Example**

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

```
Sentry: set port speed 38400<Enter>
```

## Enabling or disabling active signal checking for serial/Pass-Thru connections

The Set Port Dsrchk command enables or disables active signal checking for serial/Pass-Thru connections to devices attached to any of the available serial ports.

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

At the Sentry: prompt, type **set port dsrchk**, followed by serial port name, **on** or **off**, and press **Enter**, or Type **set port dsrchk all, on** or **off**, and press **Enter**.

### **Examples**

The following command disables active signal checking for the Modem serial port:

```
Sentry: set port dsrchk modem off<Enter>
```

The following command enables active signal checking for Pass-Thru port 1:

```
Sentry: set port dsrchk 1 on<Enter>
```

The following command disables active signal checking for all serial/Pass-Thru ports:

```
Sentry: set port dsrchk all off<Enter>
```

## Setting the serial port timeout value

The Set Port Timeout command is used to set the serial port inactivity timeout period. The timeout period defines the maximum period of inactivity before automatically closing the Pass-Thru session. The valid range for the period parameter is 0 to 5 (in minutes). The default period is 5.

---

**NOTE: Setting the timeout to '0' disables the timer.**

---

### *To set the serial port timeout value:*

At the Sentry: prompt, type **set port timeout**, followed by a value from 0 to 5 (in minutes) and press **Enter**.

## Enabling or disabling modem initialization strings

By default, the Sentry assumes an external modem is attached to the Modem port and sends initialization strings to that modem as necessary. The Sentry sends the initialization strings under the following conditions:

- System start – DSR is high and DCD is low
- Normal operations – If DSR transitions from low to high and DCD is low
- Normal operations – After a session initiated from the Modem port ends
- Normal operations – After a Pass-Thru connection to the Modem port is disconnected

The Set Modem command is used to enable or disable these initialization strings. Predefined initialization strings are enabled by default.

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

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

### **Example**

The following command disables the modem initialization strings for the Modem serial port:

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

## Editing modem initialization strings

The predefined modem initialization strings may be edited by an administrative user. The Init 1 and Init 2 strings may be up to 48 characters each and the Attention and Hang-up strings may be up to 16 characters.

For more information on the predefined initialization strings, see *Enabling or disabling modem initialization strings*: on page 15.

### *Editing modem initialization strings:*

At the Sentry: prompt, type **set modem**, followed by **attn**, **hangup**, **init1**, or **init 2** and the initialization string. Press **Enter**.

### **Examples**

The following command set the Init 2 string to 'AT E0 Q1 S0=3 S2=64 S12=50 &C1 &D2':

```
Sentry: set modem init2 AT E0 Q1 S0=3 S2=64 S12=50 &C1 &D2<Enter>
```

## Displaying serial/Pass-Thru port information

The Show Ports command displays information about all serial/Pass-Thru ports. This information includes:

- Serial/Pass-Thru port data rate
- Modem port initialization strings
- Descriptive port name, if applicable
- DSR signal checking settings

### *To display serial port information:*

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

### **Example**

The following command displays all serial/Pass-Thru port information:

```
Sentry: show ports<Enter>
Serial Port Configuration
  ALL Ports:
    Baud Rate: 38400
  Console Port:
    DSR Check: ON
  Modem Port:
    DSR Check: ON
  Initializations: ON
    Init String 1:  AT
    Init String 2:  AT E0 Q1 S0=1 S2=64 S12=50 &C1 &D2
    Attention String: @@@
    Hang-Up String:  ATH
More (Y/es N/o): Y
Pass-Through Ports
  Port   Port           DSR
  ID     Name            Check
  ---     ---            ---
  1      Router1         ON
  2      Port_2          OFF
  3      Port_3          ON
  4      Port_4          ON
```

## **System Administration**

### **Creating a location description**

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

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.

### *To create a location description:*

At the Sentry: prompt, type **set location**, followed by a descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 32 to 126 decimal - 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.

## Setting the LED display orientation

The Set Display command is used to configure the Current LED(s) display orientation.

### *To set the LED display orientation:*

At the Sentry: prompt, type **set display**, followed by **normal** or **inverted** and press **Enter**.

### **Example**

The following set the LED display orientation to Inverted:

```
Sentry: set display inverted<Enter>
```

---

**NOTE:** When set to Inverted, the load will be reported in whole ampere increments

---

## Displaying system configuration information

The Show System command displays all system configuration information.

- Firmware version
- NIC module serial number and MAC address
- Hardware revision code and Flash size
- Uptime since last system restart
- System location description

See Chapter 4: Advanced Operations on page 43 for more information on SNMP.

### *To display system configuration information:*

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

### **Example**

```
System Information
  F/W Version:   Sentry Version 5.2b
  NIC S/N:       1600001
  MAC Address:   00-0a-9c-10-00-01
  H/W Rev Code:  0
  Flash Size:    1 MB
  Uptime:        0 days 6 hours 14 minutes 1 second
  Location:      Florida HQ
```

## Creating a descriptive tower name

The Set Tower Name command assigns a descriptive name to a tower. This descriptive name is displayed when the Show Traps command is issued. See *Displaying trap configuration information* on page 38 for more information on the Show Traps command.

### *To create a tower name:*

At the Sentry: prompt, type **set tower name**, followed by the absolute tower name, then the descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal - spaces are not allowed). Press **Enter**.

### **Example**

The following command adds the descriptive name Florida\_HQ\_1 to tower .a:

```
Sentry: set tower name .a Florida_HQ_1<Enter>
```

## Displaying tower information

The Show Towers command displays information about the Sentry. This information includes the absolute and descriptive Sentry names.

### *To display tower information:*

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

### **Example**

```
Sentry: show towers<Enter>
Tower   Tower
ID      Name
.A      Florida_HQ_1
```

## Creating a descriptive infeed name

The Set Infeed Name command assigns a descriptive name to an infeed. This descriptive name is displayed when the Show Traps command is issued. See *Displaying trap configuration information* on page 38 for more information on the Show Traps command.

### *To create a infeed name:*

At the Sentry: prompt, type **set infeed name**, followed by the absolute infeed name, then the descriptive name of up to 24 alphanumeric and other typeable characters (ASCII 33 to 126 decimal - spaces are not allowed). Press **Enter**.

### *Example*

The following command adds the descriptive name HQ\_1\_Infeed\_A to the infeed on the Sentry:

```
Sentry: set infeed name .aa HQ_1_Infeed_A<Enter>
```

## Displaying infeed information

The Show Infeeds command displays information about all infeeds. This information includes the absolute and descriptive infeed names.

### *To display tower information:*

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

### *Example*

```
Sentry: show infeeds<Enter>
      Input      Input
      Feed ID    Feed Name
      .AA        HQ_1_Infeed_A
```

## Displaying the Sentry firmware version

The Version command displays the Sentry firmware version.

### *To display the firmware version:*

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

## Performing a warm boot

The Restart command performs a warm boot of the Sentry.

---

**NOTE:** System user/outlet/group/port configuration or outlet states are NOT changed or reset with this command.

---

### *To perform a warm boot:*

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

## TCP/IP Administration

---

**NOTE:** A restart of the Sentry is required after setting or changing ANY TCP/IP configurations. See *Performing a warm boot* on page 38 for more information.

---

## Setting the IP address

The Set Ippaddress command sets the TCP/IP address of the network interface controller.

### *To set the IP address:*

At the Sentry: prompt, type **set ipaddress**, followed by the IP address and press **Enter**.

### *Example*

The following command sets the IP address to 12.34.56.78:

```
Sentry: set ipaddress 12.34.56.78<Enter>
```

## Setting the subnet mask

The Set Subnet command sets the subnet mask for the network the PT40 will be attached to.

### *To set the subnet mask:*

At the Sentry: prompt, type **set subnet**, followed by the subnet mask and press **Enter**.

### **Example**

The following command sets the subnet mask to 255.0.0.0

```
Sentry: set subnet 255.0.0.0<Enter>
```

## Setting the gateway

The Set Gateway command sets the IP address of the default gateway the Sentry uses to access external networks.

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

At the Sentry: prompt, type **set gateway**, followed by the gateway IP address and press **Enter**.

### **Example**

The following command set the gateway IP address to 12.34.56.1:

```
Sentry: set gateway 12.34.56.1<Enter>
```

## Setting the DNS IP address

The Set DNS command sets the TCP/IP address of the Domain Name server (DNS).

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

At the Sentry: prompt, type **set**, followed by **dns1** or **dns2** and the Domain Name server's IP address. Press **Enter**.

### **Example**

The following command sets the primary Domain Name server IP address to 98.76.54.254:

```
Sentry: set dns1 98.76.54.254<Enter>
```

## Displaying network configuration information

The Show Network command displays TCP/IP, Telnet, SSH, Web, SSL and SNMP configuration information.

- IP address, subnet mask, gateway and DNS IP addresses
- Enabled-disabled status and port numbers for Telnet, SSH, HTTP,SSL and SNMP support
- HTTP authentication method and SSL access setting
- Network status

See Chapter 4: Advanced Operations on page 43 for more information on SNMP and Remote Authentication

### *To display network configuration information:*

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

### **Example**

The following command displays the network configuration information:

```
Sentry: show network<Enter>
Network Configuration
  IP Address:    12.34.56.78           DNS1: 98.76.54.254
  Subnet Mask:  255.0.0.0             DNS2: 0.0.0.0
  Gateway:      12.34.56.1
  Telnet:       Enabled               Port:   23
  SSH:          Enabled               Port:  65535
  HTTP:         Enabled               Port:   80   Security: BASIC
  SSL:          Enabled
  SNMP:         Enabled               Access:  Required

Network Status
  Link:         Up
  Speed:        100 Mbps
  Duplex:       Full
  Negotiation:  Auto
```

## HTTP Administration

---

*NOTE: A restart is required after setting or changing ANY Telnet/Web configurations. See [Performing a warm boot on page 38](#) for more information.*

---

### Enabling and disabling HTTP support

The Set HTTP command is used to enable or disable HTTP support.

#### *To enable or disable HTTP support:*

At the Sentry: prompt, type **set http**, followed by **enabled** or **disabled** and press **Enter**.

### Changing the HTTP server port

With HTTP support enabled, the HTTP server watches and responds to requests on the default HTTP port number 80. This port number may be changed using the Set HTTP Port command.

#### *To change the HTTP port:*

At the Sentry: prompt, type **set http port**, followed by the port number and press **Enter**.

#### **Example**

The following changes the HTTP port number to 2048:

```
Sentry: set HTTP port 2048<Enter>
```

### Setting the HTTP authentication method

The Set HTTP Security command is used to set the method of authentication. The Sentry HTTP server supports two authentication methods for security and validation of the username-password – Basic and MD5 digest.

For more information on authentication methods, see *Setting the HTTP authentication method:* on page 14.

#### *To set the HTTP authentication method:*

At the Sentry: prompt, type **set http security**, followed by **basic** or **md5** and press **Enter**.

## Telnet Administration

---

*NOTE: A restart of the Sentry is required after setting or changing ANY Telnet/Web configurations. See [Performing a warm boot on page 38](#) for more information.*

---

### Enabling and disabling Telnet support

The Set Telnet command is used to enable or disable Telnet support.

#### *To enable or disable Telnet support:*

At the Sentry: prompt, type **set telnet**, followed by **enabled** or **disabled** and press **Enter**.

### Changing the Telnet port

With Telnet support enabled, the Telnet server watches and responds to requests on the default Telnet port number 23. This port number may be changed using the Set Telnet Port command.

#### *To change the Telnet socket:*

At the Sentry: prompt, type **set telnet port**, followed by the port number and press **Enter**.

#### **Example**

The following changes the Telnet port number to 7001:

```
Sentry: set telnet port 7001<Enter>
```

## **FTP Administration**

You may upload new versions of firmware into the Sentry using File Transfer Protocol (FTP). This allows access to new firmware releases for firmware improvements and new features additions. The following commands are used to configure the Sentry for an FTP firmware upload. See Appendix B: Uploading Firmware for more information on initiating a FTP firmware upload.

### **Setting the FTP Host IP address**

The Set FTP Host command sets the FTP host IP address allowing for firmware file uploads.

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

At the Sentry: prompt, type **set ftp host**, followed by the Host IP address and press **Enter**.

#### ***Example***

The following command sets the FTP Host IP address to 12.34.56.99:

```
Sentry: set ftp host 12.34.56.99<Enter>
```

### **Setting the FTP username**

The FTP Username command sets the username as required by the FTP Host.

#### ***To set the FTP username:***

At the Sentry: prompt, type **set ftp username**, followed by the FTP username and press **Enter**.

#### ***Example***

The following command sets the FTP username to Guest:

```
Sentry: set ftp username guest<Enter>
```

### **Setting the FTP Password**

The FTP Password command sets the password as required by the FTP Host.

#### ***To set the FTP password:***

At the Sentry: prompt, type **set ftp password**, followed by the FTP password and press **Enter**.

#### ***Example***

The following command sets the FTP password to OpenSesame:

```
Sentry: set ftp password OpenSesame<Enter>
```

### **Setting the filename to be uploaded**

The FTP Filename command sets the filename of the firmware file to be uploaded.

#### ***To set the FTP filename:***

At the Sentry: prompt, type **set ftp filename**, followed by the firmware filename and press **Enter**.

#### ***Example***

The following command sets the FTP filename to snb\_s50a.bin:

```
Sentry: set ftp filename snb_s50a.bin<Enter>
```

### **Setting the filepath for the file to be uploaded**

The FTP Filepath command sets the filepath for the firmware file to be uploaded.

#### ***To set the FTP filepath:***

At the Sentry: prompt, type **set ftp filepath**, followed by the filepath and press **Enter**.

#### ***Example***

The following command sets the FTP filepath to ftp://Sentry:

```
Sentry: set ftp filepath ftp://sentry<Enter>
```

## Displaying FTP configuration information

The Show FTP command displays all FTP configuration information.

- FTP Host IP address
- FTP Host username and password
- Firmware filepath and filename

### *To display FTP configuration information:*

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

### **Example**

The following command displays the FTP configuration information:

```
Sentry: show ftp<Enter>
FTP Configuration
Host IP Address: 12.34.56.99
Username:       guest
Password:       OpenSesame
Directory:      ftp://sentry
Filename:       snb_s52a.bin
```

## SNTP Administration

Sentry supports the use of a network time service to provide a synchronized time reference.

### Setting the SNTP server address

The Set SNTP command is used to set the primary and secondary SNTP server addresses.

### *To set the SNTP server address:*

At the Sentry: prompt, type **set sntp**, followed by **primary** or **secondary**, and the SNTP server IP address. Press **Enter**.

### **Example**

The following command set the primary SNTP server address to 204.152.184.72:

```
Sentry: set sntp primary 204.152.184.72<Enter>
```

## Displaying SNTP configuration information

The Show SNTP command displays all SNTP configuration information.

### *To display SNTP configuration information*

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

### **Example**

The following command displays the SNTP configuration information:

```
Sentry: show sntp <Enter>
SNTP Date/Time (GMT): 2003-02-21 21:32:48
SNTP Primary IP Address: 204.152.184.72
SNTP Secondary IP Address: 0.0.0.0
```

## Chapter 4: Advanced Operations

<b>SSL</b>	<b>44</b>
Enabling and Setting up SSL Support	44
SSL Technical Specifications	44
<b>SSH</b>	<b>45</b>
Enabling and Setting up SSH Support	45
SSH Technical Specifications	45
<b>SNMP</b>	<b>46</b>
MIB, OID and Support	46
Enabling and Setting up SNMP Support	46
SNMP Traps	48
Configuring Traps	49
<b>LDAP</b>	<b>52</b>
Enabling and Setting up LDAP Support	53
Configuring LDAP Groups	57
LDAP Technical Specifications	60
<b>TACACS+</b>	<b>61</b>
Enabling and Setting up TACACS+ Support	61
Configuring TACACS+ Privilege Levels	63
TACACS+ Technical Specifications	65

## SSL

Secure Socket Layers (SSL) version 3 enables secure HTML sessions between a Sentry Remote Power Manager and a remote user. SSL provides two chief features designed to make TCP/IP (Internet) transmitted data more secure:

- Authentication – The connecting client is assured of the identity of the server.
- Encryption – All data transmitted between the client and the server is encrypted rendering any intercepted data unintelligible to any third party.

SSL uses the public-and-private key encryption system by RSA, which also requires the use of digital certificates. An SSL Certificate is an electronic file uniquely identifying individuals or websites and enables encrypted communication; SSL Certificates serve as a kind of digital passport or credential. The Sentry product's SSL Certificate enables the client to verify the Sentry's authenticity and to communicate with the Sentry securely via an encrypted session, protecting confidential information from interception and hacking.

### SSL Command Summary

Command	Description
Set SSL	Enables/disables SSL support
Set SSL access	Sets SSL access as optional or required

### Enabling and Setting up SSL Support

**NOTE:** A restart of the Sentry is required after setting or changing ANY SSL configurations. See *Performing a warm boot* on page 38 for more information.

#### Enabling or disabling SSL support

The Set SSL command is used to enable or disable SSL support.

*To enable or disable SSL support:*

At the Sentry: prompt, type **set ssl**, followed by **enabled** or **disabled** and press **Enter**.

#### Setting SSL access level

The Set SSL Access command is used to assign use of SSL as optional or required. The default access level is set to optional.

*To change the access level:*

At the Sentry: prompt, type **set ssl access**, followed **optional** or **required**, and press **Enter**.

#### Example

The following changes the access level to required:

```
Sentry: set ssl access required<Enter>
```

### SSL Technical Specifications

Secure Socket Layer (SSL) version 3

Transport Layer Security (TLS) version 1 (RFC 2246)

SSL/TLS-enabled HTTPS server (RFC 2818)

Self-Signed X.509 Certificate version 3 (RFC 2459)

Asymmetric Cryptography:

1024-bit RSA Key Exchange

Symmetric Cryptography Ciphers:

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

TLS\_RSA\_WITH\_DES\_CBC\_SHA

## SSH

Secure Shell (SSH) version 2 enables secure network terminal sessions between a Sentry Remote Power Manager and a remote user over insecure network. SSH provides an encrypted terminal sessions with strong authentication of both the server and client, using public-key cryptography and is typically used as a replacement for unencrypted Telnet. In addition to enabling secure network terminal sessions to the Sentry for configuration and power management, the SSH session may be used for secure Pass-Thru connections to attached devices.

SSH requires the configuration and use of a client agent on the client PC. There are many freeware, shareware or for-purchase SSH clients available. Two examples are the freeware client PuTTY and the for-purchase client SecureCRT® by VanDyke® Software. For configuration and use of these clients, please refer to the applicable software documentation.

### SSH Command Summary

Command	Description
Set SSH	Enables/disables SSH support
Set SSH port	Sets the SSH server port number

### Enabling and Setting up SSH Support

**NOTE:** A restart of the Sentry is required after setting or changing ANY SSH configurations. See *Performing a warm boot* on page 38 for more information.

#### Enabling or disabling SSH support

The Set SSH command is used to enable or disable SSH support.

##### *To enable or disable SSH support:*

At the Sentry: prompt, type **set ssh**, followed by **enabled** or **disabled** and press **Enter**.

#### Changing the SSH server port

With SSH support enabled, the SSH server watches and responds to requests on the default SSH port number 22. This port number may be changed using the Set SSH Port command.

##### *To change the SSH port:*

At the Sentry: prompt, type **set ssh port**, followed by the port number and press **Enter**.

##### **Example**

The following changes the SSH port number to 65535:

```
Sentry: set ssh port 65535<Enter>
```

### SSH Technical Specifications

Secure Shell (SSH) version 2

Asymmetric Cryptography:

Diffie-Hellman DSA/DSS 512-1024 (random) bits per NIST specification

Symmetric Cryptography:

AES256-CBC	RIJNDAEL256-CBC	3DES-192-CBC
AES192-CBC	RIJNDAEL192-CBC	BLOWFISH-128-CBC
AES128-CBC	RIJNDAEL128-CBC	ARCFOUR-128

Message Integrity:

HMAC-SHA1-160	HMAC-SHA1-96
HMAC-MD5-128	HMAC-MD5-96

Authentication:

Username/Password

Session Channel Break Extension (for RS232 Break)

## SNMP

The Sentry family of products 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 outlets.

The Sentry includes an SNMP v2c agent supporting standard MIB I and MIB II objects. A private enterprise MIB extension (Sentry3 MIB) is also supported to provide remote power control.

See *SNMP* on page 18, for information on enabling and configuring SNMP.

---

**NOTE:** For security, SNMP support is disabled by default.

---

### SNMP Command Summary

Command	Description
Set snmp	Enables or disables SNMP support
Set snmp getcomm	Sets the 'get' community string
Set snmp setcomm	Sets the 'set' community string
Set snmp trapdest1	Sets a destination IP addresses for traps
Set snmp trapdest2	Sets a destination IP addresses for traps
Set snmp traptime	Sets the delay for steady state condition traps
Show snmp	Displays all SNMP configuration information

### MIB, OID and Support

The Sentry SNMP MIB and OID are available on the Server Technology website:

`ftp://ftp.servertech.com/pub/SNMP/sentry3`

Technical support is available 8:30AM to 5:00 PM Pacific Time, Monday-Friday.

For SNMP Support, email: `mibmaster@servertech.com`

### Enabling and Setting up SNMP Support

Sentry SNMP support must be enabled and configured for access to Sentry3 MIB objects and generation of all Sentry3 traps.

#### Enabling/disabling SNMP support

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

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

At the Sentry: prompt, type **set snmp**, followed by **enabled** or **disabled** and press **Enter**.

---

**NOTE:** A restart of the Sentry is required after enabling or disabling SNMP support. See *Performing a warm boot* on page 38 for more information.

---

#### Setting trap destinations

The Set SNMP Trapdest1 and Trapdest2 commands are 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 Sentry: prompt, type **set snmp, trapdest1** or **trapdest2**, the Ipaddress and press **Enter**.

##### **Example**

The following sets the trap destination 1 to 64.42.31.208:

```
Sentry: set snmp trapdest1 64.42.31.208<Enter>
```

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

At the Sentry: prompt, type **set snmp, trapdest1** or **trapdest2, 0.0.0.0** and press **Enter**.

## Setting the trap timer

The Set Traptimer command sets the timer period between repeated error-condition traps. The valid range for the timer period is 1 to 65535 (in seconds). The default value for the timer period is 60 seconds.

### *To set the trap timer:*

At the Sentry: prompt, type **set traptimer**, followed by the timer period and press **Enter**.

### *Example*

The following sets the timer period to 180 seconds:

```
Sentry: set traptimer 180<Enter>
```

## Setting the Get/Set community strings

Sentry supports two SNMP community strings that provide varying levels of access to objects defined in the Sentry3 MIB.

Community strings may be 1 to 24 characters.

### Setcomm

The Setcomm string provides read-write access to sentry3 MIB objects. The default Setcomm string is "private".

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

At the Sentry: prompt, type **set snmp setcomm**, followed by the string and press **Enter**.

### Getcomm

The Getcomm string provides read-only access to sentry3 MIB objects. The default Getcomm string is "public".

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

At the Sentry: prompt, type **set snmp getcomm**, followed by the string and press **Enter**.

## Setting the Trap community string

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

The trap community string may be 1 to 24 characters. The default Trapcomm string is "trap".

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

At the Sentry: prompt, type **set snmp trapcomm**, followed by the string and press **Enter**.

## Displaying SNMP configuration information

The Show SNMP command displays all SNMP configuration information.

- SNMP support status
- SNMP community strings
- Trap timer value
- Trap destinations

### *To display SNMP configuration information:*

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

### *Example*

The following command displays the SNMP configuration information:

```
Sentry: show snmp<Enter>
SNMP Configuration
SNMP:                               Enabled
SET Community String:                private
GET Community String:                public
TRAP Community String:               trap
Error Trap Repeat Time (seconds):    180
Trap Destination 1:                  64.42.31.208
Trap Destination 2:                  (undefined)
```

## SNMP Traps

The Sentry supports three types of SNMP traps. Traps are enabled at the tower (T), infeed (I) or outlet (O) level.

### Trap Summary

Name	Level(s)	Description
Status	T, I, O	Operational status change
Change	O	Control status change
Load	I	Input load out of limit

All traps include the Location of the Sentry as defined with the Set Location command.

### Status trap

A Status trap is generated when an error condition occurs on a tower, infeed, Environmental Monitor or individual sensor. Status traps include the reported Status, the Location of the Sentry and identifier and name of the affected tower, infeed, outlet, environmental monitor or sensor.

Any error state generates a Status trap and triggers the trap timer. A new trap is generated at the end of every timer period until the Status returns to a non-error status. All status traps are enabled by default.

### Tower Status traps

Status	Error	Description
Normal		Tower is working correctly
NoComm	x	Communication to the tower has been lost

### Infeed Status traps

Status	Error	Description
On		Infeed is on
OffError	x	Infeed should be on but no current is sensed at the infeed
NoComm	x	Communication to the infeed has been lost

### Outlet Status traps

Status	Error	Description
On		Outlet is on
Off		Outlet is off
OnWait		Outlet Status in transition
OffWait		Outlet Status in transition
OnError	x	Outlet should be off but current is sensed at the outlet
OffError	x	Outlet should be on but no current is sensed at the outlet
OffFuse	x	Outlet should be on but a blown fuse has been detected
NoComm	x	Communication to the outlet has been lost

**NOTE:** Traps are generated according to a hierarchical architecture; i.e. if a Tower Status enters a trap condition, only the Tower Status trap is generated. Infeed and Outlet Status traps are suppressed until the Tower Status returns to Normal.

### Change trap

The Change trap is generated for all outlet status changes between any on/off conditions. Change traps include the outlet status, Location of the Sentry, and identifier and name of the affected outlet. For descriptions of the outlet status types, please refer to the prior table.

## Load Trap

The Load trap is generated whenever the total input load on an infeed exceeds a preset threshold. Load traps include the reported input load, load status, Location of the Sentry, and identifier and name of the affected infeed.

Any error state generates a Load trap and triggers the trap timer. A new trap is generated at the end of every timer period until the Load returns to a non-error status.

### **Load traps**

Status	Error	Description
Normal		Infeed is on and within preset thresholds
NotOn		Infeed is off
Reading		Non-error state – Load status currently being read
LoadHigh	x	Infeed current load exceeds preset threshold
OverLoad	x	Infeed current load exceeds the measurable range for the infeed
ReadError	x	Unable to read Load status
NoComm	x	Communication to the infeed has been lost

## Configuring Traps

### **SNMP Trap Command Summary**

Command	Description
Set Trap Tower Status	Enables or disables the Tower Status trap
Set Trap Infeed Status	Enables or disables the Infeed Status trap off
Set Trap Infeed Load	Enables or disables the Infeed Load trap
Set Trap Infeed HighThresh	Sets the Infeed Load trap high limit
Set Trap Outlet Change	Enables or disables the Outlet Change trap
Set Trap Outlet Status	Enables or disables the Outlet Status trap
Show Traps	Displays trap configurations

### **Enabling or Disabling a Status trap**

The Set Trap ... Status command is used to enable or disable Status traps for a Tower, Infeed or Outlet.

#### ***To Enable or Disable a Status trap:***

At the Sentry: prompt, type **set trap (tower, infeed, or outlet) status**, followed by the tower, infeed or outlet name, and **on** or **off**. Press **Enter**, or

Type **set trap (tower, infeed, or outlet) status all**, followed by **on** or **off** and press **Enter**.

#### **Examples**

The following command enables the Status trap for the first tower, using the tower's absolute name:

```
Sentry: set trap tower status .a on<Enter>
```

The following command enables the Status trap for the tower named Florida\_HQ\_1:

```
Sentry: set trap tower status Florida_HQ_1 on<Enter>
```

**NOTE:** Enabling lower hierarchical traps automatically enables traps of higher hierarchical value: i.e. enabling an Outlet Status trap automatically enables the Infeed and Tower Status traps for that outlet. Conversely, if a Tower Status trap is disabled, all associated Infeed Status & Load and Outlet Status traps will be disabled.

## Enabling or Disabling a Load trap

The Set Trap Infeed Load command is used to enable or disable an Infeed Load trap.

### *To Enable or Disable a Load trap:*

At the Sentry: prompt, type **set trap infeed load**, followed by the infeed name, and **on** or **off**. Press **Enter**, or

Type **set trap infeed load all**, followed by **on** or **off** and press **Enter**.

### **Examples**

The following command enables the Load trap for second infeed on the first tower, using the infeed's absolute name:

```
Sentry: set trap infeed load .AB on<Enter>
```

The following command disables the Load trap for all infeeds:

```
Sentry: set trap infeed load all off<Enter>
```

---

**NOTE:** Enabling lower hierarchical traps automatically enables traps of higher hierarchical value: i.e. enabling an Infeed Load trap automatically enables the Infeed and Tower Status traps for that infeed.

---

## Setting the Infeed Load limit

The Set Trap Infeed Loadhigh command is used to set the upper load limits for an input feed.

### *To set the infeed load limit:*

At the Sentry: prompt, type **set trap infeed loadhigh**, followed by the infeed name, and a value from 0 to 255 in amperes. Press **Enter**.

### **Example**

The following command sets the infeed load limit for the second infeed on the first tower to 25 amperes, using the infeed's absolute name:

```
Sentry: set trap infeed loadhigh .ab 25<Enter>
```

## Enabling or Disabling a Change trap

The Set Trap Outlet Change command is used to enable or disable an Outlet Change trap.

### *To Enable or Disable a Change trap:*

At the Sentry: prompt, type **set trap outlet change**, followed by the outlet name and **on** or **off**. Press **Enter**, or

Type **set trap outlet change all**, followed by **on** or **off** and press **Enter**.

### **Example**

The following command enables the Change trap for the third outlet on the first infeed of the second tower, using the outlet's absolute name:

```
Sentry: set trap outlet change .ba3 on<Enter>
```

## Displaying trap configuration information

The Show Traps command displays information about all traps.

### *To display trap information:*

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

### **Example**

The following command requests trap configuration information:

```
Sentry: show traps <Enter>
Tower trap configuration:
  Tower      Tower      Status
  ID         Name         Trap
  .A         Florida_HQ_1  ON
More (Y/es N/o): y
Input feed trap configuration:
  Input      Input      Status  Load  High
  Feed ID    Feed Name   Trap    Trap  Thresh
  .AA        HQ_1_Infeed_A  ON      ON    255 A
More (Y/es N/o): y
Outlet trap configuration:
  Outlet      Outlet      Change  Status
  ID          Name        Trap    Trap
  .AA1        DataServer_1  OFF    ON
  .AA2        WebServer_1   OFF    ON
  .AA3        FileServer_1  OFF    ON
  .AA4
```

## LDAP

The Sentry family of products supports Lightweight Directory Access Protocol (LDAP) Version 3. This support enables authentication with LDAP servers; user accounts do not need to be individually created locally on each Sentry device.

This allows administrators to pre-define and configure (in each Sentry product, and in the LDAP server) a set of necessary LDAP Groups, and access rights for each. User's access rights can then be assigned or revoked simply by making the user a member of one-or-more pre-defined Sentry LDAP Groups. User accounts can be added, deleted, or changed in the LDAP server without any changes needed on individual Sentry products.

Sentry 5.3b LDAP support has been tested in the following environments:

- Microsoft Active Directory (MSAD)
- Novell eDirectory (eDir)
- OpenLDAP

### LDAP Command Summary

Command	Description
Set Authorder	Specifies the authentication order for each new session attempt
Set LDAP	Enables/disables LDAP support
Set LDAP HostIP	Sets the IP address of the Directory Services server
Set LDAP Port	Sets the LDAP server port number
Set LDAP Bind	Specifies the LDAP bind request password type
Set LDAP BindDN	Specifies the user account Fully-Qualified Distinguished Name (FQDN) for binds
Set LDAP BindPW	Specifies the user account password for binds
Set LDAP GroupAttr	Specifies the user class distinguished name (DN) or names of groups a user is a member of
Set LDAP GroupType	Specifies the data type for the Set LDAP GroupAttr command
Set LDAP UserBaseDN	Sets the base distinguished name (DN) for the username search at login
Set LDAP UserFilter	Sets the filter used for the username search at login
Show LDAP	Displays LDAP configurations
Set DNS	Sets the IP address of the Domain Name server
Ping	Verifies proper DNS configuration by name resolution
Show Network	Displays network configuration information
Create LDAPGroup	Adds an LDAP group name
Remove LDAPGroup	Deletes an LDAP group name
Add GrouptoLDAP	Grants an LDAP group access to one or more groups
Add OutlettoLDAP	Grants an LDAP group access to one or all outlets
Add PorttoLDAP	Grants an LDAP group access to one or serial ports
Delete GroupfromLDAP	Removes access to one or more groups for an LDAP group
Delete OutlettoLDAP	Removes access to one or more outlets for an LDAP group
Delete PortfromLDAP	Removes access to one or more serial ports for an LDAP group
Set LDAPGroup Access	Sets the access level for an LDAP group
Set LDAPGroup Envmon	Grants or removes privileges to view input and environmental monitoring status
List LDAPGroup	Displays all accessible outlet/groups/ports for an LDAP group
List LDAPGroups	Displays privilege levels for all LDAP groups

## **Enabling and Setting up LDAP Support**

There are a few configuration requirements for properly enabling and setting up LDAP support. Below is an overview of the minimum requirements.

Directory Services server configuration requirements:

1. Define at least one LDAP group.
2. Assign users to that LDAP group.

Sentry configuration requirements:

1. Enable LDAP support.
2. Define the IP address and domain component of at least one Directory Services server.
3. Set the LDAP bind request method being utilized by the Directory Services server.
4. Define the IP address of at least one DNS server.
5. Test DNS server configuration using Sentry 'ping' support.
6. Define at least one LDAP group and assign access rights for that group.

---

**NOTE:** LDAP group names on the Directory Service server and the Sentry must match.

---

### **Enabling and disabling LDAP support**

The Set LDAP command is used to enable or disable LDAP support.

*To enable or disable LDAP support:*

At the Sentry: prompt, type **set ldap**, followed by **enabled** or **disabled** and press **Enter**.

### **Setting the LDAP host IP address**

The Set LDAP HostIP command sets the TCP/IP address of the Directory Services server.

*To set the LDAP host IP address:*

At the Sentry: prompt, type **set ldap**, followed by **hostip1** or **hostip2** and the Directory Services server's IP address. Press **Enter**.

#### **Example**

The following command sets the primary Directory Services server IP address to 98.76.54.32:

```
Sentry: set ldap hostip1 98.76.54.32<Enter>
```

### **Changing the LDAP server port**

The Set LDAP port command sets the port to which the Sentry sends LDAP requests to on the previously defined LDAP server. The default port is 389.

*To change the LDAP server port:*

At the Sentry: prompt, type **set ldap port**, followed by the port number and press **Enter**.

#### **Example**

The following command sets the LDAP server port number to 8888:

```
Sentry: set ldap port 8888<Enter>
```

### **Setting the LDAP bind password type**

The Set LDAP Bind command sets the password type used in the bind requests. The Sentry supports two LDAP bind methods – Simple and MD5.

The Simple method utilizes unencrypted delivery of a username-password over the network to the Active Directory server for authentication.

The MD5 digest method provides much stronger protection utilizing one-way encoded hash numbers, never placing the username-password on the network. For more information on MD5, see *Setting the HTTP authentication method*: on page 14.

---

**NOTE:** Windows 2000 is known only to support Simple binding. Windows 2003 supports both Simple and MD5 binding.

---

*To set the bind password type:*

At the Sentry: prompt, type **set ldap bind**, followed by **simple** or **md5** and press **Enter**.

## Setting the search bind Distinguished Name (DN)

The Set LDAP BindDN command is used to set the fully-qualified distinguished name (FQDN) for user accounts to bind with. This is required for directory services that do not support anonymous binds. This field is used ONLY with Simple Binds. Maximum string length is 124 characters.

---

**NOTE:** If left blank, then an anonymous bind will be attempted. This field is used ONLY with Simple binds.

---

### *To set the search bind DN:*

At the Sentry: prompt, type **set ldap binddn**, and press **Enter**. At the following prompt, type the FQDN and press **Enter**.

### **Example**

The following sets the FQDN for MSAD to 'cn=guest,cn=Users,dc=servertech,dc=com':

```
Sentry: set ldap binddn<Enter>
Enter Search Bind DN (Max characters 124):
cn=guest,cn=Users,dc=servertech,dc=com<Enter>
```

## Setting the search bind Distinguished Name (DN) password

The Set LDAP BindPW command is used to set the password for the user account specified in the Search Bind DN. Maximum password size is 20 characters.

### *To set the Bind Password DN:*

At the Sentry: prompt, type **set ldap bindpw** and press **Enter**. At the following prompt, type the bind password and press **Enter**.

## Setting the group membership attribute.

The Set LDAP GroupAttr command is used to specify the name of user class attributes that lists distinguished names (DN), or names of groups that a user is a member of. Maximum string length is 30 characters.

### *To set Group Membership Attribute:*

At the Sentry: prompt, type **set ldap groupattr** and press **Enter**. At the following prompt, type the group membership attribute and press **Enter**.

### **Example**

The following sets the group membership attribute for MSAD to 'memberof':

```
Sentry: set ldap groupattr<Enter>
Enter Group Member Attr (Max character 30):
memberof<Enter>
```

## Setting the group membership value type:

The Set LDAP GroupType command is used to specify whether the values of Group Membership Attribute represent the Distinguished Name (DN) of a group or just the name of the group.

### *To set group membership value type:*

At the Sentry: prompt, type **set ldap grouptype** followed by **DN** or **Name** and press **Enter**.

### **Example**

The following sets group membership value to DN

```
Sentry: set ldap grouptype DN<Enter>
```

## Setting the user search base Distinguished Name (DN)

The Set LDAP UserBaseDN command is used to set the base (DN) for the login username search. This is where the search will start, and will include all subtrees. Maximum size is 100 characters.

### *To set the user search base DN:*

At the Sentry: prompt, type **set ldap userbasedn** and press **Enter**. At the following prompt, type the search base DN and press **Enter**.

### **Example**

The following sets the DN user search base for MSAD to 'cn=Users,dc=servertech,dc=com':

```
Sentry: set ldap userbasedn<Enter>
Enter User Search Base DN (Max characters 100):
cn=Users,dc=servertech,dc=com<Enter>
```

## Setting the user search filter

The Set LDAP UserFilter command is used to set the search filter for the username entered at the login prompt.

The search filter must be entered within parenthesis and adhere to the following format:

(searchfilter=%s)

where 'searchfilter' is the name of the attribute in the user class which has a value that represents the user's login name. In this string, the '%s' will be replaced by the entered username. Maximum string length is 100 characters.

### *To set the user search filter:*

At the Sentry: prompt, type **set ldap userfilter** and press **Enter**. At the following prompt, type the User Search Filter and press **Enter**.

### **Example**

The following sets the user search filter for MSAD to 'samaccountname':

```
Sentry: set ldap userfilter<Enter>
Enter User Search Filter (Max characters 100):
(samaccountname=%s)<Enter>
```

## Setting the authentication order

The Set Authorder command sets the authentication order for remote authentication sessions. The Sentry supports two methods for authentication order - Remote -> Local and Remote Only.

The Remote -> Local method first attempts authentication with the Active Directory server and if unsuccessful with the local user database on the Sentry device.

The Remote Only method attempts authentication only with the Active Directory server and if unsuccessful, access is denied.

---

**NOTE:** With the Remote Only method, if authentication fails due to a communication failure with the Active Directory server automatic authentication fallback will occur to authenticate with the local user data base on the Sentry device.

---

### *To set the authentication order:*

At the Sentry: prompt, type **set authorder**, followed by **remotelocal** or **remoteonly** and press **Enter**.

---

**NOTE:** Server Technology recommends NOT setting the authentication order to Remote Only until the LDAP has been fully configured and tested.

---

## Displaying LDAP configuration information

The Show LDAP command displays LDAP configuration information.

- Enabled-disabled status of LDAP support
- Directory Services server IP address and port
- Bind request password type and remote authentication order
- Search bind distinguished name and password
- User search base distinguished name and filter
- Group membership attribute and type

### *To display the LDAP configuration information:*

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

### **Example**

The following command displays the LDAP configuration information:

```
Sentry: show ldap
LDAP Configuration
LDAP:          Enabled
Host IP1:      98.76.54.32
Host IP2:      0.0.0.0
Port:          8888
Bind Type:     MD5
Auth Order:    Remote->Local
Search Bind
  DN:          cd=guest,cn=Users,dc=servertech,dc=com
  Password:    OpenSesame
User Search
  Base DN:     cn=Users,dc=servertech,dc=com
  Filter:      (samaccountname=%s)
Group Membership
  Attribute:   memberof
  Value Type:  DN
```

## Setting the DNS IP address

The Set DNS command sets the TCP/IP address of the Domain Name server (DNS).

---

**NOTE:** LDAP requires the definition of at least one Domain Name server.

---

To display the DNS configuration information, use the Show Network command as described on page 39.

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

At the Sentry: prompt, type **set**, followed by **dns1** or **dns2** and the Domain Name server's IP address. Press **Enter**.

### **Example**

The following command sets the primary Domain Name server IP address to 98.76.54.254:

```
Sentry: set dns1 98.76.54.254<Enter>
```

## Verifying the DNS configuration

The Ping command may be used to verify the configuration of the DNS IP address.

### *To verify the DNS configuration:*

At the Sentry: prompt, type **ping**, followed by the domain component of the Directory Services server previously configured and press **Enter**.

### **Example**

The following command verifies the DNS configuration:

```
Sentry: ping servertech.com
Pinging servertech.com [98.76.54.32] with 64 bytes of data:
Reply from 98.76.54.32: bytes=64 pseq=0 triptime=0
Reply from 98.76.54.32: bytes=64 pseq=1 triptime=0
Reply from 98.76.54.32: bytes=64 pseq=2 triptime=0
Reply from 98.76.54.32: bytes=64 pseq=3 triptime=0
Reply from 98.76.54.32: bytes=64 pseq=4 triptime=0
```

## **Configuring LDAP Groups**

### **Creating an LDAP group**

The Create LDAPGroup command creates an LDAP group.

#### ***To create an LDAP group:***

At the Sentry: prompt, type **create ldapgroup**, optionally followed by a 1-16 character group name (Spaces are not allowed, and LDAP group names are not case sensitive). Press **Enter**.

#### ***Example***

The following command creates the LDAP group PowerUser:

```
Sentry: create ldapgroup PowerUser<Enter>
```

### **Removing an LDAP group**

The Remove LDAPGroup command removes an LDAP group.

#### ***To remove an LDAP group:***

At the Sentry: prompt, type **remove ldapgroup**, optionally followed by a group name. Press **Enter**.

### **Setting LDAP group access level privileges**

The Set LDAPGroup Access command sets the access level privileges for an LDAP group. The Sentry has four defined access privilege levels; Admin, User, On-Only and View-Only. For more information on user access levels, see *Changing a user's access privilege level:* on page 17.

#### ***To set the access level privilege for an LDAP group :***

At the Sentry: prompt, type **set ldapgroup access**, followed by **admin**, **user**, **ononly** or **viewonly**, optionally followed by a LDAP group name and press **Enter**.

#### ***Examples***

The following command sets the LDAP group access level for LDAPAdmin to Admin:

```
Sentry: set ldapgroup access admin ldapadmin<Enter>
```

The following command sets the LDAP group access level for PowerUser to User:

```
Sentry: set ldapgroup access user poweruser<Enter>
```

### **Granting and removing input status viewing privileges**

The Set LDAPGroup Envmon command grants or removes input status viewing privileges to/from an LDAP group.

#### ***To grant or remove input status viewing privileges for an LDAP group:***

At the Sentry: prompt, type **set ldapgroup envmon** followed by **on** or **off**, optionally followed by a group name and press **Enter**.

#### ***Example***

The following command grants input status viewing privileges to the LDAP group PowerUser:

```
Sentry: set ldapgroup envmon on poweruser<Enter>
```

## Displaying the LDAP access privilege levels

The List LDAPGroups command displays all defined LDAP group with their access privilege level.

### *To display LDAP group access privilege levels:*

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

### **Example**

The following command displays all LDAP groups with their access privilege level:

```
Sentry: list ldapgroups<Enter>
LDAP          Access      Environmental
Group Name    Level          Monitoring
LDAPAdmin     Admin          Allowed
PowerUser     User           Allowed
User          On-Only        Not Allowed
Guest         View-Only      Not Allowed
```

## Adding outlet access to an LDAP group

The Add OutletToLDAP command grants an LDAP group access to one or all outlets. To grant access for more than one outlet, but not all outlets, you must use multiple Add OutletToLDAP commands.

### *To grant outlet access to an LDAP group:*

At the Sentry: prompt, type **add outlettoldap**, optionally followed by an outlet name and a group name. Press **Enter**, or

Type **add outlettoldap all**, followed by a group name and press **Enter**.

### **Examples**

The following commands grant the LDAP group PowerUser access to outlets A1 and Webserver\_1:

```
Sentry:add outlettoldap .a1 poweruser<Enter>
Sentry:add outlettoldap WebServer_1 poweruser<Enter>
```

## Deleting outlet access for an LDAP group

The Delete OutletFromLDAP command removes an LDAP group's access to one or all outlets. You cannot remove access to any outlet for an administrative level group.

### *To delete outlet access for an LDAP group:*

At the Sentry: prompt, type **delete outletfromldap**, optionally followed by an outlet name and a group name. Press **Enter**, or

Type **delete outletfromldap all**, followed by a group name and press **Enter**.

## Adding outlet group access to an LDAP group

The Add GroupToLDAP command grants an LDAP group access to a outlet group. To grant access for more than one outlet group, you must use multiple Add GroupToLDAP commands.

### *To gran toutlet group access to an LDAP Group:*

At the Sentry: prompt, type **add grouptoldap**, optionally followed by an outlet group name and an LDAP group name. Press **Enter**.

### **Examples**

The following commands grants to LDAP group PowerUser access to the outlet groups ServerGroup\_1 and ServerGroup\_2:

```
Sentry:add grouptoldap servergroup_1 poweruser<Enter>
Sentry:add grouptoldap servergroup_2 poweruser<Enter>
```

## Deleting outlet group access for an LDAP group

The Delete GroupFromLDAP command removes an LDAP group's access to a outlet group. You cannot remove access to any group for an administrative level group.

### *To delete outlet group access for an LDAP group:*

At the Sentry: prompt, type **delete groupfromldap**, optionally followed by a outlet group name and an LDAP group name. Press **Enter**.

## Adding serial port access to an LDAP group

The Add PortToLDAP command grants an LDAP group access to the serial port.

### *To grant serial port access to an LDAP group:*

At the Sentry: prompt, type **add porttoldap console** and a group name. Press **Enter**.

## Deleting serial port access for an LDAP group

The Delete PortFromLDAP command removes an LDAP group's access to the serial port. You cannot remove access to the serial port for an administrative level group.

### *To delete serial port access for a user:*

At the Sentry: prompt, type **delete portfromldap console** and a group name. Press **Enter**.

## Displaying outlet, outlet group and serial port access

The List LDAPGroup command displays all accessible outlets, outlet groups and serial ports for an LDAP group.

### *To display outlet, outlet group and serial port access:*

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

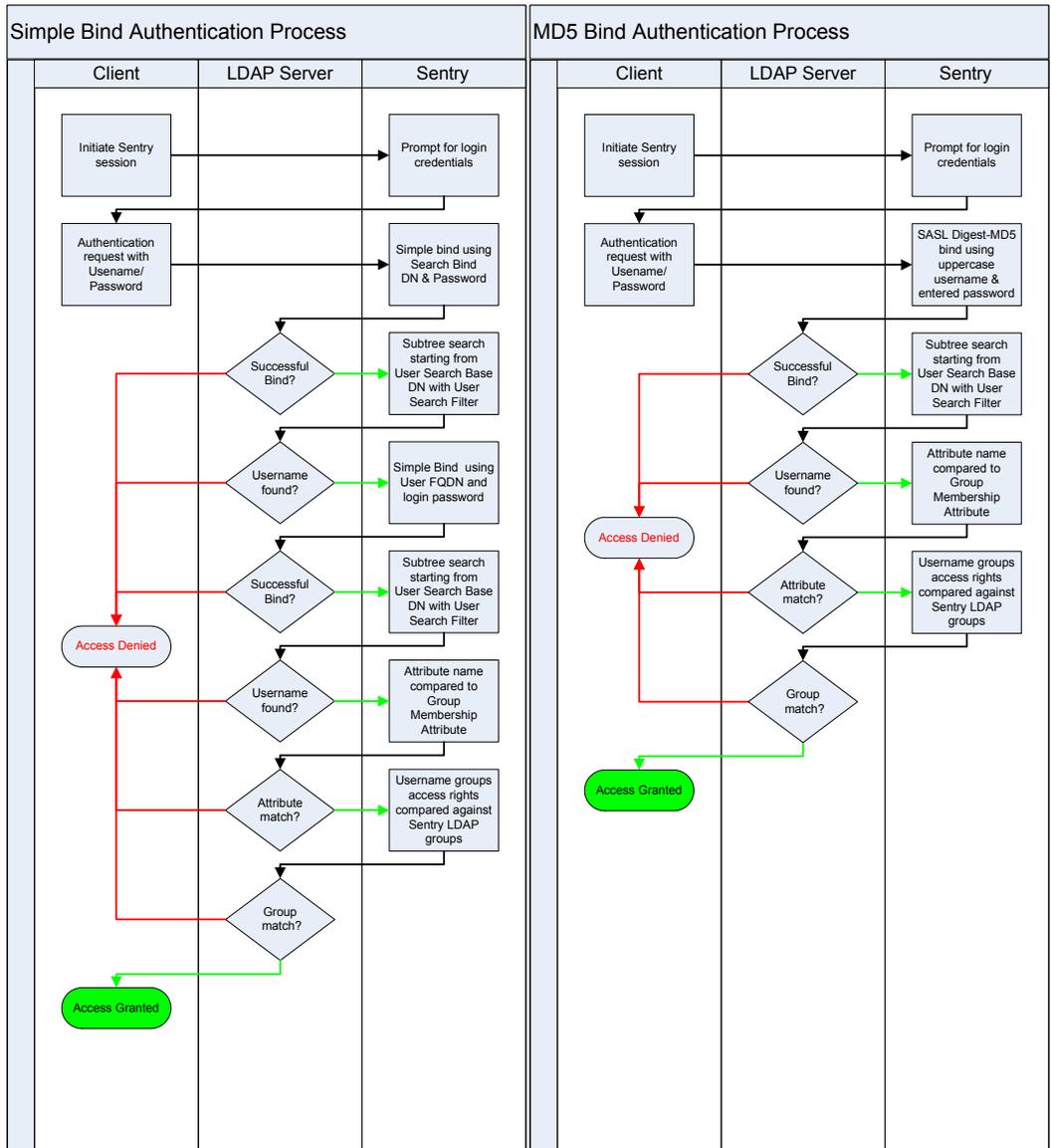
### **Example**

The following command displays information about the LDAP group PowerUser:

```
Sentry: list ldapgroup poweruser<Enter>
Username: PowerUser
  Outlet  Outlet
  ID      Name
  .A1     DataServer_1
  .A2     WebServer_1
Groups:
  ServerGroup_1
  ServerGroup_2
More (Y/es N/o): Y
Ports:
  Port      Port
  ID        Name
  Console   Console
```

Members of the PowerUser LDAP group may access the following outlets, outlet groups and serial ports: outlet A1 which has a descriptive name of DataServer\_1, outlet A2 which has a descriptive name of WebServer\_1, group ServerGroup\_1 group ServerGroup\_2 and Console serial port.

# LDAP Technical Specifications



## TACACS+

The Sentry family of products supports the Terminal Access Controller Access Control System (TACACS+) protocol. This enables authentication and authorization with a central TACACS+ server; user accounts do not need to be individually created locally on each Sentry device.

This allows administrators to pre-define and configure (in each Sentry product, and in the TACACS+ server) a set of necessary TACACS+ privilege levels, and users access rights for each. User's access rights can then be assigned or revoked simply by making the user a member of one-or-more pre-defined Sentry TACACS+ privilege levels. User account rights can be added, deleted, or changed within TACACS+ without any changes needed on individual Sentry products.

The Sentry supports 16 different TACACS+ privilege levels; 15 are entirely configurable by the system administrator (1 is reserved for default Admin level access to all Sentry resources).

### TACACS+ Command Summary

Command	Description
Set Authorder	Specifies the authentication order for each new session attempt
Set TACACS	Enables/disables SSL support
Set TACACS HostIP	Sets the IP address of the TACACS server
Set TACACS Key	Sets the TACACS encryption key
Show TACACS	Displays TACACS configurations
Add GrouptoTACACS	Grants a TACACS account access to one or more groups
Add OutlettoTACACS	Grants a TACACS account access to one or all outlets
Add PorttoTACACS	Grants a TACACS account access to one or serial ports
Delete GroupfromTACACS	Removes access to one or more groups for a TACACS account
Delete OutlettoTACACS	Removes access to one or more outlets for a TACACS account
Delete PortfromTACACS	Removes access to one or more serial ports for a TACACS account
Set TacPriv Access	Sets the access level for a TACACS account
Set TacPriv Envmon	Grants or removes privileges to view input and environmental monitoring status
List TacPrivs	Displays access levels for all TACACS accounts
List TacPriv	Displays all accessible outlet/groups/ports for a TACACS account

### Enabling and Setting up TACACS+ Support

There are a few configuration requirements for properly enabling and setting up TACACS+ support. Below is an overview of the minimum requirements:

1. Enable TACACS+ support.
2. Define the IP address and domain component of at least one TACACS+server.
3. Set the TACACS+ key configured on the supporting TACACS+server.

### Enabling and disabling TACACS+ support

The Set TACACS command is used to enable or disable TACACS+ support.

*To enable or disable TACACS+ support:*

At the Sentry: prompt, type **set tacacs**, followed by **enabled** or **disabled** and press **Enter**.

### Setting the TACACS+ server IP address

The Set TACACS HostIP command sets the TCP/IP address of the TACACS+ server.

*To set the TACACS+ server IP address:*

At the Sentry: prompt, type **set tacacs**, followed by **hostip1** or **hostip2** and the TACACS+ server's IP address. Press **Enter**.

### Example

The following command sets the primary TACACS+ server IP address to 98.76.54.32:

```
Sentry: set tacacs hostip1 98.76.54.32<Enter>
```

## Setting the TACACS+ encryption key

The Set TACACS Key command sets the encryption key used to encrypt all data packets between the Sentry and the TACACS+ server. This key must match the key configured on the TACACS+ server.

### *To set the encryption key:*

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

At the TACACS+ Key: prompt, type a key of up to 60 alphanumeric and other typeable characters (ASCII 32 to 126 decimal). Keys are case sensitive. Press **Enter**. To specify no password, press **Enter** at the prompt.

At the Verify TACACS+ Key: prompt, retype the key. Press **Enter**. To verify no password, press **Enter** at the prompt.

### **Example**

```
Sentry: set tacacs key<Enter>
TACACS+ Key: <Enter>
Verify TACACS+ Key: <Enter>
```

For security, key characters are not displayed.

---

**NOTE:** A key size of zero results in no encryption being applied which may not be supported by the TACACS+ server and is not recommended for a production environment.

---

## Setting the authentication order

The Set Authorder command sets the authentication order for remote authentication sessions. The Sentry supports two methods for authentication order - Remote -> Local and Remote Only.

The Remote -> Local method first attempts authentication with the TACACS+ server and if unsuccessful with the local user database on the Sentry device.

The Remote Only method attempts authentication only with the TACACS+ server and if unsuccessful, access is denied.

---

**NOTE:** With the Remote Only method, if authentication fails due to a communication failure with the TACACS+ server automatic authentication fallback will occur to authenticate with the local user data base on the Sentry device.

---

### *To set the authentication order:*

At the Sentry: prompt, type **set authorder**, followed by **remotelocal** or **remoteonly** and press **Enter**.

---

**NOTE:** Server Technology recommends NOT setting the authentication order to Remote Only until the TACACS+ has been fully configured and tested.

---

## Displaying TACACS+ configuration information

The Show TACACS command displays TACACS+ configuration information.

- Remote authentication order
- Enabled-disabled status of LDAP support
- Directory Services server IP address and domain components
- Bind request password type

### *To display the LDAP configuration information:*

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

### **Example**

The following command displays the LDAP configuration information:

```
TACACS+ Configuration
TACACS+:      Disabled
Host IP1:     98.76.54.32
Host IP2:     0.0.0.0
TACACS+ Key:  (Set)
Auth Order:  Remote->Local
```

## Configuring TACACS+ Privilege Levels

### Setting TACACS+ account access level privileges

The Set TacPriv Access command sets the access level privileges for a TACACS+ account. The Sentry has four defined access privilege levels; Admin, User, On-Only and View-Only. For more information on user access levels, see *Changing a user's access privilege level:* on page 17.

#### *To set the access level privilege for a TACACS+ account :*

At the Sentry: prompt, type **set tacpriv access**, followed by **admin**, **user**, **ononly** or **viewonly**, optionally followed by a TACACS+ account number and press **Enter**.

#### **Examples**

The following command sets the TACACS+ account access level for account 14 to Admin:

```
Sentry: set tacpriv access admin 14<Enter>
```

The following command sets the TACACS+ account access level for account 5 to User:

```
Sentry: set tacpriv access user 5<Enter>
```

### Granting and removing input status viewing privileges

The Set TacPriv Envmon command grants or removes input status viewing privileges to/from a TACACS+ account.

#### *To grant or remove input status viewing privileges for a TACACS+ account:*

At the Sentry: prompt, type **set tacpriv envmon**, followed by **on** or **off**, optionally followed by a TACACS+ account number and press **Enter**.

#### **Example**

The following command grants input status viewing privileges to the TACACS+ account 5:

```
Sentry: set tacpriv envmon on 5<Enter>
```

### Displaying the TACACS+ access privilege levels

The List TacPrivs command displays all TACACS+ accounts with their access privilege levels.

#### *To display TACACS+ account access privilege levels:*

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

#### **Example**

The following command displays all TACACS+ account with their access privilege level:

```
Sentry: list tacprivs<Enter>
TACACS          Access      Environmental
Account Name   Level       Monitoring
TACAdmin        Admin       Allowed
PowerUser       User        Allowed
User            On-Only     Not Allowed
Guest           View-Only   Not Allowed
```

### Adding outlet access to a TACACS+ account

The Add OutletToTACACS command grants a TACACS+ account access to one or all outlets. To grant access for more than one outlet, but not all outlets, you must use multiple Add OutletToTACACS commands.

#### *To grant outlet access to a TACACS+ account:*

At the Sentry: prompt, type **add outlettotacacs**, optionally followed by an outlet name and a TACACS+ account number. Press **Enter**, or

Type **add outlettotacacs all**, followed by a TACACS+ account number and press **Enter**.

#### **Examples**

The following commands grant the a TACACS+ account 5 access to outlets A1 and Webserver\_1:

```
Sentry:add outlettotacacs .a1 5<Enter>
Sentry:add outlettotacacs WebServer_1 5<Enter>
```

## Deleting outlet access for a TACACS+ account

The Delete OutletFromTACACS command removes a TACACS+ account's access to one or all outlets. You cannot remove access to any outlet for an administrative level account.

### *To delete outlet access for a TACACS+ account:*

At the Sentry: prompt, type **delete outletfromtacacs**, optionally followed by an outlet name and a TACACS+ account number. Press **Enter**, or

Type **delete outletfromtacacs all**, followed by a TACACS+ account number and press **Enter**.

## Adding outlet group access to a TACACS+ account

The Add GroupToTACACS command grants a TACACS+ account access to an outlet group. To grant access for more than one outlet group, you must use multiple Add GroupToTACACS commands.

### *To grant outlet group access to a TACACS+ account:*

At the Sentry: prompt, type **add grouptotacacs**, optionally followed by an outlet group name and a TACACS+ account number. Press **Enter**.

### **Examples**

The following commands grants to a TACACS+ account number 5 access to the outlet groups ServerGroup\_1 and ServerGroup\_2:

```
Sentry:add grouptotacacs servergroup_1 5<Enter>
Sentry:add grouptotacacs servergroup_2 5<Enter>
```

## Deleting outlet group access for a TACACS+ account

The Delete GroupFromTACACS command removes a TACACS+ account's access to an outlet group. You cannot remove access to any group for an administrative level account.

### *To delete outlet group access for a TACACS+ account:*

At the Sentry: prompt, type **delete groupfromtacacs**, optionally followed by a outlet group name and a TACACS+ account number. Press **Enter**.

## Adding serial port access to a TACACS+ account

The Add PortToTACACS command grants a TACACS+ account access to the serial port.

### *To grant serial port access to a TACACS+ account:*

At the Sentry: prompt, type **add porttotacacs console** and a TACACS+ account number. Press **Enter**.

## Deleting serial port access for a TACACS+ account

The Delete PortFromTACACS command removes a TACACS+ account's access to the serial port. You cannot remove access to the serial port for an administrative level account.

### *To delete serial port access for a TACACS+ account:*

At the Sentry: prompt, type **delete portfromtacacs console** and a TACACS+ account number. Press **Enter**.

## Displaying outlet, outlet group and serial port access

The List TacPriv command displays all accessible outlets, outlet groups and serial ports for a TACACS+ account.

### *To display outlet, outlet group and serial port access:*

At the Sentry: prompt, type **list tacpriv**, optionally followed by a TACACS+ account. Press **Enter**.

### **Example**

The following command displays information about the TACACS+ account 1:

```
Sentry: list tacpriv 1<Enter>
TACACS+ Privilege Level: 1
Ports:
  Port ID   Port Name
  Console   Console
```

Members of PowerUser TACACS+ account members may access the Console serial port.

## **TACACS+ Technical Specifications**

Authentication START Packet includes:

```
action = 1 (TAC_PLUS_AUTHEN_LOGIN)
priv_lvl = 0 (TAC_PLUS_PRIV_LVL_MIN)
authen_type = 1 (TAC_PLUS_AUTHEN_TYPE_ASCII)
service = 1 (TAC_PLUS_AUTHEN_SVC_LOGIN)
user = (entered username)
port = (access path into the Sentry)
rem_addr = 'Sentry3_XXXXXX' (XXXXXX is last six digits of MAC address)
data = "" (null)
```

---

**NOTE:** The password is sent in a CONTINUE packet.

---

Authorization REQUEST Packet includes:

```
authen_method = 6 (TAC_PLUS_AUTHEN_METH_TACACSPLUS)
priv_lvl = 0 (TAC_PLUS_PRIV_LVL_MIN)
authen_type = 1 (TAC_PLUS_AUTHEN_TYPE_ASCII)
authen_service = 1 (TAC_PLUS_AUTHEN_SVC_LOGIN)
user = (entered username)
port = (access path into the Sentry)
rem_addr = 'Sentry3_XXXXXX' (XXXXXX is last six digits of Ethernet MAC address)
service = 'shell' (for exec)
cmd = "" (null)
```

---

**NOTE:** The access paths into the Sentry which support TACACS+ are 'Console', 'Telnet', 'SSH', 'HTTP' and 'HTTPS'. In the case of 'Console' and 'Modem', an administrator is allowed to rename these ports in which case the assigned name is used.

---

## Chapter 5: Appendices

### Appendix A: Resetting to Factory Defaults

You may reset the non-volatile RAM that stores all configurable options. This clears all administrator-editable fields and resets all command line configurable options to their default values, including all user accounts.

You may reset the unit to factory defaults from the command line or the HTML interface, or by pressing the reset button. You must have administrator-level privileges to issue the command. Using the reset button may be necessary when a forgotten password prevents administrator login. Each of the methods updates the current working configuration to the factory defaults.

---

**NOTE:** Resetting the unit resets all TCP/IP and Telnet/Web configurations. Reconfiguring the TCP/IP and Telnet/web settings will be required.

---

#### **To reset to factory defaults from the HTML interface**

On the Restart page in the Tools section of the HTML interface, select **Restart and reset to factory defaults** from the drop-down menu and press **Apply**.

#### **To reset to factory defaults from the command line**

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

#### **To reset to factory defaults using the reset button**

Locate the recessed reset button directly beside the Serial & Ethernet ports. You will need a non-conductive, non-metallic tool that fits inside the recess.

Insert the tool in the recess, then depress and hold the reset button for at least ten seconds.

---

**NOTE:** If the reset button is depressed and held for more than 15 seconds, the reset will abort.

---

### Appendix B: Uploading Firmware

You may upload new versions of firmware using File Transfer Protocol (FTP). This allows access to new firmware releases for firmware improvements and new features additions.

---

**NOTE:** To begin an FTP upload session, you must first configure the FTP Host address, username/password, filename and filepath. For information on configuring the FTP settings required for firmware upload see Chapter 3: Operations.

---

You may initiate an FTP upload session by issuing a command or from the HTML interface. You must have administrator-level privileges to initiate an upload.

#### **To initiate an FTP upload session from the HTML interface**

On the Restart page in the Tools section of the HTML interface, select **Restart and upload firmware via FTP** from the drop-down menu and press **Apply**.

Upon issuing this command the unit will restart and upload the firmware file specified with the FTP Filename command from the previously configured FTP Host. See *FTP Administration* in Chapter 3: for more information.

#### **To initiate an FTP upload session from the command line**

The Restart FTPLoad command initiates an upload of firmware. Upon issuing this command the unit will restart and upload the firmware file specified with the FTP Filename command from the previously configured FTP Host. See *FTP Administration* in Chapter 3: for more information.

To initiate an FTP firmware upload session:

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

## Appendix C: Technical Specifications

### Domestic Models

Model	Voltage	Inlet*	Outlets	Additional Ports
PT40-H404-1-02	100-120V, 50/60Hz	IEC 60320 C20	4 NEMA 5-20R	4 Pass-Thru
PT40-H404-2-02	208-240V, 60Hz	IEC 60320 C20	4 IEC 60320 C13	4 Pass-Thru

### International Models

Model	Voltage	Inlet*	Outlets	Additional Ports
PT40-H404-2-02	230V, 50/60Hz	IEC 60320 C20	4 IEC 60320 C13	4 Pass-Thru

\* Input cordset selected at time of purchase. (Contact your account representative for more information).

### Power Ratings

Model <i>Modele</i> Modell	Input Current Ratings <sub>1</sub> <i>L'indice du courant d'entrée</i> Eingangsstromstärke		Output Current Ratings <i>L'indice du courant de sortie</i> Ausgangsstromstärke			Total <i>Total</i> Insgesamt
	Voltage <i>Tension</i> Spannung	Current <i>Courant</i> Strom	Voltage <i>Tension</i> Spannung	Outlet <i>Prise</i> Anschlussstelle		
PT40-H404-1-02	100-120V 50/60Hz	16	100-120V 50/60Hz	16		16
PT40-H404-2-02	208-240V 60Hz	16	208-240V 60Hz	12		16
	230V 50/60Hz	16	230V 50/60Hz	10		16

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

### Physical Specifications

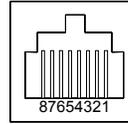
	Operating	Storage
<b>Temperature</b>	32° to 122° F (0° to 50° C)	-40° to 185° F (-40° to 85° C)
<b>Elevation</b> (above MSL)	0 to 10,000 ft (0 to 3000m)	0 to 50,000 ft (0 to 15000m)
<b>Relative Humidity</b>	10 to 90%, non-condensing	10 to 90%, non-condensing
	Dimensions (H x W x D)	Weight
PT40-H404	1.75 x 17.0 x 7.0 in. (45 x 432 x 178 mm)	8.2 lbs (3.7 kg)

## Data Connections

### RS-232 port

Commanders are equipped standard with an RJ45 DTE RS-232c serial port. This connector may be used for direct local access or from other serial devices such as a terminal server. An RJ45 crossover cable is provided for connection to an RJ45 DCE serial port.

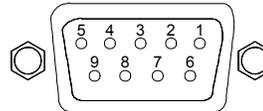
Pin	DTE Signal Name		Input/Output
1	Request to Send	RTS	Output
2	Data Terminal Ready	DTR	Output
3	Transmit Data	TD	Output
4	Signal Ground		
5	Signal Ground		
6	Receive Data	RD	Input
7	Data Set Ready	DSR	Input
8	Clear to Send	CTS	Input



### RJ45 to DB9F serial port adapter

Additionally, an RJ45 to DB9F serial port adapter is provided for use in conjunction with the RJ45 crossover cable to connect to a PC DB9M DCE serial port. The adapter pinouts below reflect use of the adapter with the provided RJ45 crossover cable.

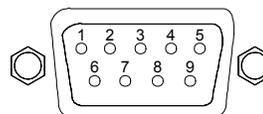
Pin	DCE Signal Name		Input/Output
1			
2	Receive Data	RD	Output
3	Transmit Data	TD	Input
4	Data Terminal Ready	DTR	Input
5	Signal Ground		
6	Data Set Ready	DSR	Output
7	Request to Send	RTS	Input
8	Clear to Send	CTS	Output



### Modem Port

Commanders are equipped standard 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 Commanders 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



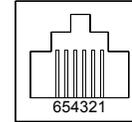
**NOTE:** To connect to a PC serial port, a null-modem adapter and a female-to-female gender changer are required in addition to the included cable.

## Pass-Thru Port

The Commander be may be equipped with up to eight RJ12 DTE Pass-Thru 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.

For information on additional available adapters for non-standard applications, please review the Technical Note - *Data & ShutDown Adapters, Cables & Kits* on the Server Technology website.

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		



## LED Indicators

Units 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.

## **Regulatory Compliance**

### **Product Safety**

Units have been safety tested and certified to the following standards:

- USA/Canada UL 60950:2003 and CAN/CSA 22.2 No. 60950-1-03
- European Union EN60950-1:2001

This product is also designed for Norwegian IT power system with phase-to phase voltage 230V.

### **USA Notification**

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.

Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC rules.

### **Canadian Notification**

This Class A digital apparatus complies meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

### **European Union Notification**

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms:

- EN55022 Electromagnetic Interference
- EN55024 Electromagnetic Immunity
- EN60950-1 Product Safety
- EN61000-3 Harmonics and Flicker

### **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 ( V C C I ) 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。

## **Recycling**



Server Technology Inc. encourages the recycling of its products. Disposal facilities, environmental conditions and regulations vary across local, state and country jurisdictions, so Server Technology encourages consultation with qualified professional and applicable regulations and authorities within your region to ensure proper disposal.

### **Waste Electrical and Electronic Equipment (WEEE)**



In the European Union, this label indicates that this product should not be disposed of with household waste. It should be deposited at an appropriate facility to enable recovery and recycling.

For information on how to recycle this product responsibly in your country, please visit: [www.servertech.com/support/recycling](http://www.servertech.com/support/recycling).

## Appendix D: 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 IF 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.

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/support](http://www.servertech.com/support)

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 firmware

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.





**Solutions for the Data Center Equipment Cabinet**

Server Technology, Inc.  
1040 Sandhill Drive  
Reno, NV 89521

**+1.800.835.1515 TF**  
+1.775.284.2000 Tel  
+1.775.284.2065 Fax

[www.servertech.com](http://www.servertech.com)  
[sales@servertech.com](mailto:sales@servertech.com)

Sentry, Commander, Environmental Monitoring Control Unit, Pass-Thru and Post-On are trademarks of Server Technology, Inc.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Server Technology, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

301-0402-1 Rev. E (081305) © 2004-2005 Server Technology, Inc. All rights reserved.