Switched Cabinet Distribution Unit

Installation and Operations Manual

- CWG/CXG-16Vx
- CWG/CXG-24Vx
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.

Notices

301-0429-1 Rev. B (011711)
Copyright © 2009-2011 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. 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.

The Globe logo is a trademark of Server Technology, Inc., registered in the US. Use of the logos for commercial purposes without the prior written consent of Server Technology may constitute trademark infringement and unfair competition in violation of federal and state laws.

Server Technology, the Globe logo, Switched CDU and CDU are trademarks of Server Technology, Inc., registered in the US. Sentry, POPS and the POPS logo, Cabinet Distribution Unit, Environmental Monitor, Post-On and SMARTER Technical Support 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.

Please Recycle

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

## Chapter 1: Introduction
- Quick Start Guide ................................................................. 4
- Technical Support ...................................................................... 4
- Equipment Overview ............................................................ 5

## Chapter 2: Installation
- Standard Accessories ......................................................... 6
- Optional Accessories .......................................................... 6
- Additional Required Items ................................................... 6
- Safety Precautions ............................................................... 7
- Installing the Power Input Retention Bracket ....................... 8
- Mounting ................................................................................ 8
- Attaching the Expansion Module ......................................... 9
- Connecting to the Power Source ........................................... 9
- Connecting Devices ............................................................. 9
- Connecting the Sensors ......................................................... 9
- Connecting to the Unit .......................................................... 9

## Chapter 3: Operations
- Interfaces .............................................................................. 13
- Web Interface ....................................................................... 14
- Command Line Interface ..................................................... 33

## Chapter 4: Advanced Operations
- SSL ..................................................................................... 68
- SSH ...................................................................................... 69
- SNMP/Thresholds ............................................................... 71
- LDAP .................................................................................... 80
- TACACS+ .............................................................................. 90
- RADIUS ............................................................................... 96
- Logging ............................................................................... 100
- Upload/Download ............................................................... 104
- Remote Shutdown ............................................................ 106

## Chapter 5: Appendices
- Appendix A: Resetting to Factory Defaults ......................... 110
- Appendix B: Uploading Firmware ........................................ 110
- Appendix C: Technical Specifications ................................. 111
- Appendix D: Warranty, Product Registration and Support .... 116
Chapter 1: Introduction

Quick Start Guide

The following instructions will help you quickly install and configure your POPS Switched CDU 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 POPS Switched CDU ................................................................. 7
2. Connect to the power source ........................................................................ 8
3. Connect the devices ....................................................................................... 9
4. Connect the sensors ....................................................................................... 9
5. Connect to the POPS Switched CDU .............................................................. 9
6. Configure the POPS Switched CDU ............................................................... 11
   - Login as the predefined Administrator (admn/admn) ........................................... 13
   - Configure the network settings ........................................................................ 19
   - Create new administrative user account ............................................................. 20
   - Configure location and Switched CDU names .................................................... 17
   - Configure sensor names .................................................................................... 18
   - Configure new user account(s) ........................................................................ 20
   - Remove the predefined Administrator .............................................................. 23
7. Connect the POPS Switched CDU to the network.

Technical Support

Experience Server Technology's FREE SMARTER 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 a.m. to 5 p.m. PST, Monday through Friday. After-hours service is provided to ensure your requests are handled quickly no matter what time zone or country you are located in.

Server Technology, Inc.
1040 Sandhill Drive Tel: 775.284.2000 Web: www.servertech.com
Reno, Nevada 89521 USA Fax: 775.284.2065 Email: support@servertech.com
Equipment Overview

1. The power inlet/cord(s) connects the CDU to the electrical power source.
2. The Current LED(s) displays the current load for each infeed, branch or electrical phase per infeed.
3. Two RJ45 connectors for Serial (RS-232) and Ethernet connection.
4. Two mini RJ11 connectors for Temperature/Humidity sensors.

A number is printed above each outlet. These numbers may be used in commands that require an outlet name. See Outlet Naming and Grouping in Chapter 3: Operations for more information.

Figure 1. POPS Switched Cabinet Distribution Unit (CDU) Views
Chapter 2: Installation

Before installing your Sentry POPS Switched Cabinet Distribution Unit (CDU), 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 hardware:
  - *Vertical models* -
    - Two removable flanges with four M4 screws.
    - Two mounting L-brackets with nut plates, four sets of screws and washers.
    - Optional button mounts.

- Cables/Adapters:
  - *CWG models* -
    - RJ45 to RJ45 crossover cable.
    - RJ45 to DB9F serial port adapter (for connection to standard DB9M DTE serial port).
  - *CXG models* -
    - RJ12 to RJ12 crossover cable.

- Outlet retention clips (208-240V models).

**Optional Accessories**

- Temperature/Humidity sensors

**Additional Required Items**

- Flathead and Phillips screwdrivers
- Screws, washers and nuts to attach the CDU to your rack
### Safety Precautions

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

<table>
<thead>
<tr>
<th>English</th>
<th>French</th>
<th>German</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only for installation and use in a Restricted Access Location in accordance with the following installation and use instructions.</td>
<td>Seulement pour l'installation et l'utilisation dans une Zone Interdite conformément aux installations et l’utilisation des indications suivants.</td>
<td>Nur zur Installation und Verwendung in einem Sicherheitsbereich gemäß den folgenden Installations- und Verwendungsanleitungen.</td>
</tr>
<tr>
<td>This equipment is designed to be installed on a dedicated circuit.</td>
<td>Cet équipement est conçu à être installé sur un circuit spécialisé.</td>
<td>Diese Ausrüstung ist zur Installation in einem festen Stromkreis vorgesehen.</td>
</tr>
<tr>
<td>Dedicated circuit must have circuit breaker or fuse protection. CDUs 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 CDU must be provided and must meet all applicable codes and regulations. In North America, protection must have a 10,000A interrupt capacity.</td>
<td>Le circuit spécialisé doit avoir un disjoncteur ou une protection de fusible. CDUs 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 équivalant 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.</td>
<td>Der feste Stromkreis muss mit einem Schutzschalter oder einem Sicherungsschutz versehen sein. CDUs verfügt über keinen Hauptschutzschalter bzw. über keine Sicherung, damit kein einziger 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 verfügbar sein.</td>
</tr>
<tr>
<td>The plug on the power supply cord shall be installed near the equipment and shall be easily accessible.</td>
<td>La prise sur le cordon d’alimentation sera installée près de l’équipement et sera facilement disponible.</td>
<td>Der Stecker des Netzkabels muss in der Nähe der Ausrüstung installiert werden und leicht zugänglich sein.</td>
</tr>
<tr>
<td>Installation Orientation: Cx-xxVx-x units are design to be installed in vertical orientation.</td>
<td>Installation Orientation : Les unités Cx-xxVx-x sont conçues pour être installées dans une orientation verticale.</td>
<td>Installationsausrichtung: Cx-xxVx-x Einheiten sind zur vertikalen Installation vorgesehen.</td>
</tr>
<tr>
<td>Always disconnect the power supply cord before opening to avoid electrical shock.</td>
<td>Toujours déconnecter le cordon d’alimentation avant d’ouvrir pour éviter un choque électrique.</td>
<td>Vor dem Öffnen immer Netzteile abziehen um elektrischen Schlag zu vermeiden.</td>
</tr>
<tr>
<td>WARNING! Earth connection is essential before connecting supply!</td>
<td>ATTENTION ! Une connection de masse est essentielle avant de connecter l’alimentation !</td>
<td>ACHTUNG! Hoher Ableitstrom! Ein Erdungsanschluss ist vor dem Einschalten der Stromzufuhr erforderlich!</td>
</tr>
<tr>
<td>WARNING! Cx-xxxxE-x units Double Pole/Neutral Fusing</td>
<td>ATTENTION! Les unités Cx-xxxxE-x Double Pôle/Fusible sur le Neutre</td>
<td>ACHTUNG!: Cx-xxxxE-x Zweipolige bzw. Neutralleiter-Sicherung</td>
</tr>
<tr>
<td>This equipment should only be installed by trained personnel.</td>
<td>Cet équipement est uniquement destiné à être installé par personnel qualifié.</td>
<td>Dieses Gerät ist nur für den Einbau durch Personal vorgesehen.</td>
</tr>
<tr>
<td>Products rated for 240/415VAC may be fitted with a plug that is rated for a higher voltage. Caution must be taken to assure that the rating of the unit and the supply voltage match.</td>
<td>Les produits prévus pour 240/415VAC peut être équipé d’un bouchon qui est conçu pour une tension plus élevée. Des précautions doivent être prises pour assurer que la cote de l’unité et la tension d’alimentation correspondent.</td>
<td>Produkte die für 240/415VAC zugelassen sind können mit einem Stecker der für eine höhere Spannung ausgestattet sein. Vorsicht ist geboten, um sicherzustellen, dass die erlaubten Betriebswerte des Gerätes und der Versorgungsspannung zueinander passen.</td>
</tr>
</tbody>
</table>
Installing the Power Input Retention Bracket

For units with a total maximum output <30A, it may be necessary to install the power input retention bracket prior to mounting the unit within the rack.

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.

Mounting

1. Attach the removable flanges to the mount points on the rear of the enclosure using M4 screws.
2. Attach the mounting L-brackets to the flanges with the supplied screws, washers and nut plates. The slots allow about 1½ inches of vertical adaptability.
3. Attach the top and bottom brackets to your rack.

NOTE: Contact your Server Technology Sales Representative for information regarding custom bracket design and fabrication services if you are unable to find a suitable manner for utilizing the included mounting brackets.

Optionally, the supplied button mounts may be used for mounting the CDU into cabinets supporting this method of equipment mounting.
**Attaching the Expansion Module**

Connect the Expansion Module CDU with provided RJ12 crossover cable at the Link port on the POPS Switched CDU.

*NOTE:*  The overall length of the RJ12 crossover cable should not exceed 10 feet.

**Connecting to the Power Source**

On 30A units, the input power cord is attached to the base of the unit. On units with a total maximum output <30A, you must first attach the power cord to the unit before connecting the unit to the power source.

**To attach a 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 CDU 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 111 for more information.

**Connecting the Sensors**

The Switched CDU is equipped with two mini RJ11 T/H ports for attachment of the Temperature/Humidity sensors. Attach the mini RJ11 plug of the sensor(s) to the appropriate T/H port.

**Connecting to the Unit**

**Serial (RS232) port**

The POPS Switched Cabinet Distribution Unit 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 *Data Connections* in Appendix C: Technical Specifications for more information on the Serial RS-232 port.

**Ethernet port**

The POPS Switched Cabinet Distribution Unit is equipped with an RJ45 10/100Base-T Ethernet port for attachment to an existing network. This connection allows access to the Switched CDU via Telnet or Web.

The Switched Cabinet Distribution Unit is configured with the following network defaults to allow unit configuration out-of-the-box through either Telnet or Web:

*NOTE:* When installed on a DHCP enabled networks, the following network defaults DO NOT apply as the Sentry ships with DHCP support enabled.

- 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
UPS Administration ............................................................................................................. 62
Feature Administration .................................................................................................... 66
Interfaces

The POPS Switched Cabinet Distribution Unit has two interfaces: the Web interface accessed via the HTTP enabled Ethernet connections, and the command line for serial and Telnet connections.

Outlet Naming and Grouping

Absolute names are specified by a period (.) followed by a tower letter and outlet number. The tower letter for the Switched Cabinet Distribution Unit is A and the tower letter for the optional Expansion Module is B.

Usernames and Passwords

The Switched Cabinet Distribution Unit 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.
Web Interface

The Web interface is constructed of three major components:

1. System Location bar
2. User/Navigation bar
3. 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 Web pages. 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.

![Figure 3.1 Example of Web Interface Page](image.png)

Logging In

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

To log in by Web:

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 admn/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 outlet’s absolute and descriptive names, the Outlet Status reported to the Sentry by the outlet, the current Control State being applied by the Sentry, the outlet load in amperes, and outlet active power in watts.

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. From the Individual page, the user applies 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

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

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

Outlets

The Outlets page displays:

- Outlet’s absolute and descriptive names
- Outlet status
- POPS outlet load in amperes.
- POPS outlet voltage
- POPS outlet active power in watts

This page will refresh automatically every 10 seconds.

Input Feeds

The Input Feeds page displays:

- Infeed’s absolute and descriptive names
- Infeed status
- Input/branch phase load in amperes
- Input voltage
- Calculated power usage in watts

This page will refresh automatically every 10 seconds.

System

The System page displays:

- Calculated power usage for ALL infeeds in watts
- Configured total system area in square feet.
- Calculated power usage in watts/square foot

This page will refresh automatically every 10 seconds.

UPS

The UPS page displays the following information for each UPS device associated with the Sentry unit:

- Status
- Voltage
- Hostname/IP address

This page will refresh automatically every 10 seconds.

Environmental Monitoring

Sensors

The Sensors page displays:

- Temperature/humidity sensor’s absolute and descriptive names
- Temperature/humidity sensor readings in degrees Celsius and percent relative humidity

This page will refresh automatically every 10 seconds.

Shutdown

The Shutdown section offers access to all Remote Shutdown configuration options. This section is available to administrative level users only. For more information about configuration requirements, see Remote Shutdown on page 106.

Outlets

Enabling or disabling Remote Shutdown support:

Select or deselect outlets to enable/disable Remote Shutdown support for the Shutdown/Delay field and press Apply.

Setting the Remote Shutdown delay:

Enter the shutdown delay (in seconds) in the outlet Shutdown/Delay field and press Apply.
Operations

17

Installation and Operations Manual

Editing the target server’s Hostname/IP address:
In the outlet Hostname/IP field, enter an IP address or Hostname and press Apply.

Enabling or disabling shutdown script support:
Select or deselect outlet to enable/disable shutdown script support for in the Script/Delay column and press Apply.

Setting the shutdown script delay:
Enter the shutdown delay (in minutes) in the outlet Script/Delay field and press Apply.

Configuration
The Configuration section offers access to all unit configuration options. 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 other system wide configurations.

For descriptive names, up to 24 alphanumeric and other typed characters (ASCII 33 to 126 decimal) are allowed; spaces are not allowed.

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

Creating a pre-login banner:
Click on the Login Banner link.

On the subsequent Login Banner page, enter a pre-login banner and press Apply.

NOTE: The pre-login banner may be up to 2070 characters in length and is displayed prior to the login prompt. If left blank, no system banner will be displayed prior to login prompt.

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.

Enabling or disabling strong password requirements:
Sentry supports enforcement of strong passwords for enhanced security. When enabled, all new passwords must be a minimum of 8 characters in length with at least one uppercase letter, one lowercase letter, one number and one special character.

Acceptable strong passwords:
n0tOnmyw@tch
john2STI?
H3reUgo!

NOTE: Strong password requirements also enforce a minimum change of four character positions when defining new strong passwords.

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

NOTE: The strong password requirement is applied against all new passwords.

Enabling or disabling the external reset button:
Select Enabled or Disabled from the External Reset Button drop-down menu and press Apply.

Setting the temperature scale:
Select Celsius or Fahrenheit from the Temperature Scale drop-down menu and press Apply.
Setting the system area:
Enter a system area value in the Area field and press Apply.

Setting the system area unit of measure:
Select the unit of measure from the Unit of Measure drop-down list and press Apply.

Setting the system input power factor:
The Power Factor value is used to provide calculated power usage displayed in the Power Monitoring pages.
Enter a numeric value from 0.50 to 1.00 in the Power Factor field, and press Apply.

Setting the 3-phase load out-of-balance threshold:
This setting is used for devices with 3-phase input voltages to notify of a system imbalance between the three phases of power.
In the 3-Phase Load Out-of-Bounds Threshold field, enter a value from 0 to 100% and press Apply.

Configuring the Command Line Interface (CLI) session timeout:
Enter a timeout period (in minutes) in the CLI Session Timeout field, and press Apply. The valid timeout range is 1 minute to 1440 minutes (24 hours); the default is 5 minutes.

Configuring the web session (Web Interface) timeout:
Enter a timeout period (in minutes) in the Web Session Timeout field.
The valid timeout range is 1 to 1440 minutes (24 hours); the default is 5 minutes.

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 222 for additional information on creating descriptive outlet names.

Creating a descriptive serial port name:
Click on the Serial Port Names link which will open the Serial Ports configuration page. See Serial Ports on page 20 for additional information on creating descriptive serial port names.

Creating a descriptive Environmental Monitor name:
Click on the Environmental Monitor Names link.
On the subsequent Environmental Monitor Names page, enter a descriptive name and press Apply.

Creating descriptive sensor names:
Click on the Sensor Names link.
On the subsequent Sensor Names page, enter a descriptive name and press Apply.
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 Web:

- 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 32.

Enabling or disabling DHCP support:

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

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 enables or disables Telnet and SSH support and configures the port number that the Telnet or SSH server watches. For more information on SSH see page 69 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.

Enabling or disabling SSH server authentication methods:

The Sentry SSH server supports two authentication methods for security and validation: Password and Keyboard-Interactive.

Password is an authentication method where the SSH client gathers username/password credentials and makes the authentication request to the SSH sever with the credentials. The Password method is controlled by the SSH client.

Keyboard-Interactive is an authentication method where the SSH server controls an information field followed by one or more prompts requesting credential information from the SSH client. The client gathers credential information keyed-in by the user and sends it back to the server. The Keyboard-Interactive method is controlled by the SSH server.

Individual enabling and disabling of the Password and Keyboard-Interactive authentication methods are supported to allow an SSH client to be forced to use a specific method. Although both methods are available, by enabling the Keyboard-Interactive method and disabling the Password method, the SSH client is forced to use Keyboard-Interactive, which is required to display the login banner.

NOTE: At least one authentication method must be enabled.

Select the Password checkbox and/or the Keyboard-Interactive checkbox 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 67 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 uses 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 the serial port.

NOTE: Pass-Thru connections may only be initiated from the command line interface via a Telnet/SSH session.

Setting the data-rate for all serial ports:
Select the serial port data-rate from the drop-down menu and press Apply.

Setting the serial port timeout value:
Enter the timeout value (in minutes) in the Connection Timeout field and press Apply.

Creating a descriptive serial 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 a descriptive name up to 24 alphanumeric and other typed characters - (ASCII 33 to 126 decimal) are allowed; spaces are not allowed. Press Apply.

Enabling or disabling serial 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.
Towers

The Towers configuration page is used for assignment and/or editing of:

- Descriptive names
- Serial and Model numbers
- Operation voltage types

NOTE: If set at the factory, the serial number, model number and voltage type WILL NOT be user-editable.

Creating a descriptive tower name:

In the Tower Name field, enter a descriptive name and press Apply.

Setting the tower serial number:

In the Serial Number field, enter the serial number of the unit and press Apply.

Setting the tower model number:

In the Model Number field, enter the model number of the unit and press Apply.

Setting the operational AC or DC voltage type:

From the AC/DC drop-down menu, select AC or DC, and press Apply.

Input Feeds

The Input Feeds configuration page is used for assignment and/or editing of input feed descriptive names, operational voltage and maximum load capacity.

Creating a descriptive input feed name:

In the Input Feed Name field, enter a descriptive name and press Apply.

Setting the infeed operational voltage:

In the Input Feed Voltage field, enter a value from 0 to 480 and press Apply.

NOTE: If Smart Load-Shedding has been activated and UPS voltage polling configured for an infeed, the polled voltage value will be used for all power calculations.

Setting the infeed maximum load capacity:

In the Input Feed Load Capacity field, enter a value from 1 to 255 and press Apply.

UPS

The UPS Configuration page is used for adding a new UPS device and configuring the UPS devices connected to Sentry units.

To add a new UPS:

Select the UPS manufacturer type from the Type drop-down list, type an IP address (or hostname) for the UPS, and press Apply.

To edit the UPS type:

Under the Action heading, click the Edit link for the UPS to be configured. The Configuration UPS page reformats to an edit page where UPS device settings are configured and UPS devices are associated with an infeed.

Selecting the UPS type:

Select the UPS manufacturer type from the UPS Type drop-down list and press Apply.

Editing the UPS Hostname/IP Address:

In the Hostname/IP field, type an IP Address or Hostname and press Apply.

Editing the UPS SNMP GET community string:

In the SNMP GET Community String field, type the community string configured on the UPS device and press Apply.
Enabling/Disabling UPS voltage polling:
From the Poll UPS Voltage drop-down list, select Enabled or Disabled and press Apply.

Editing the UPS SNMP port number:
In the Port field, type the port number and press Apply.

Associate the UPS with an infeed:
Select the infeed(s) powered by the UPS and press Apply.

To remove a UPS:
On the Configuration UPS page, under the Action heading, click the Remove link for the UPS you want to remove.

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 a descriptive name. Up to 24 alphanumeric and other typed characters (ASCII 33 to 126 decimal) are allowed; spaces are not 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 typed characters (ASCII 33 to 126 decimal) are allowed; spaces are not 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 typed characters (ASCII 33 to 126 decimal) are allowed; spaces are not 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 the following defined privilege levels:

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

**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 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, configure automatic FTP updates or system configuration uploads/downloads. See Appendix B: Firmware for more information on uploading firmware.

Setting the FTP Host Address:
Enter the IP address or hostname in the Host 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.

Enabling or disabling automatic updates:
The Sentry features the ability to schedule automatic firmware updates. When enabled and configured, the Sentry will regularly check the FTP server for a new firmware image and upload it.
Select Enabled or Disabled from the drop-down menu and press Apply.

Setting the automatic update scheduled day:
Select the desired day for the automatic update from the drop-down menu and press Apply.

Setting the automatic update scheduled hour:
Select the desired hour for the automatic update from the drop-down menu and press Apply.

Enabling or disabling the FTP server:
The Sentry features the ability to upload and download system configuration files to ease implementation across multiple Sentry devices. See Chapter 4: Advanced Operations - Upload/Download for more information on configuration upload and download.
Select Enabled or Disabled from the drop-down menu and press Apply.

NOTE: The FTP server must be enabled for configuration upload or download.
SNTP/Syslog

The SNTP/Syslog configuration page is used for setup and maintenance of SNTP and Syslog support. For additional information and configuration requirements for Syslog support, see Syslog on page 96.

Setting the SNTP server address:
Enter the IP address or hostname in the Primary and/or Secondary Host field and press Apply.

Setting the Local GMT offset:
Select the local offset from GMT value from the drop-down menu and press Apply.

Setting the Syslog server address:
Enter the IP address or hostname in the Primary and/or Secondary Host field and press Apply.

Changing the Syslog server port number:
In the Syslog Port field, enter the port number and press Apply.

SNMP/Thresholds

The SNMP/Thresholds configuration page is used for setup and maintenance of all settings required to enable SNMP support, and to provide access to the trap configuration pages. For additional information on SNMP support and detailed descriptions of available traps, see SNMP on page 71.

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 or hostname in the appropriate Trap Destination field and press Apply.

Setting IP Restrictions:
Select No Restrictions or Trap Destinations Only from the IP Restrictions drop-down menu and press Apply.

NOTE: When Trap Destinations Only is selected, SNMP Manager GET and SET requests are only allowed from the IP addresses of the defined traps destinations.

Setting the SNMP SysName, SysLocation or SysContact objects:
In the appropriate field, enter the SysName, SysLocation or SysContact objects 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 and thresholds:
Click on the Input Feed Traps and Thresholds 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 default input feed high load threshold is 80% of the input feed maximum load capacity.
Configuring outlet traps:
Click on the Outlet Traps and Thresholds link.
On the subsequent Outlet Traps and Thresholds page, select or deselect the desired traps and press Apply.

Enabling or disabling Environmental Monitor traps:
Click on the Environmental Monitor Traps link.
On the subsequent page, select or deselect the desired traps and press Apply.

Configuring Temperature and Relative Humidity sensor traps:
Click the Sensor Traps and Thresholds link.
On the subsequent Sensor Traps and Thresholds page, select or deselect the desired trap checkboxes and press Apply.

Configuring Temperature and Relative Humidity sensor thresholds:
Click the Sensor Traps and Thresholds link.

For temperature thresholds, type a low and high temperature value in the Low Temp and High temp fields and press Apply.

For relative humidity thresholds, type a low and high humidity percentage in the Low Humid and High Humid fields, and press Apply.

NOTE: For temperature thresholds, the valid range is 0 to 123 in degrees Celsius or 32 to 254 in degrees Fahrenheit. For relative humidity, the valid range is 0 to 100 (in percent relative humidity).

Configuring Temperature Recovery Delta:
Click the Sensor Traps and Thresholds link.

The Recovery Delta field allows configuration of the number of degrees of change needed to recover from a temperature alarm. After exceeding the high-temperature threshold, the temperature value must fall below the high-temperature threshold by the number of degrees specified in the Recovery Delta field before the sensor recovers.

For example, if the High Temp value is 80 degrees Fahrenheit, and the Recovery Delta field is 2 degrees Fahrenheit, the sensor will not recover until a temperature value of 78 degrees Fahrenheit is reported.

To configure a temperature recovery delta, type a value (in degrees) in the Recovery Delta field and press Apply.

NOTE: The acceptable value range for the Recovery Delta field is 0-10 degrees for Celsius and 0-18 degrees for Fahrenheit. The default value for the Recovery Delta field is 1 degree Celsius and 2 degrees Fahrenheit.
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 80.

Enabling or disabling LDAP support:
Select Enabled or Disabled from the LDAP drop-down menu and press Apply.

Changing the LDAP server port:
Enter the port number in the LDAP Port field and press Apply.

Setting the LDAP server address:
Enter the IP address or hostname in the Primary and/or Secondary Host field and press Apply.

Enabling or disabling LDAP over TLS/SSL:
Select Yes or No from the Use TLS/SSL drop-down menu and press Apply.

NOTE: If LDAP over TLS/SSL is enabled, MD5 binding is disabled.

Setting the LDAP bind password type:
Select Simple or MD5 from the Bind Type drop-down menu and press Apply.

NOTE: If MD5 binding is enabled, LDAP over TLS/SSL is disabled.

For more information on LDAP bind password types, see Setting the LDAP bind password type on page 82.

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 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 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.

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 84.

NOTE: Server Technology recommends NOT setting the authentication order to Remote Only until the LDAP has been fully configured and tested.
Setting the DNS IP address:
See Network on page 19 for information on how to set the DNS IP address.

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 typed characters (ASCII 33 to 126 decimal) are allowed; spaces are not 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 23.

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 90.

Enabling or disabling TACACS+ support:
Select Enabled or Disabled from the TACACS+ drop-down menu and press Apply.

Changing the TACACS+ server port:
Enter the port number in the Port field and press Apply.

Setting the TACACS+ server address:
Enter the IP address or hostname in the Primary and/or Secondary Host field and press Apply.

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 92.

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

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 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 23.

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.
RADIUS

The Remote Authentication Dial-in User Service (RADIUS) configuration page is used for setup and maintenance of all settings required to enable RADIUS support. For additional information and configuration requirements, see RADIUS on page 96.

Enabling or disabling RADIUS support:
Select Enabled or Disabled from the RADIUS drop-down menu and press Apply.

Configuring the authentication order:
Select Remote->Local or Remote Only from the drop-down menu and press Apply.
For more information about remote authentication order, see Setting the authentication order on page 92.

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

Changing the RADIUS server address:
Enter the IP address or hostname in the Primary and/or Secondary Server field and press Apply.

Setting the RADIUS shared secret:
The shared secret is the RADIUS authentication key.
Enter the shared secret in the Primary and Secondary Shared Secret field. Up to 48 upper and lowercase alphanumeric and other typed characters (ASCII 33 to 126 decimal) and spaces are allowed; control characters are not allowed. Press Apply.
To change the shared secret, check the Change checkbox to clear the Shared Secret field, enter the new shared secret, and press Apply.

Changing the RADIUS server port:
This field specifies the port number used by the RADIUS server for incoming RADIUS authentication requests.
Enter the port number in the Primary and/or Secondary Port field and press Apply.
The valid port number range is 1-65535; default is 1812.

Setting the RADIUS server timeout value:
The Timeout field specifies the time interval (in seconds) to wait for a reply from the RADIUS server before resending an authentication request.
Enter the timeout value (in seconds) in the Primary and/or Secondary Timeout field and press Apply.
The valid timeout range is 1-30 seconds; default is 5 seconds.

Setting the number of RADIUS server retries:
The Set RADIUS Retries command specifies the number of times an authentication request is sent to the RADIUS server. The Sentry will attempt authentication with the primary server until the number of retries is reached, then will attempt authentication with the secondary server. If no server response is received from all attempts, then the Sentry will reject the authentication request.
Enter the number of retries in the Primary and/or Secondary Retries field and press Apply.
The valid retries range is 0-10; default is 2.
Email

The Email configuration page is used for setup and maintenance Email log support. For additional information and configuration requirements for Email support, see Email on page 96.

Enabling or disabling Email support:
Select Enabled or Disabled from the Email Notifications drop-down menu and press Apply.

Setting the SMTP server address:
Enter the IP address or hostname in the SMTP Host field and press Apply.

Changing the SMTP server port:
Enter the port number in the SMTP Port field and press Apply.

Setting the ‘From’ email address:
Enter the ‘from’ email address in the ‘From’ Address field and press Apply.

Setting the ‘To’ email address:
Enter the ‘to’ email address in the Primary or Secondary ‘Send To’ Address field and press Apply.

Enabling or disabling event type notifications:
Select Enabled or Disabled from the Include…Messages drop-down menus and press Apply.

Features

The Features configuration page is used for activation and maintenance of special features purchased from Server Technology. From this page an administrator may review all activated features as well as activate newly purchased features.

To activate a special feature:
In the Feature Key Value field, enter the activation key provided by Server Technology and press Apply.

NOTE: A restart of the Sentry is required after activating new special features.

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.

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.

Change Password

The Change Password feature allows users to change their own password.

NOTE: An administrator can always assign a new password.

Changing a password:
Enter the current password, enter a new password and verify the new password. Press Apply.

View Log

The View Log feature enables viewing of the internal system log. This features logs all authentication attempts, power actions, configuration changes and other system events. The system memory stores more than 4000 entries in a continuously aging log. For permanent off-system log storage, the Syslog protocol is supported. For additional information and configuration requirements for the system log and Syslog support, see Logging on page 100.

NOTE: The system log is viewable only by users with administrative privileges.

Reviewing the system log:
Click on the Previous 100 entries or Next 100 entries link to navigate through the log.
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 Web interface.

**Uploading new firmware:**
See page 110  for more information on uploading new firmware from the Web interface.

**Generating a new SSL X.509 certificate:**
Select the Restart and generate a new X.509 certificate from the Action drop-down menu and press Apply.

**Computing new SSH security keys:**
Select the Restart and compute new SSH keys from the Action drop-down menu and press Apply.
**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). The default data rate is 9600.

### 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 (Switched CDU:) appears. If a location identifier was defined, it will be displayed before the Switched CDU: prompt. See Creating a location description: on page 53 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect</td>
<td>Connects to a serial/Pass-Thru port</td>
</tr>
<tr>
<td>Envmon</td>
<td>Displays the status of the integrated Environmental Monitor</td>
</tr>
<tr>
<td>ILoad</td>
<td>Displays the status of the infeeds</td>
</tr>
<tr>
<td>IStat</td>
<td>Displays the status of the infeeds</td>
</tr>
<tr>
<td>List Group</td>
<td>Lists all assigned outlets for a group name</td>
</tr>
<tr>
<td>List Groups</td>
<td>Lists all accessible groups for the current user</td>
</tr>
<tr>
<td>List Outlets</td>
<td>Lists all accessible outlets for the current user</td>
</tr>
<tr>
<td>List Ports</td>
<td>Lists all accessible serial/Pass-Thru ports for the current user</td>
</tr>
<tr>
<td>Login</td>
<td>Ends the current session and brings up the Username: prompt</td>
</tr>
<tr>
<td>Logout</td>
<td>Ends a session</td>
</tr>
<tr>
<td>Off</td>
<td>Turns one or more outlets off</td>
</tr>
<tr>
<td>On</td>
<td>Turns one or more outlets on</td>
</tr>
<tr>
<td>OStat</td>
<td>Displays the status of the outlets</td>
</tr>
<tr>
<td>Password</td>
<td>Changes the password for the current user</td>
</tr>
<tr>
<td>Quit</td>
<td>Ends a session</td>
</tr>
<tr>
<td>Reboot</td>
<td>Reboots one or more outlets</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the on/off status of one or more outlets</td>
</tr>
<tr>
<td>UPSStat</td>
<td>Displays the status of the associated UPSs</td>
</tr>
<tr>
<td>Add Group touser</td>
<td>Grants a user access to one or more groups</td>
</tr>
<tr>
<td>Add Outletgroup</td>
<td>Adds an outlet to a group name</td>
</tr>
<tr>
<td>Add Outlet touser</td>
<td>Grants a user access to one or all outlets</td>
</tr>
<tr>
<td>Add Port touser</td>
<td>Grants a user access to one or all serial/Pass-Thru ports</td>
</tr>
</tbody>
</table>
### Administrative Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Group</td>
<td>Adds a group name</td>
</tr>
<tr>
<td>Create UPS</td>
<td>Adds a UPS association</td>
</tr>
<tr>
<td>Create User</td>
<td>Adds a user account</td>
</tr>
<tr>
<td>Delete Group from user</td>
<td>Removes access to one or more groups for a user</td>
</tr>
<tr>
<td>Delete Outlet from group</td>
<td>Deletes an outlet from a group name</td>
</tr>
<tr>
<td>Delete Outlet from user</td>
<td>Removes access to one or all outlets for a user</td>
</tr>
<tr>
<td>Delete Port from user</td>
<td>Removes access to one or all serial/Pass-Thru ports</td>
</tr>
<tr>
<td>List User</td>
<td>Displays all accessible outlets/groups/ports for a user</td>
</tr>
<tr>
<td>List Users</td>
<td>Displays privilege levels for all users</td>
</tr>
<tr>
<td>Remove Group</td>
<td>Deletes a group name</td>
</tr>
<tr>
<td>Remove UPS</td>
<td>Deletes a UPS association</td>
</tr>
<tr>
<td>Remove User</td>
<td>Deletes a user account</td>
</tr>
<tr>
<td>Restart</td>
<td>Performs a warm boot</td>
</tr>
<tr>
<td>Set Banner</td>
<td>Sets the pre-login banner text</td>
</tr>
<tr>
<td>Set DHCP</td>
<td>Enables or disables DHCP support</td>
</tr>
<tr>
<td>Set DNS</td>
<td>Sets the IP address of the Domain Name server</td>
</tr>
<tr>
<td>Set Envmon Name</td>
<td>Specifies a descriptive field for the integrated Environmental Monitor</td>
</tr>
<tr>
<td>Set Envmon THS Name</td>
<td>Specifies a descriptive field for a temperature-humidity sensor</td>
</tr>
<tr>
<td>Set FTP Autoupdate Day</td>
<td>Sets the automatic FTP update day</td>
</tr>
<tr>
<td>Set FTP Autoupdate Hour</td>
<td>Sets the automatic FTP update hour</td>
</tr>
<tr>
<td>Set FTP Autoupdate</td>
<td>Enables or disables automatic FTP update support</td>
</tr>
<tr>
<td>Set FTP Directory</td>
<td>Specifies the directory for the file to be uploaded</td>
</tr>
<tr>
<td>Set FTP Filename</td>
<td>Specifies the file to be uploaded via FTP</td>
</tr>
<tr>
<td>Set FTP Host</td>
<td>Sets the FTP Host IP address or hostname</td>
</tr>
<tr>
<td>Set FTP Password</td>
<td>Sets the password for the FTP Host</td>
</tr>
<tr>
<td>Set FTP Server</td>
<td>Enables or disables the FTP server</td>
</tr>
<tr>
<td>Set FTP Username</td>
<td>Sets the username for the FTP Host</td>
</tr>
<tr>
<td>Set Gateway</td>
<td>Sets the Gateway of the Sentry</td>
</tr>
<tr>
<td>Set HTTP Port</td>
<td>Specifies the target port for HTTP access</td>
</tr>
<tr>
<td>Set HTTP Security</td>
<td>Specifies the HTTP server authentication method</td>
</tr>
<tr>
<td>Set HTTP</td>
<td>Enables or disables HTTP access</td>
</tr>
<tr>
<td>Set Infeed Loadmax</td>
<td>Specifies the maximum load capacity for the infeed</td>
</tr>
<tr>
<td>Set Infeed Name</td>
<td>Specifies a descriptive field for the infeed</td>
</tr>
<tr>
<td>Set Infeed Voltage</td>
<td>Specifies the nominal input voltage for the infeed</td>
</tr>
<tr>
<td>Set Ipaddress</td>
<td>Sets the IP address of the Sentry</td>
</tr>
<tr>
<td>Set LDAP UseTLS</td>
<td>Enables or disables LDAP over TLS/SSL support</td>
</tr>
<tr>
<td>Set Location</td>
<td>Specifies a descriptive field for the Web control screen and login banner</td>
</tr>
<tr>
<td>Set Option Button</td>
<td>Enables or disables the external configuration reset button</td>
</tr>
<tr>
<td>Set Option Coldboot Alert</td>
<td>Enables or disables the Coldboot Alert feature using a serial protocol</td>
</tr>
<tr>
<td>Set Option Display</td>
<td>Sets the LED orientation for external Current displays</td>
</tr>
<tr>
<td>Set Option More</td>
<td>Enables or disables the ‘more’ prompt</td>
</tr>
<tr>
<td>Set Option StrongPasswords</td>
<td>Enables or disables strong password requirements</td>
</tr>
<tr>
<td>Set Option Tempscale</td>
<td>Sets the Environmental Monitor temperature scale</td>
</tr>
<tr>
<td>Set Option CLI Timeout</td>
<td>Sets the Command Line Interface (CLI) session timeout period</td>
</tr>
<tr>
<td>Set Option Web Timeout</td>
<td>Sets the web session (Web Interface) timeout period</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set Outlet Name</td>
<td>Specifies a descriptive field for a device attached to an outlet</td>
</tr>
<tr>
<td>Set Outlet PostOnDelay</td>
<td>Sets the Post-On delay for an outlet</td>
</tr>
<tr>
<td>Set Outlet RebootDelay</td>
<td>Sets the reboot delay for all outlets</td>
</tr>
<tr>
<td>Set Outlet SeqInterval</td>
<td>Sets the sequencing interval for all outlets</td>
</tr>
<tr>
<td>Set Outlet Wakeup</td>
<td>Sets the wakeup state for an outlet</td>
</tr>
<tr>
<td>Set Port DSR Check</td>
<td>Sets the DSR active signal checking for a serial/Pass-Thru port</td>
</tr>
<tr>
<td>Set Port Name</td>
<td>Specifies a descriptive field for a serial/Pass-Thru port</td>
</tr>
<tr>
<td>Set Port Speed</td>
<td>Set the connection speed for all serial/Pass-Thru ports</td>
</tr>
<tr>
<td>Set Port Timeout</td>
<td>Sets the inactivity timer for Pass-Thru sessions</td>
</tr>
<tr>
<td>Set SNMP IP Restrict</td>
<td>Allows SNMP GET and SET requests from defined traps destinations only</td>
</tr>
<tr>
<td>Set SNTP</td>
<td>Sets the IP address or hostname of the SNTP servers</td>
</tr>
<tr>
<td>Set SNTP GMTOffset</td>
<td>Sets the local GMT offset applied to the SNTP date/time</td>
</tr>
<tr>
<td>Set Subnet</td>
<td>Sets the Subnet Mask of the Sentry</td>
</tr>
<tr>
<td>Set System Area</td>
<td>Specifies total system area for the system</td>
</tr>
<tr>
<td>Set System Area Unit</td>
<td>Specifies the system area (footprint) unit of measure</td>
</tr>
<tr>
<td>Set System Balance</td>
<td>Sets the percent load out-of-balance threshold for 3-phase systems</td>
</tr>
<tr>
<td>Set System PF</td>
<td>Sets the power factor used in the total system power calculation</td>
</tr>
<tr>
<td>Set Telnet Port</td>
<td>Sets the Telnet server port number</td>
</tr>
<tr>
<td>Set Telnet</td>
<td>Enables or disables Telnet access</td>
</tr>
<tr>
<td>Set Tower 3Phase</td>
<td>Specifies the AC voltage type for the tower</td>
</tr>
<tr>
<td>Set Tower Model</td>
<td>Specifies the model number for the tower</td>
</tr>
<tr>
<td>Set Tower Name</td>
<td>Specifies a descriptive field for the tower</td>
</tr>
<tr>
<td>Set Tower ProdSN</td>
<td>Specifies the serial number for the tower</td>
</tr>
<tr>
<td>Set Tower</td>
<td>Specifies the AC or DC voltage type for the tower</td>
</tr>
<tr>
<td>Set UPS AddInfeed</td>
<td>Adds an infeed association to a UPS</td>
</tr>
<tr>
<td>Set UPS DelInfeed</td>
<td>Deletes an infeed association from a UPS</td>
</tr>
<tr>
<td>Set UPS GETComm</td>
<td>Sets the UPS 'get' community string</td>
</tr>
<tr>
<td>Set UPS Host</td>
<td>Sets the UPS Host IP address or hostname</td>
</tr>
<tr>
<td>Set UPS Port</td>
<td>Specifies the target port for a UPS</td>
</tr>
<tr>
<td>Set UPS Type</td>
<td>Sets the UPS type</td>
</tr>
<tr>
<td>Set UPS VPoll</td>
<td>Enables or disables UPS voltage polling</td>
</tr>
<tr>
<td>Set User Access</td>
<td>Sets the access level for a user</td>
</tr>
<tr>
<td>Set User Environ</td>
<td>Grants or removes privileges to view input/environmental monitoring status</td>
</tr>
<tr>
<td>Set User Password</td>
<td>Changes the password for a user</td>
</tr>
<tr>
<td>Show FTP</td>
<td>Displays FTP configuration information</td>
</tr>
<tr>
<td>Show Infeeds</td>
<td>Displays infeed configuration information</td>
</tr>
<tr>
<td>Show Network</td>
<td>Displays network configuration information</td>
</tr>
<tr>
<td>Show Options</td>
<td>Displays system option information</td>
</tr>
<tr>
<td>Show Outlets</td>
<td>Displays configuration information for all outlets</td>
</tr>
<tr>
<td>Show Ports</td>
<td>Displays serial/Pass-Thru port configuration information</td>
</tr>
<tr>
<td>Show SNTP</td>
<td>Displays SNTP configuration information</td>
</tr>
<tr>
<td>Show System</td>
<td>Displays system configuration information</td>
</tr>
<tr>
<td>Show Towers</td>
<td>Displays tower configuration information</td>
</tr>
<tr>
<td>Show UPS</td>
<td>Displays UPS configuration information</td>
</tr>
<tr>
<td>System Status</td>
<td>Displays system status configuration information</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the Sentry firmware version</td>
</tr>
</tbody>
</table>
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 Switched CDU: 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:

```
Switched CDU: on .a2<Enter>
```

The following command turns on all the outlets in the group named ServerGroup_1:

```
Switched CDU: 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 Switched CDU: 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:

```
Switched CDU: off FileServer_1<Enter>
```

The following command turns off all outlets:

```
Switched CDU: 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 Switched CDU: 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:

Switched CDU: 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, the current Control State being applied by the Sentry, and outlet load and outlet active power values. 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 15.

To display on/off status of one or more outlets:
At the Switched CDU: 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:

Switched CDU: status FileServer_1<Enter>

Outlet   Outlet                    Outlet     Load      Power     Control
ID       Name                      Status     (Amps)    (Watts)   State
.A3      FileServer_1              On         0.00      0         Idle On

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

Switched CDU: status<Enter>

Outlet   Outlet                    Outlet     Load      Power     Control
ID       Name                      Status     (Amps)    (Watts)   State
.A1      DataServer_1              On         1.73      356       Idle On
.A2      WebServer_1               On         0.00      0         Idle On
.A3      FileServer_1              On         0.00      0         Idle On
.A4      TowerA_Outlet4            On         0.00      0         Idle On
.A5      TowerA_Outlet5            On         0.00      0         Idle On
.A6      TowerA_Outlet6            On         0.00      0         Idle On

More (Y/es N/o):
The following command displays the on/off status for outlets in the group ServerGroup_1:

```
Switched CDU: status ServerGroup_1<Enter>
```

<table>
<thead>
<tr>
<th>Outlet ID</th>
<th>Outlet Name</th>
<th>Status</th>
<th>Load (Amps)</th>
<th>Power (Watts)</th>
<th>Control State</th>
</tr>
</thead>
<tbody>
<tr>
<td>.A1</td>
<td>Data_Server_1</td>
<td>On</td>
<td>1.73</td>
<td>353</td>
<td>Idle On</td>
</tr>
<tr>
<td>.A2</td>
<td>WebServer_1</td>
<td>On</td>
<td>1.75</td>
<td>363</td>
<td>Idle On</td>
</tr>
<tr>
<td>.A3</td>
<td>FileServer_1</td>
<td>On</td>
<td>1.71</td>
<td>366</td>
<td>On</td>
</tr>
</tbody>
</table>

**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 Switched CDU: prompt, type `list outlets` and press Enter.

*Example*

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

```
Switched CDU: list outlets<Enter>
```

<table>
<thead>
<tr>
<th>Outlet ID</th>
<th>Outlet Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>.A1</td>
<td>DataServer_1</td>
</tr>
<tr>
<td>.A2</td>
<td>WebServer_1</td>
</tr>
</tbody>
</table>

**Displaying accessible groups:**

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

**To display accessible groups:**

At the Switched CDU: prompt, type `list groups` and press Enter.

*Example*

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

```
Switched CDU: 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 Switched CDU: 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:

```
Switched CDU: list group ServerGroup_1<Enter>
```

<table>
<thead>
<tr>
<th>Outlet ID</th>
<th>Outlet Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>.A1</td>
<td>DataServer_1</td>
</tr>
<tr>
<td>.A2</td>
<td>WebServer_1</td>
</tr>
<tr>
<td>.A3</td>
<td>FileServer_1</td>
</tr>
</tbody>
</table>
Displaying accessible serial ports:
The List Ports command displays accessible serial ports for the current user.

*To display accessible serial ports:*
At the Switched CDU: prompt, type `list ports` and press Enter.

**Example**
The follow command displays all accessible serial ports for the current user:

```
Switched CDU: list ports<Enter>
```

<table>
<thead>
<tr>
<th>Port ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Console</td>
</tr>
</tbody>
</table>

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, branch, or phase.

*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:

```
Switched CDU: istat
```

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

Displaying output status:
The OStat command displays the power monitoring status of one or more outlets.

This display includes the outlet absolute and descriptive names and the Outlet Status, current Load, Voltage, and active Power (in Watts) reported to the Sentry by the outlet, branch, or phase.

*To display status of one or more outlets:*
At the Switched CDU: prompt, type `ostat`, followed by an outlet name, or outlet ID, or group name, or `all`, and press Enter, or
Type `ostat`, followed by an outlet name, or outlet ID, or group name, or `all`, followed by `details`, and press Enter.

**Examples**
The following command displays the outlet status of the outlet named FileServer_1:

```
Switched CDU: ostat FileServer_1<Enter>
```

```
Outlet   Outlet                Outlet     Load      Voltage   Power
ID       Name                  Status     (Amps)    (Volts)   (Watts)
.A3      FileServer_1          On          0.00      204.1     0
```

The following command displays the outlet status of all accessible outlets:

```
Switched CDU: ostat all<Enter>
```

```
Outlet   Outlet                Outlet     Load      Voltage   Power
ID       Name                  Status     (Amps)    (Volts)   (Watts)
.AA1     TowerA_PhaseXY_Outlet1 On        1.73      204.1     356
.AA2     TowerA_PhaseXY_Outlet2 On        0.00      204.1     0
.AA3     TowerA_PhaseXY_Outlet3 On        0.00      204.1     0
.AA4     TowerA_PhaseXY_Outlet4 On        0.00      204.1     0
.AA5     TowerA_PhaseXY_Outlet5 On        0.00      204.0     0
.AA6     TowerA_PhaseXY_Outlet6 On        0.00      204.0     0
```
The following command displays the outlet status for outlets in the group ServerGroup_1:

```
Switched CDU: ostat ServerGroup_1<Enter>
Group: ServerGroup_1
```

<table>
<thead>
<tr>
<th>Outlet ID</th>
<th>Name</th>
<th>Status</th>
<th>Load (Amps)</th>
<th>Voltage (Volts)</th>
<th>Power (Watts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.A1</td>
<td>Data_Server_1</td>
<td>On</td>
<td>1.74</td>
<td>205.0</td>
<td>359</td>
</tr>
<tr>
<td>.A2</td>
<td>WebServer_1</td>
<td>On</td>
<td>1.76</td>
<td>206.1</td>
<td>369</td>
</tr>
<tr>
<td>.A3</td>
<td>FileServer_1</td>
<td>On</td>
<td>1.72</td>
<td>204.1</td>
<td>360</td>
</tr>
</tbody>
</table>

The following command displays the detailed POPS outlet values for all accessible outlets:

```
Switched CDU: ostat all details<Enter>
Outlet ID: .A1
```

**Name:** Data_Server_1  
**Outlet Status:** On  
**Control State:** Idle On  
**Load Status:** Normal  
**Capacity (Amps):** 20  
**Load (Amps):** 1.74  
**Voltage (Volts):** 205.6  
**Active Power (Watts):** 361  
**Apparent Power (VA):** 361  
**Crest Factor:** 1.4  
**Power Factor:** 1.00  
**Energy (Watt-Hours):** 172777

More (Y/es N/o):

**Connecting to a serial device:**

The Connect command allows Pass-Thru serial connection to devices attached to the standard serial port (Console).

**To connect to a serial device:**

At the Switched CDU: prompt, type `connect console` and press **Enter**.

**To disconnect from a serial device:**

Type `!*break` and press **Enter**.
Displaying the status of the Environmental Monitor:

The Envmon command displays the status of the integrated Environmental Monitor.

By default, only administrative user accounts are allowed access to the Envmon command. An administrator may use the Set User Envmon command to enable and disable access for other user accounts.

To display the status of the Environmental Monitor:

At the Switched CDU prompt, type `envmon` and press Enter.

Example

The following command displays the status of the Environmental Monitor.

```
Switched CDU: envmon<Enter>
Environmental Monitor .A
    Name: Florida_HQ_1                  Status: Normal
    Temperature/Humidity Sensors
      ID   Name                       Temperature    Humidity
          .A1   Temp_Humid_Sensor_A1       Not Found      Not Found
          .A2   T/H2_Florida_HQ_1          23.5 Deg. C    22 % RH
```

Changing a password:

The Password command changes the current 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 Switched CDU prompt, type `password` and press Enter.

At the Enter Current Password: prompt, type the current password and press Enter.

At the Enter New 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.

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 Switched CDU prompt, type `login` and press Enter. The Username: prompt appears.

Ending a session:

The Quit or Logout commands end 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 Switched CDU prompt, type `quit` and press Enter, or

Type `logout` and press Enter.
Displaying UPS status:

The UPSStat command displays the status of one or more UPS devices associated with the Sentry unit. The display includes UPS index number, type, line/battery status, and reported voltage.

**NOTE:** Access to this command requires enabling user privileges for environmental monitoring using the Set User Envmon command.

**To display status of one or more UPS devices:**

At the Switched CDU: prompt, type `upsstat` and press `Enter`.

**Example**

The following command displays the UPS status:

```
Switched CDU: upsstat<Enter>
```

<table>
<thead>
<tr>
<th>UPS Index</th>
<th>UPS Type</th>
<th>Line/Battery Status</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generic (RFC1628)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>Liebert</td>
<td>On Battery</td>
<td>120.0</td>
</tr>
<tr>
<td>3</td>
<td>MGE</td>
<td>On Utility</td>
<td>119.9</td>
</tr>
</tbody>
</table>

**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 Switched CDU: 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 typed characters - (ASCII 33 to 126 decimal) are allowed; 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:

```
Switched CDU: 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 Switched CDU: 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 Switched CDU: 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:
```
Switched CDU: 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 the following defined access privilege levels; Admin, Power User, User, Reboot-Only, On-Only and View-Only. For more information on user access levels, see Changing a user’s access privilege level: on page 23.

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 Switched CDU: prompt, type `set user access`, followed by `admin`, `poweruser`, `user`, `rebootonly`, `ononly` or `viewonly`, optionally followed by a username and press Enter.

Examples
The following command sets the user access level for JohnDoe to Admin:
```
Switched CDU: set user access admin johndoe<Enter>
```
The following command sets the user access level for JaneDoe to User:
```
Switched CDU: set user access user janedoe<Enter>
```

Granting and removing input load viewing privileges:
The Set User Envmon command grants or removes input status viewing privileges to/from a user.

To grant or remove input load viewing privileges for a user:
At the Switched CDU: 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:
```
Switched CDU: 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 Switched CDU: prompt, type list users and press Enter.

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

```
Switched CDU: list users<Enter>
```

<table>
<thead>
<tr>
<th>User</th>
<th>Privilege</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOHNDOE</td>
<td>Admin</td>
<td>Allowed</td>
</tr>
<tr>
<td>JILLDOE</td>
<td>Power-User</td>
<td>Allowed</td>
</tr>
<tr>
<td>JANEDOE</td>
<td>User</td>
<td>Allowed</td>
</tr>
<tr>
<td>JAKEDOE</td>
<td>Reboot-Only</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>JOSEYDOE</td>
<td>On-Only</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>JOEDOE</td>
<td>View-Only</td>
<td>Not Allowed</td>
</tr>
</tbody>
</table>

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 Switched CDU: 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:

```
Switched CDU: add outlettouser .a1 janedoe<Enter>
Switched CDU: 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 Switched CDU: 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 Switched CDU: 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:

```
Switched CDU: add GroupToUser ServerGroup_1 janedoe<Enter>
Switched CDU: 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 Switched CDU: prompt, type delete GroupFromUser, optionally followed by a group name and a username. Press Enter.

Adding serial port access to a user:
The Add PortToUser command grants a user access to the serial port.

To grant serial port access to a user:
At the Switched CDU: prompt, type add porttouser console and a username. Press Enter.

Deleting serial port access for a user:
The Delete PortFromUser command removes a user’s access to the serial port. You cannot remove access to the serial port
for an administrative level user.

To delete serial port access for a user:
At the Switched CDU: prompt, type delete portfromuser console and a username. Press Enter.

Displaying user outlet, group and serial port access:
The List User command displays all accessible outlets, groups and serial ports for a user.

To display user outlet, group and serial port access:
At the Switched CDU: prompt, type list user, optionally followed by a username. Press Enter.

Example
The following command displays information about the user JaneDoe:

Switched CDU: 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

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, and
Console 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 Switched CDU: prompt, type `set outlet seqinterval all`, followed by a value from 0 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 Switched CDU: 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 Switched CDU: prompt, type `set outlet name` followed by the absolute outlet name, then a descriptive name of up to 24 alphanumeric and other typed characters - (ASCII 33 to 126 decimal) are allowed; 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:

```
Switched CDU: 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 Switched CDU: 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:

```
Switched CDU: 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 Switched CDU: 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 .a5 to 90 seconds:

```
Switched CDU: set outlet postondelay .a5 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 Switched CDU: prompt, type **show outlets** and press Enter.

**Example**

The following command displays all outlet information:

```
Switched CDU: show outlets<Enter>
```

<table>
<thead>
<tr>
<th>Outlet</th>
<th>Name</th>
<th>Wakeup</th>
<th>Post-On</th>
</tr>
</thead>
<tbody>
<tr>
<td>.A1</td>
<td>DataServer_1</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A2</td>
<td>WebServer_1</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A3</td>
<td>FileServer_1</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A4</td>
<td>TowerA_Outlet4</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A5</td>
<td>TowerA_Outlet5</td>
<td>On</td>
<td>90</td>
</tr>
<tr>
<td>.A6</td>
<td>TowerA_Outlet6</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A7</td>
<td>TowerA_Outlet7</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A8</td>
<td>TowerA_Outlet8</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A9</td>
<td>TowerA_Outlet9</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A10</td>
<td>TowerA_Outlet10</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A11</td>
<td>TowerA_Outlet11</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A12</td>
<td>TowerA_Outlet12</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A13</td>
<td>TowerA_Outlet13</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A14</td>
<td>TowerA_Outlet14</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A15</td>
<td>TowerA_Outlet15</td>
<td>On</td>
<td>0</td>
</tr>
<tr>
<td>.A16</td>
<td>TowerA_Outlet16</td>
<td>On</td>
<td>0</td>
</tr>
</tbody>
</table>

More (Y/es N/o):

Outlet Options:

- Sequence Interval: 2 seconds
- Reboot Delay: 15 seconds

Input Feed Administration

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 47 for more information on the Show Traps command.

To create a infeed name:

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

**Example**

The following command adds the descriptive name HQ_1_Infeed_A to the infeed on the Switched CDU:

```
Switched CDU: set infeed name .aa HQ_1_Infeed_A<Enter>
```

Setting the infeed operational voltage

The Set Infeed Voltage command is use to edit the input operational voltage.

To set the infeed operational voltage:

At the Switched CDU: prompt, type **set infeed voltage**, followed by the absolute infeed name, and a value from 0 to 480. Press Enter.

**Example**

The following commands sets the operational voltage for input .AA to 100V:

```
Switched CDU: set infeed voltage .aa 100<Enter>
```
Setting the infeed maximum load capacity

The Set Infeed LoadMax command is use to edit the input maximum load capacity.

To set the infeed maximum load capacity:
At the Switched CDU: prompt, type `set infeed loadmax`, followed by the absolute infeed name, and a value from 1 to 255 (in amperes). Press Enter.

Example
The following commands sets the maximum load capacity for input .AA to 15 amperes:

```
Switched CDU: set infeed loadmax .aa 15<Enter>
```

Displaying infeed information:

The Show Infeeds command displays information about all infeeds. This information includes the absolute and descriptive infeed names, operational voltages and maximum load capacities.

To display tower information:
At the Switched CDU: prompt, type `show infeeds` and press Enter.

Example

```
Switched CDU: show infeeds<Enter>
```

<table>
<thead>
<tr>
<th>Input</th>
<th>Feed Name</th>
<th>Feed Voltage</th>
<th>Feed Capacity (Amps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.AA</td>
<td>HQ_1_Infeed_A</td>
<td>100</td>
<td>15</td>
</tr>
<tr>
<td>.AB</td>
<td>HQ_1_Infeed_B</td>
<td>120</td>
<td>20</td>
</tr>
<tr>
<td>.BA</td>
<td>HQ_2_Infeed_A</td>
<td>120</td>
<td>30</td>
</tr>
<tr>
<td>.BB</td>
<td>HQ_2_Infeed_B</td>
<td>120</td>
<td>30</td>
</tr>
</tbody>
</table>

Tower Administration

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 47 for more information on the Show Traps command.

To create a tower name:
At the Switched CDU: prompt, type `set tower name` followed by the absolute tower name, then a descriptive name of up to 24 alphanumeric and other typed characters - (ASCII 33 to 126 decimal) are allowed; spaces are not allowed. Press Enter.

Example
The following command adds the descriptive name Florida_HQ_1 to tower .a:

```
Switched CDU: set tower name .a Florida_HQ_1<Enter>
```

Setting the tower serial number:

The Set Tower ProdSN command is use to set the product serial number.

NOTE: If set at the factory, the serial number WILL NOT be user-editable.

To set the tower serial number:
At the Switched CDU: prompt, type `set tower prodsn`, followed by the absolute tower name, and the tower serial number. Press Enter.

Example
The following command sets the serial number for tower .A to ‘AA06F011157’:

```
Switched CDU: set tower prodsn .a AA06F011157<Enter>
```
Setting the tower model number:
The Set Tower Model command is used to set the product model number.

NOTE: If set at the factory, the model number WILL NOT be user-editable.

To set the tower model number:
At the Switched CDU: prompt, type `set tower model`, followed by the absolute tower name, and the tower model number. Press Enter.

Example
The following command sets the model number for tower .A to ‘CW-8H1-C20’:

```
Switched CDU: set tower prodsn .a CW-8H1-C20<Enter>
```

Setting the tower AC or DC voltage type:
The Set Tower command is used to set the product input AC or DC voltage type.

NOTE: If set at the factory, the voltage type WILL NOT be user-editable.

To set the tower AC/DC voltage type:
At the Switched CDU: prompt, type `set tower`, followed by `ac` or `dc`, and the absolute tower name. Press Enter.

Example
The following command sets the AC/DC voltage type for tower .A to AC:

```
Switched CDU: set tower ac.a<Enter>
```

Setting the tower AC voltage type:
The Set Tower 3phase command is used to set the product input AC voltage type.

NOTE: If set at the factory, the voltage type WILL NOT be user-editable.

To set the tower AC voltage type:
At the Switched CDU: prompt, type `set tower 3phase`, followed by the absolute tower name and `yes` or `no`. Press Enter.

Example
The following command sets the AC voltage type for tower .A to non-3-phase:

```
Switched CDU: set tower 3phase.a no<Enter>
```

Displaying tower information:
The Show Towers command displays information about the Sentry. This information includes the absolute and descriptive Sentry names, serial and model numbers, and voltage types.

To display tower information:
At the Switched CDU: prompt, type `show towers` and press Enter.

Example
```
Switched CDU: show towers<Enter>
Tower ID:       .A
Name:         TowerA
Product S/N:  AA06F011157
Model No.:    CW-8H1-C20
3-Phase:      No
Power Type:   AC

More (Y/es N/o):
```
Group Administration

Creating a group name:
The Create Group command creates a new group name.

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

Example
The following command creates group name ServerGroup_1:
Switched CDU: create group ServerGroup_1<Enter>

Removing a group name:
The Remove Group command removes a group name.

To remove a group name:
At the Switched CDU: prompt, type remove group, optionally followed by a username. Press Enter.

Example
The following command removes group name ServerGroup_1:
Switched CDU: 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 Switched CDU: 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:
Switched CDU:add OutletToGroup .a1 ServerGroup_1<Enter>
Switched CDU: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:
Switched CDU:add OutletToGroup DataServer_1 ServerGroup_1<Enter>
Switched CDU:add OutletToGroup WebServer_1 ServerGroup_1<Enter>
The following command add all outlets to group name ServerGroup_1:
Switched CDU: 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 Switched CDU: 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.
Environmental Monitor Administration

Creating a descriptive Environmental Monitor name:

The Set Envmon Name command assigns a descriptive name to the integrated Environmental Monitor. This descriptive name is displayed when the Evnmon command is issued.

To create an Environmental Monitor name:

At the Switched CDU: prompt, type `set envmon name` followed by the absolute environmental monitor name, then the descriptive name of up to 24 alphanumeric and other typed characters - (ASCII 33 to 126 decimal) are allowed; spaces are not allowed. Press Enter.

Example

The following command adds the descriptive name Florida_HQ_1 to the Environmental Monitor:

```
Switched CDU: set envmon name .a Florida_HQ_1<Enter>
```

Creating a descriptive temperature/humidity sensor name:

The Set Envmon THS Name command assigns a descriptive name to a temperature/humidity sensor. This descriptive name is displayed when the Evnmon command is issued.

To create an temperature/humidity sensor name:

At the Switched CDU: prompt, type `set envmon ths name` followed by the absolute name of the temperature/humidity sensor, then the descriptive name of up to 24 alphanumeric and other typed characters - (ASCII 33 to 126 decimal) are allowed; spaces are not allowed. Press Enter.

Example

The following command adds the descriptive name T/H2_Florida_HQ_1 to the second temperature/humidity sensor:

```
Switched CDU: set envmon ths name .a2 T/H2_Florida_HQ_1<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 Switched CDU: prompt, type `set port name` followed by the absolute outlet name, then a descriptive name of up to 24 alphanumeric and other typed characters - (ASCII 33 to 126 decimal) are allowed; spaces are not allowed; port names are not case sensitive. Press Enter.

Example

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

```
Switched CDU: 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 Switched CDU: 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:

```
Switched CDU: set port speed 38400<Enter>
```

Enabling or disabling active signal checking for serial connections:

The Set Port DSR Check command enables or disables active signal checking for serial connections to devices attached to any of the available serial ports.

To enable or disable active signal checking for serial connections:

At the Switched CDU: prompt, type `set port dsrcheck console, on or off, and press 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 Switched CDU: prompt, type set port timeout, followed by a value from 0 to 5 (in minutes) and press Enter.

Displaying serial port information:
The Show Ports command displays information about all serial ports. This information includes:
- Serial port data rate
- Descriptive port name, if applicable
- DSR signal checking settings

To display serial port information:
At the Switched CDU: prompt, type show ports and press Enter.

Example
The following command displays all serial port information:
Switched CDU: show ports<Enter>
Serial Port Configuration
ALL Ports:
  Baud Rate: 38400      Connection Timeout: 5 minutes
  Port ID: Console      Port Name: CONSOLE
  DSR Check: ON

System Administration
Creating a pre-login banner:
The Set Banner command specifies text that appears prior to the login authentication. This feature allows administrators to configure a message up to 2070 characters for display of legal, disclaimer or other text as required by application. If left blank, the user will be taken directly to the login prompt.

NOTE: For SSH sessions, the “keyboard-interactive” authentication method must be used for the banner to display.

To create a pre-login banner:
At the Switched CDU: prompt, type set banner and press Enter. Type the desired pre-login banner text and when finished type Ctrl-z.
Creating a location description:

The Set Location command specifies text that appears in the Web 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 Switched CDU: prompt, type `set location` followed by a descriptive name of up to 24 alphanumeric and other typed characters - (ASCII 33 to 126 decimal) are allowed; 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:

```
Switched CDU: set location Florida HQ<Enter>
```

The following command deletes any previously specified location description:

```
Switched CDU: 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 system area value:

The Set System Area command specifies the numeric value for the system area that is used to calculate total system watts per area unit.

To set the system area:

At the Switched CDU: prompt, type `set system area`, followed by a value from 0.0-100.0, and press Enter.

Example:

The following command sets the system area to 95.5:

```
Switched CDU: set system area 95.5<Enter>
```

Setting the system area unit of measure:

The Set System Area Unit command sets the value for the system area in either square meters or square feet. The default unit of area is a square meter.

To set the system area unit of measure:

At the Switched CDU: prompt, type `set system areauunit`, followed by `squaremeter` or `squarefoot`, and press Enter.

Setting the power factor:

The Set System PF command sets the power factor used in the total system power calculation. The valid range is .50 to 1.00.

To set the power factor:

At the Switched CDU: prompt type `set system pf`, followed by the power factor, and press Enter.

Setting the 3-phase load out-of-balance threshold:

The Set System Balance command sets the percent load out-of-balance threshold for 3-phase systems.

To set the 3-phase load out-of-balance threshold:

At the Switched CDU: prompt, type `set system balance`, followed by the load out-of-balance threshold (in percent), and press Enter.

Example:

The following command sets the 3-phase load out-of-balance threshold to 15%.

```
Switched CDU: set system balance 15<Enter>
```
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
- System area, input power factor and 3-phase load out-of-balance threshold.

See Chapter 4: Advanced Operations on page 67 for more information on SNMP.

To display system configuration information:

At the Switched CDU: prompt, type `show system` and press Enter.

Example

```
System Information
  F/W Version:           Sentry Version 6.0a
  NIC S/N:               1600001
  MAC Address:           00-0a-9c-10-00-01
  H/W Rev Code:          0
  Flash Size:            2 MB
  Uptime:                0 days 6 hours 14 minutes 1 second
  Location:              Florida HQ
  Area <Footprint>:      6.3 square feet
  Power Factor:          0.80
  3-Phase Load
      Out-of-Balance Threshold: 20 percent
```

Displaying system power status:

The System Status command displays all power status information.

To display system power status:

At the Switched CDU: prompt, type `sysstat` and press Enter.

Example

```
Switched CDU: sysstat

System Power Status
  Total Power Consumption: 170 Watts
  Area <Footprint>: 100.0 Square Meters
  Watts Per Area Unit: 2 Watts Per Square Meter
```

Setting the LED display orientation:

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

To set the LED display orientation:

At the Switched CDU: prompt, type `set option display`, followed by `normal` or `inverted` and press Enter.

Example

```
The following set the LED display orientation to Inverted:

Switched CDU: set option display inverted<Enter>
```

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

Enabling or disabling strong passwords:

The Set Option Strong Password command is used to enable or disable the requirements for strong passwords. When enabled, all new passwords must be a minimum of 8 characters in length with at least one uppercase letter, one lowercase letter, one number and one special character.

To enable or disable strong passwords:

At the Switched CDU: prompt, type `set option strong password`, followed by `enabled` or `disabled` and press Enter.
Enabling or disabling the external configuration reset button:
The Set Option Button command enables or disables the external configuration reset button. This feature can enhance system security by protecting the Sentry configurations from being reset locally.

NOTE: If this feature has been enabled and the administrative account username/password has been lost, then the Sentry must be returned to the factory for non-warranty reset of the configuration.

To enable or disable the configuration reset button:
At the Switched CDU: prompt, type `set option button`, followed by `enabled` or `disabled` and press `Enter`.

Enabling or disabling the ‘more’ prompt:
The Set Option More command enables or disables the ‘more’ prompt for display of data larger than the terminal window.

To enable or disable ‘more’:
At the Switched CDU: prompt, type `set option more`, followed by `enabled` or `disabled` and press `Enter`.

Setting the temperature scale:
The Set Option TempScale command sets the temperature scale that the Sentry will report in.

To set the temperature scale:
At the Switched CDU: prompt, type `set option tempscale`, followed by `celsius` or `fahrenheit` and press `Enter`.

Configuring the Command Line Interface (CLI) session timeout:
The Set Option CLI Timeout command configures the CLI session timeout in minutes. The valid timeout range is 1 to 1440 minutes (24 hours). The default session timeout is 5 minutes.

To configure the CLI Session Timeout:
At the Switched CDU: prompt, type `set option clitimeout`, followed by the session timeout (in minutes), and press `Enter`.

Example:
The following command sets the CLI session timeout to 15 minutes:

```
Switched CDU: set option clitimeout 15<Enter>
```

Configuring the web session (Web Interface) timeout:
The Set Option Web Timeout command configures the Web session timeout in minutes. The valid timeout range is 1 to 1440 minutes (24 hours). The default session timeout is 5 minutes.

To configure the web session timeout:
At the Switched CDU: prompt, type `set option webtimeout`, followed by the session timeout (in minutes), and press `Enter`.

Example:
The following command sets the web session (Web Interface) timeout to 10 minutes:

```
Switched CDU: set option webtimeout 10<Enter>
```

To enable or disable coldboot alert:
Upon a coldboot of the system (if the Coldboot Alert feature is enabled), the system sends a ½ second RS-232 break out on any serial ports that are also enabled.
The Set Option Coldboot Alert command enables or disables the Coldboot Alert feature.

To enable or disable coldboot alert:
At the Switched CDU: prompt, type `set option cbalert`, followed by `enabled` or `disabled`, and press `Enter`.
Displaying system options:
The Show Options command displays all system option information.

To display system option information:
At the Switched CDU: prompt, type show options and press Enter.

Example
    Sentry: show options
    System Options
        Display Orientation: NORMAL
        Strong Passwords: DISABLED
        Configuration Reset Button: ENABLED
        More Prompt: ENABLED
        Temperature Scale: CELSIUS
        CLI Session Timeout: 10 minutes
        Web Session Timeout: 10 minutes
        Coldboot Alert <SCP>: DISABLED

Displaying the Sentry firmware version:
The Version command displays the Sentry firmware version.

To display the firmware version:
At the Switched CDU: 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 Switched CDU: 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 57 for more information.

Enabling or disabling DHCP support:
The Set DHCP command enables or disables DHCP support.

To enable or disable DHCP support:
At the Switched CDU: prompt, type set dhcp, followed by enabled or disabled and press Enter.

Setting the IP address:
The Set Ipaddress command sets the TCP/IP address of the network interface controller.

To set the IP address:
At the Switched CDU: 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:
    Switched CDU: 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 Switched CDU: 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
```
Switched CDU: 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 Switched CDU: 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:
```
Switched CDU: 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 Switched CDU: 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:
```
Switched CDU: 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 67 for more information on SNMP and Remote Authentication

To display network configuration information:
At the Switched CDU: prompt, type `show network` and press Enter.

Example
The following command displays the network configuration information:
```
Switched CDU: 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  Auth:  Password, Kb-Int
  HTTP:  Enabled  Port:  80  Security:  BASIC
  SSL:  Enabled
  SNMP:  Enabled
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 57 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 Switched CDU: 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 Switched CDU: prompt, type set http port, followed by the port number and press Enter.

Example
The following changes the HTTP port number to 2048:

Switched CDU: 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 20.

To set the HTTP authentication method:
At the Switched CDU: 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 57 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 Switched CDU: 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 Switched CDU: prompt, type set telnet port, followed by the port number and press Enter.

Example
The following changes the Telnet port number to 7001:

Switched CDU: 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 address:

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

To set the FTP Host address:

At the Switched CDU: prompt, type set ftp host, followed by the IP address or hostname and press Enter.

Examples

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

```
Switched CDU: set ftp host 12.34.56.99<Enter>
```

The following command sets the FTP hostname to ftp.servertech.com:

```
Switched CDU: set ftp host ftp.servertech.com<Enter>
```

Setting the FTP username:

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

To set the FTP username:

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

Example

The following command sets the FTP username to Guest:

```
Switched CDU: set ftp username guest<Enter>
```

Setting the FTP Password:

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

To set the FTP password:

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

Example

The following command sets the FTP password to ABC_123:

```
Switched CDU: set ftp password ABC_123<Enter>
```

Setting the filename to be uploaded:

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

To set the FTP filename:

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

Example

The following command sets the FTP filename to swcdu-v60g.bin:

```
Switched CDU: set ftp filename swcdu-v60g.bin<Enter>
```

Setting the directory for the file to be uploaded:

The Set FTP Directory command sets the directory for the firmware file to be uploaded.

To set the FTP directory:

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

Example

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

```
Sentry: set ftp directory ftp://sentry<Enter>
```
Enabling or disabling automatic updates:
The Set FTP Autoupdate command is used to enable or disable automatic firmware update support.

To enable or disable automatic updates:
At the Switched CDU: prompt, type `set ftp autoupdate`, followed by `enabled` or `disabled` and press `Enter`.

Setting the automatic update scheduled day:
The Set FTP Autoupdate Day command is used to set the day when automatic updates occur.

To set the automatic update day:
At the Switched CDU: prompt, type `set ftp autoupdate day`, followed by a day of the week or `everyday` and press `Enter`.

Example
The following command sets the automatic update day to Sunday:
```
Switched CDU: set ftp autoupdate day sunday<Enter>
```

Setting the automatic update scheduled hour:
The Set FTP Autoupdate Hour command is used to set the hour of the day when automatic updates occur.

To set the automatic update hour:
At the Switched CDU: prompt, type `set ftp autoupdate hour`, followed by an hour of the day and press `Enter`.

Examples
The following command sets the automatic update hour to 12 AM:
```
Switched CDU: set ftp autoupdate hour 12am<Enter>
```
The following command sets the automatic update hour to 3 PM:
```
Switched CDU: set ftp autoupdate hour 3pm<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 Switched CDU: prompt, type `show ftp` and press `Enter`.

Example
The following command displays the FTP configuration information:
```
Switched CDU: show ftp<Enter>
FTP Configuration
  Host:       ftp.servertech.com
  Username:   guest
  Password:   ********
  Directory:  ftp://sentry
  Filename:   swcdav60g.bin
FTP Automatic Updates Configuration
  Automatic Updates: 12.34.56.99
  Scheduled Day: Sunday
  Scheduled Hour: 3 PM
```
**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 Switched CDU: prompt, type `set snntp`, followed by `primary` or `secondary`, and the SNTP server IP address or hostname. Press **Enter**.

**Examples**

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

```
Switched CDU: set snntp primary 204.152.184.72<Enter>
```

The following command sets the secondary SNTP server address to cuckoo.nevada.edu:

```
Switched CDU: set snntp secondary cuckoo.nevada.edu<Enter>
```

**Setting the local GMT offset:**

The Set SNTP GMToffset command is used to set the offset from GMT for the date/time returned by SNTP. The offset can be configured in whole hours between -12 and 12 hours.

**NOTE:** The Sentry does not support automatic adjustment for daylight savings.

*To set the local GMT offset:*

At the Switched CDU: prompt, type `set snntp gmtoffset`, followed by the offset value, and press **Enter**.

**Examples**

The following command sets the local GMT offset to -12:

```
Switched CDU: set snntp gmtoffset -12<Enter>
```

**Displaying SNTP configuration information:**

The Show SNTP command displays all SNTP configuration information.

*To display SNTP configuration information*

At the Switched CDU: prompt, type `show snntp` and press **Enter**.

**Example**

The following command displays the SNTP configuration information:

```
Switched CDU: show snntp <Enter>
  Date/Time (Local GMT Offset -12): 2006-02-21  21:32:48
  Primary Host:    204.152.184.72
  Secondary Host:  cuckoo.nevada.edu
```
UPS Administration

Creating a UPS record:

The Create UPS command adds a new UPS device to the Sentry unit.

To create a UPS record:

At the Switched CDU: prompt, type `create UPS` and press Enter.

At the prompt, type the corresponding number from the list of the UPS types and press Enter.

At the Host Name: prompt, type the UPS’s IP address or hostname and press Enter.

Example

The following command creates a UPS record for a Toshiba UPS with the hostname ‘DC1Toshiba1’:

```
Switched CDU: create ups<Enter>
  UPS types:
  1 -- APC
  2 -- Liebert
  3 -- MGE
  4 -- Tripp Lite
  5 -- Generic (RFC1628)
  6 -- Hewlett Packard
  7 -- Minuteman
  8 -- Mitsubishi
  9 -- Powerware
  10 -- Toshiba
  Select type(1-10): 10<Enter>
  Host/IP: DC1Toshiba1<Enter>
```

Removing a UPS record:

The Remove UPS command removes a UPS record.

To remove a UPS record:

At the Switched CDU: prompt, type `remove ups` and press Enter.

At the prompt, type the index number of the UPS to be removed and press Enter.

Example

The following command removes the UPS record at index 3:

```
Switched CDU: remove ups<Enter>
  1 Type: Liebert
      Host/IP: DC1Liebert1
  2 Type: Powerware
      Host/IP: DC1Powerware1
  3 Type: Toshiba
      Host/IP: DC1Toshiba1
  Select UPS(1-8): 3<Enter>
```
Changing the UPS type:
The Set UPS Type command is used to change the type of UPS for each UPS record.

To change a UPS record:
At the Switched CDU: prompt, type set ups type and press Enter.
At the prompt, type the index number for the UPS record to be changed and press Enter.
At the prompt, type the corresponding number from the list of the UPS types and press Enter.

Example
The following command changes UPS type for the record at index number 2 to ‘MGE’:

```
Switched CDU: set ups type<Enter>
1   Type: Liebert
    Host/IP: DC1Liebert1
2   Type: Powerware
    Host/IP: DC1Powerware1
Select UPS(1-8): 2<Enter>
UPS types:
1 -- APC
2 -- Liebert
3 -- MGE
4 -- Tripp Lite
5 -- Generic (RFC1628)
6 -- Hewlett Packard
7 -- Minuteman
8 -- Mitsubishi
9 -- Powerware
10 -- Toshiba
Select type(1-10): 3<Enter>
```

Changing the UPS host address:
The Set UPS Host command is used to change the IP address or hostname for each UPS record. Hostnames may be up to 60 characters long.

To change a UPS host address:
At the Switched CDU: prompt, type set ups host and press Enter.
At the prompt, type the index number for the UPS record to be changed and press Enter.
At the prompt, type IP address or hostname for the UPS and press Enter.

Example
The following command changes UPS hostname for the record at index number 2 to ‘DC1MGE1’:

```
Switched CDU: set ups host<Enter>
1   Type: Liebert
    Host/IP: DC1Liebert1
2   Type: MGE
    Host/IP: DC1Powerware1
Select UPS(1-8): 2<Enter>
Host/IP: DC1MGE1<Enter>
```
Changing the UPS SNMP port:

With a UPS record configured, the Sentry sends data requests to the default UPS SNMP port number 161. This port number may be changed using the Set UPS Port command.

To change the UPS SNMP port:

At the Switched CDU: prompt, type set ups port and press Enter.

At the prompt, type the index number for the UPS record to be changed and press Enter.

At the prompt, type the desired port number and press Enter.

Example

The following command changes port for the UPS record at index number 1 to ‘162’:

Switched CDU: set ups port<Enter>

UPS     UPS
Index   Type         Port
1       Liebert      161
2       MGE          161
Select UPS(1-8): 1<Enter>
Port: 162<Enter>

Changing the UPS SNMP Get community string:

With a UPS record configured, the Sentry sends data requests to the UPS using the default Get community string of ‘public’. This string may be changed using the Set UPS Port command.

NOTE: The GET community string configured on the Sentry MUST match the read-only community string configured on the UPS.

To change a UPS record:

At the Switched CDU: prompt, type set ups getcomm and press Enter.

At the prompt, type the index number for the UPS record to be changed and press Enter.

At the prompt, type the Get community string for the UPS and press Enter.

Example

The following command changes Get community string for the record at index number 2 to ‘readonly’:

Switched CDU: set ups getcomm<Enter>

UPS     UPS          Community
Index   Type         String
1       Liebert      public
2       MGE          public
Select UPS(1-8): 2<Enter>
Community String: readonly<Enter>

Enabling/disabling UPS voltage polling:

With a UPS record configured, the Sentry by default enables voltage polling of the UPS. This feature may be enabled or disabled using the Set UPS VPoll command.

To enable/ disable UPS voltage polling:

At the Switched CDU: prompt, type set ups vpoll and press Enter.

At the prompt, enter the index number for the UPS record to be changed and press Enter.

At the prompt, type on or off, and press Enter.

Example

The following command disables voltage polling for the record at index number 2:

Switched CDU: set ups vpoll<Enter>

UPS     UPS          Voltage
Index   Type         Polling
1       Liebert      On
2       MGE          On
Select UPS(1-8): 2<Enter>
Voltage Polling: Off<Enter>
Adding an infeed to a UPS:
The Set UPS AddInfeed command adds a logical association of an infeed to a UPS.

To add an infeed to a UPS:
At the Switched CDU: prompt, type set ups addinfeed and press Enter.
At the prompt, enter the index number for the UPS record to be changed and press Enter.
At the prompt, type the absolute infeed ID of the desired infeed, and press Enter.

Example
The following command associates infeed .aa to UPS record at index number 1:

```
Switched CDU: set ups addinfeed<Enter>
UPS     UPS          Infeed
Index   Type         IDs
1       Liebert     .AA
2       MGE         
Select UPS(1-8): 1<Enter>
Infeed ID: .aa<Enter>
```

Removing an infeed from a UPS:
The Set UPS DelInfeed command removes a logical association of an infeed from a UPS.

To remove an infeed from a UPS:
At the Switched CDU: prompt, type set ups delinfeed and press Enter.
At the prompt, enter the index number for the UPS record to be changed and press Enter.
At the prompt, type the absolute infeed ID of the desired infeed, and press Enter.

Example
The following command removes the association of infeed .aa from UPS record at index number 2:

```
Switched CDU: set ups delinfeed<Enter>
UPS     UPS          Infeed
Index   Type         IDs
1       Liebert     .AA
2       MGE         .AA
Select UPS(1-8): 2<Enter>
Infeed ID: .aa<Enter>
```
Displaying UPS configuration:
The Show UPS command displays information about all UPS devices.

- UPS Type and Host/IP address
- UPS SNMP port and community string
- SNMP Objects OID values and expected return values

To display UPS configuration information:
At the Switched CDU: prompt, type `show ups` and press Enter.

Example
The following command displays UPS configuration information:

```
Switched CDU: show ups<Enter>
  1   Type:    Liebert
        Host/IP: DC1Liebert1
        Voltage Polling: ON
        SNMP Configuration
        Community String: public
        SNMP Port:        162
        SNMP Objects/Expected Values
        Voltage:          .1.3.6.1.2.1.33.1.4.4.1.2.1
        Utility Status:   .1.3.6.1.2.1.33.1.4.1.0
        On Battery:       0x5
        On Utility:       0x3

More (Y/Es N/o):
```

Feature Administration

Displaying activated special features:
The Show Features command displays all activated special features for the device.

To display activated special features:
At the Switched CDU: prompt, type `show features` and press Enter.

Example
The following command displays all activated special features:

```
Switched CDU: show features<Enter>
Activated Features:
    Smart Load Shedding
```

NOTE: A restart of the Sentry is required after activating new special features.
# Chapter 4: Advanced Operations

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>68</td>
</tr>
<tr>
<td>Enabling and Setting up SSL Support</td>
<td>68</td>
</tr>
<tr>
<td>SSL Technical Specifications</td>
<td>68</td>
</tr>
<tr>
<td>SSH</td>
<td>69</td>
</tr>
<tr>
<td>Enabling and Setting up SSH Support</td>
<td>69</td>
</tr>
<tr>
<td>SSH Technical Specifications</td>
<td>70</td>
</tr>
<tr>
<td>SNMP/Thresholds</td>
<td>71</td>
</tr>
<tr>
<td>MIB, OID and Support</td>
<td>71</td>
</tr>
<tr>
<td>Enabling and Setting up SNMP Support</td>
<td>71</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>73</td>
</tr>
<tr>
<td>Configuring Traps</td>
<td>76</td>
</tr>
<tr>
<td>LDAP</td>
<td>80</td>
</tr>
<tr>
<td>Enabling and Setting up LDAP Support</td>
<td>81</td>
</tr>
<tr>
<td>Configuring LDAP Groups</td>
<td>85</td>
</tr>
<tr>
<td>LDAP Technical Specifications</td>
<td>89</td>
</tr>
<tr>
<td>TACACS+</td>
<td>90</td>
</tr>
<tr>
<td>Enabling and Setting up TACACS+ Support</td>
<td>90</td>
</tr>
<tr>
<td>Configuring TACACS+ Privilege Levels</td>
<td>92</td>
</tr>
<tr>
<td>TACACS+ Technical Specifications</td>
<td>95</td>
</tr>
<tr>
<td>RADIUS</td>
<td>96</td>
</tr>
<tr>
<td>Enabling and Setting Up RADIUS Support</td>
<td>96</td>
</tr>
<tr>
<td>Sentry Vendor-Specific RADIUS Attributes:</td>
<td>98</td>
</tr>
<tr>
<td>LOGGING</td>
<td>100</td>
</tr>
<tr>
<td>Internal System Log</td>
<td>100</td>
</tr>
<tr>
<td>Syslog</td>
<td>100</td>
</tr>
<tr>
<td>Email</td>
<td>101</td>
</tr>
<tr>
<td>UPLOAD/DOWNLOAD</td>
<td>104</td>
</tr>
<tr>
<td>Sentry Integrated FTP Server</td>
<td>104</td>
</tr>
<tr>
<td>FTP Configuration Files</td>
<td>104</td>
</tr>
<tr>
<td>Upload/Download Process</td>
<td>105</td>
</tr>
<tr>
<td>REMOTE SHUTDOWN</td>
<td>106</td>
</tr>
<tr>
<td>Supported Operating Systems</td>
<td>107</td>
</tr>
<tr>
<td>Shutdown Agent Installation</td>
<td>107</td>
</tr>
<tr>
<td>Enabling and Setting up Remote Shutdown Support</td>
<td>108</td>
</tr>
</tbody>
</table>
Secure Socket Layers (SSL) version 3 enables secure Web 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set SSL</td>
<td>Enables/disables SSL support</td>
</tr>
<tr>
<td>Set SSL Access</td>
<td>Sets SSL access as optional or required</td>
</tr>
</tbody>
</table>

### 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 57 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 Switched CDU: 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 Switched CDU: prompt, type `set ssl access`, followed `optional` or `required`, and press `Enter`.

**Example**

The following changes the access level to required:

Switched CDU: 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`
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set SSH</td>
<td>Enables/disables SSH support</td>
</tr>
<tr>
<td>Set SSH AuthMethod</td>
<td>Enables/disables the SSH server authentication methods</td>
</tr>
<tr>
<td>Set SSH Port</td>
<td>Sets the SSH server port number</td>
</tr>
</tbody>
</table>

### 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 57 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 Switched CDU: 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 Switched CDU: prompt, type `set ssh port`, followed by the port number and press *Enter*.

**Example**

The following changes the SSH port number to 65535:

```
Switched CDU: set ssh port 65535<Enter>
```

#### Enabling or disabling SSH server authentication methods:

The Set SSH Authentication Method command is used to set the method of SSH server authentication. The Sentry SSH server supports two authentication methods for security and validation: Password and Keyboard-Interactive.

For more information on the SSH server authentication methods, see *Enabling or disabling SSH server authentication methods* on page 19.

**To enable the SSH authentication methods:**

At the Switched CDU: prompt, type `set ssh authmethod`, followed by `password` or `kbint`, followed by `enabled` or `disabled`, and press *Enter*.

**Example**

The following example sets the SSH authentication method to keyboard-interactive:

```
Switched CDU: set ssh authmethod kbint enabled<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
- AES192-CBC
- AES128-CBC
- RIJNDAEL256-CBC
- RIJNDAEL192-CBC
- RIJNDAEL128-CBC
- 3DES-192-CBC
- BLOWFISH-128-CBC
- ARCFOUR-128

**Message Integrity:**
- HMAC-SHA1-160
- HMAC-MD5-128
- HMAC-SHA1-96
- HMAC-MD5-96

**Authentication:**
- Username/Password

**Session Channel Break Extension (for RS232 Break)**
SNMP/Thresholds

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 25, for information on enabling and configuring SNMP.

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

<table>
<thead>
<tr>
<th>SNMP Command Summary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set SNMP</td>
<td>Enables or disables SNMP support</td>
</tr>
<tr>
<td>Set SNMP Getcomm</td>
<td>Sets the ‘get’ community string</td>
</tr>
<tr>
<td>Set SNMP Setcomm</td>
<td>Sets the ‘set’ community string</td>
</tr>
<tr>
<td>Set SNMP Trapdest</td>
<td>Sets a destination IP address or hostname for traps</td>
</tr>
<tr>
<td>Set SNMP Traptime</td>
<td>Sets the delay for steady state condition traps</td>
</tr>
<tr>
<td>Set SNMP IPRestrict</td>
<td>Allows SNMP GET and SET requests from defined traps destinations only</td>
</tr>
<tr>
<td>Show SNMP</td>
<td>Displays all SNMP configuration information</td>
</tr>
</tbody>
</table>

MIB, OID and Support

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


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

For SNMP Support, email: mibmaster@servetech.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 Switched CDU: 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 57 for more information.

Setting trap destinations:

The Set SNMP Trapdest1 and Trapdest2 commands are used to set the IP addresses or hostname 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 Switched CDU: prompt, type `set snmp`, `trapdest1` or `trapdest2`, the Ipaddress or hostname and press Enter.

Examples

The following sets the trap destination 1 to 64.42.31.208:

```
Switched CDU: set snmp trapdest1 64.42.31.208<Enter>
```

The following sets the trap destination 2 to snmp.servetech.com:

```
Switched CDU: set snmp trapdest2 snmp.servetech.com<Enter>
```

To reset the trap destination:

At the Switched CDU: prompt, type `set snmp`, `trapdest1` or `trapdest2`, `0.0.0.0` and press Enter.
Setting the trap timer:
The Set SNMP Traptime 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 Switched CDU: prompt, type `set snmp traptime`, followed by the timer period and press Enter.

Example
The following sets the timer period to 180 seconds:

```
Switched CDU: set snmp traptime 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 Switched CDU: 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 Switched CDU: prompt, type `set snmp getcomm`, followed by the string and press Enter.

Setting SNMP IP Restrictions:
The Set SNMP IP Restrictions command supports SNMP Manager GET and SET requests to only be allowed from the IP addresses of the defined traps destinations.

To set SNMP IP Restrictions:
At the Switched CDU: prompt, type `set snmp iprestrict trapdests` and press Enter.

To remove SNMP IP Restrictions:
At the Switched CDU: prompt, type `set snmp iprestrict none` and press Enter.

Setting the SNMP SysName:
The Set SNMP SysName command is used to set the SNMP MIB-II SysName object.

To set the SysName object:
At the Switched CDU: prompt, type `set snmp sysname`, followed by the object name and press Enter.

Setting the SNMP SysLocation:
The Set SNMP SysLocation command is used to set the SNMP MIB-II SysLocation object.

To set the SysLocation object:
At the Switched CDU: prompt, type `set snmp syslocation`, followed by the object location and press Enter.

Setting the SNMP SysContact:
The Set SNMP SysContact command is used to set the SNMP MIB-II SysContact object.

To set the SysContact object:
At the Switched CDU: prompt, type `set snmp syscontact`, followed by the object contact 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 Switched CDU: 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 Switched CDU: prompt, type `show snmp` and press Enter.

Example
The following command displays the SNMP configuration information:

```
Switched CDU: show snmp<Enter>
SNMP Configuration
SNMP: Enabled
GET Community String: public
SET Community String: private
TRAP Community String: trap
Error Trap Repeat Time (seconds): 180 seconds
Trap Destination 1: 64.42.31.208
Trap Destination 2: snmp.servertech.com
IP Restrictions: Trap Destinations Only
SysName: No Name
SysLocation: No Location
SysContact: No Contact
```

SNMP Traps
The Switched CDU supports five types of SNMP traps. Traps are enabled at the Tower (T), Infeed (I), outlet (O), Environmental Monitor (E) or sensor (S) level.

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Level(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>T, I, O, E, S</td>
<td>Operational status change</td>
</tr>
<tr>
<td>Change</td>
<td>O</td>
<td>Control status change</td>
</tr>
<tr>
<td>Load</td>
<td>I</td>
<td>Input load out of limit</td>
</tr>
<tr>
<td>Temp</td>
<td>S</td>
<td>Temperature is out of range</td>
</tr>
<tr>
<td>Humid</td>
<td>S</td>
<td>Relative Humidity is out of range</td>
</tr>
</tbody>
</table>
```

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td></td>
<td>Tower is working correctly</td>
</tr>
<tr>
<td>NoComm</td>
<td>x</td>
<td>Communication to the tower has been lost</td>
</tr>
</tbody>
</table>

## Infeed Status traps

<table>
<thead>
<tr>
<th>Status</th>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td></td>
<td>Infeed is on</td>
</tr>
<tr>
<td>OffError</td>
<td>x</td>
<td>Infeed should be on but no current is sensed at the infeed</td>
</tr>
<tr>
<td>NoComm</td>
<td>x</td>
<td>Communication to the infeed has been lost</td>
</tr>
</tbody>
</table>

## Outlet Status traps

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

## Environmental Monitor Status traps

<table>
<thead>
<tr>
<th>Status</th>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td></td>
<td>Environmental Monitor is working correctly</td>
</tr>
<tr>
<td>NoComm</td>
<td>x</td>
<td>Communication to the Environmental Monitor has been lost</td>
</tr>
</tbody>
</table>

## Temperature/Humidity Sensor Status traps

<table>
<thead>
<tr>
<th>Status</th>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found</td>
<td></td>
<td>The sensor has been detected</td>
</tr>
<tr>
<td>NotFound</td>
<td></td>
<td>No sensor has been detected</td>
</tr>
<tr>
<td>Lost</td>
<td>x</td>
<td>Sensor initially detected but communication to the sensor has been lost</td>
</tr>
<tr>
<td>NoComm</td>
<td>x</td>
<td>Communication to the sensor has been lost</td>
</tr>
</tbody>
</table>

**NOTE:** Traps are generated according to a hierarchical architecture, for example, if an Tower Status enters a trap condition, only the Tower Status trap will be generated. Infeed, Outlet, Environmental Monitor or Sensor Status and Temp and Humid traps will be 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**

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

Temp Trap

The Temp trap is generated whenever the temperature on a temperature/humidity sensor is beyond preset thresholds. Temp traps include the reported temperature, temp status, Location of the Sentry, and identifier and name of the affected sensor.

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

**Temp traps**

<table>
<thead>
<tr>
<th>Status</th>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td></td>
<td>The sensor is working correctly and the temperature is within preset thresholds</td>
</tr>
<tr>
<td>NotFound</td>
<td></td>
<td>No sensor has been detected</td>
</tr>
<tr>
<td>Reading</td>
<td></td>
<td>Temp status currently being read</td>
</tr>
<tr>
<td>TempLow</td>
<td>x</td>
<td>Temperature at the sensor below preset low threshold</td>
</tr>
<tr>
<td>TempHigh</td>
<td>x</td>
<td>Temperature at the sensor exceeds preset high threshold</td>
</tr>
<tr>
<td>ReadError</td>
<td>x</td>
<td>Unable to read Temp status</td>
</tr>
<tr>
<td>Lost</td>
<td>x</td>
<td>Sensor initially detected but communication to the sensor has been lost</td>
</tr>
<tr>
<td>NoComm</td>
<td>x</td>
<td>Communication to the sensor has been lost</td>
</tr>
</tbody>
</table>

Humidity Trap

The Humidity trap is generated whenever the humidity on a temperature/humidity sensor is beyond preset thresholds. Humidity traps include the reported relative humidity, humidity status, Location of the Sentry, and identifier and name of the affected sensor.

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

**Humidity traps**

<table>
<thead>
<tr>
<th>Status</th>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td></td>
<td>The sensor is working correctly and the relative humidity is within preset thresholds</td>
</tr>
<tr>
<td>NotFound</td>
<td></td>
<td>No sensor has been detected</td>
</tr>
<tr>
<td>Reading</td>
<td></td>
<td>Humidity status currently being read</td>
</tr>
<tr>
<td>HumidLow</td>
<td>x</td>
<td>Relative humidity at the sensor below preset low threshold</td>
</tr>
<tr>
<td>HumidHigh</td>
<td>x</td>
<td>Relative humidity at the sensor exceeds preset high threshold</td>
</tr>
<tr>
<td>ReadError</td>
<td>x</td>
<td>Unable to read Humidity status</td>
</tr>
<tr>
<td>Lost</td>
<td>x</td>
<td>Sensor initially detected but communication to the sensor has been lost</td>
</tr>
<tr>
<td>NoComm</td>
<td>x</td>
<td>Communication to the sensor has been lost</td>
</tr>
</tbody>
</table>
## Configuring Traps

### SNMP Trap Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Trap Tower Status</td>
<td>Enables or disables the Tower Status trap</td>
</tr>
<tr>
<td>Set Trap Infeed Status</td>
<td>Enables or disables the Infeed Status trap off</td>
</tr>
<tr>
<td>Set Trap Infeed Load</td>
<td>Enables or disables the Infeed Load trap</td>
</tr>
<tr>
<td>Set Trap Infeed HighThresh</td>
<td>Sets the Infeed Load trap high limit</td>
</tr>
<tr>
<td>Set Trap Outlet Change</td>
<td>Enables or disables the Outlet Change trap</td>
</tr>
<tr>
<td>Set Trap Outlet Status</td>
<td>Enables or disables the Outlet Status trap</td>
</tr>
<tr>
<td>Set Trap EM Status</td>
<td>Enables or disables the Environmental Monitor Status trap</td>
</tr>
<tr>
<td>Set Trap THS Status</td>
<td>Enables or disables a temperature/humidity sensor Status trap</td>
</tr>
<tr>
<td>Set Trap THS Temp</td>
<td>Enables or disables a temperature/humidity sensor Temp trap</td>
</tr>
<tr>
<td>Set Trap THS Temp Delta</td>
<td>Sets temperature recovery delta</td>
</tr>
<tr>
<td>Set Trap THS Temphigh</td>
<td>Sets a temperature/humidity sensor Temp trap high limit</td>
</tr>
<tr>
<td>Set Trap THS Templow</td>
<td>Sets a temperature/humidity sensor Temp trap low limit</td>
</tr>
<tr>
<td>Set Trap THS Humid</td>
<td>Enables or disables a temperature/humidity sensor Humid trap</td>
</tr>
<tr>
<td>Set Trap THS Humidhigh</td>
<td>Sets a temperature/humidity sensor Humid trap high limit</td>
</tr>
<tr>
<td>Set Trap THS Humidlow</td>
<td>Sets a temperature/humidity sensor Humid trap low limit</td>
</tr>
<tr>
<td>Show Traps</td>
<td>Displays trap configurations</td>
</tr>
</tbody>
</table>

### 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 Switched CDU: prompt, type `set trap (tower, infeed, outlet, em or ths) status`, followed by the tower, infeed or outlet name, and `on` or `off`. Press Enter, or:

Type `set trap (tower, infeed, outlet, em or ths) 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:

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

The following command enables the Status trap for the tower named Florida_HQ_1:

```
Switched CDU: 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 Switched CDU: 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:

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

The following command disables the Load trap for all infeeds:

```
Switched CDU: 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 Switched CDU: 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:

```
Switched CDU: 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 Switched CDU: 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:

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

Enabling or Disabling the Temp trap:
The Set Trap THS Temp command is used to enable or disable the Temp trap.

To Enable or Disable the Temp trap:
At the Switched CDU: prompt, type `set trap ths temp`, followed by the sensor name and `on` or `off`. Press `Enter`.

Example
The following command enables the Temp trap for the first temperature-humidity sensor:

```
Switched CDU: set trap ths temp .a1 on<Enter>
```

Setting the Temperature sensor threshold limits:
The Set Trap THS Templow and Set Trap THS Temphigh commands are used to set the lower and upper threshold limits for the Temperature sensor.

To set the Temperature threshold limits:
At the Switched CDU: prompt, type `set trap ths templow` or `temphigh`, followed by the sensor name and a value from 0 to 123 in degrees Celsius. Press `Enter`.

Example
The following command sets the second temperature high threshold limit to 95:

```
Switched CDU: set trap ths temphigh .a2 95<Enter>
```
Configuring Temperature Recovery Delta:

The Temperature Recovery Delta command allows configuration of the number of degrees of change needed to recover from a temperature alarm.

For more information about the Temperature Recovery Delta, see Configuring Temperature Recovery Delta: on page 26.

To configure the temperature recovery delta:

At the Switched CDU: prompt, type `set event temp tempdelta`, followed by the sensor name, the number of degrees for the recovery delta, and press Enter.

Example

The following command configures the recovery delta at 2 degrees Fahrenheit for temperature/humidity sensor .A1:

```
Switched CDU: event temp tempdelta temp_humid_sensor_A1 2<Enter>
```

Enabling or Disabling the Humid trap:

The Set Trap THS Humid command is used to enable or disable the Humid trap.

To Enable or Disable the Humid trap:

At the Switched CDU: prompt, type `set trap ths humid`, followed by the sensor name and on or off. Press Enter.

Example

The following command enables the Humid trap for the first temperature-humidity sensor:

```
Switched CDU: set traps ths humid .a1 on<Enter>
```

Setting the Humidity sensor threshold limits:

The Set Trap THS Humidlow and Set Trap THS Humidhigh commands are used to set the lower and upper threshold limits for the Humidity sensor.

To set the Humidity threshold limits:

At the Switched CDU: prompt, type `set trap ths humidlow` or `humidhigh`, followed by the sensor name and a value from 0 to 100 in percent relative humidity. Press Enter.

Example

The following command sets the first humidity sensor low threshold limit to 5:

```
Switched CDU: set trap ths humidlow .a1 5<Enter>
```
Displaying trap configuration information:

The Show Traps command displays information about all traps.

**To display trap information:**

At the Switched CDU: prompt, type `show traps` and press Enter.

**Example**

The following command requests trap configuration information:

```
Switched CDU: show traps <Enter>
```

**Tower trap configuration:**

<table>
<thead>
<tr>
<th>Tower ID</th>
<th>Tower Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>.A</td>
<td>Florida_HQ_1</td>
<td>ON</td>
</tr>
<tr>
<td>.B</td>
<td>Florida_HQ_2</td>
<td>ON</td>
</tr>
</tbody>
</table>

More (Y/es N/o): y

**Input feed trap configuration:**

<table>
<thead>
<tr>
<th>Feed ID</th>
<th>Feed Name</th>
<th>Status</th>
<th>Load</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>.AA</td>
<td>HQ_1_Infeed_A</td>
<td>ON</td>
<td>ON</td>
<td>255  A</td>
</tr>
<tr>
<td>.BA</td>
<td>HQ_2_Infeed_A</td>
<td>ON</td>
<td>ON</td>
<td>255  A</td>
</tr>
</tbody>
</table>

More (Y/es N/o): y

**Outlet trap configuration:**

<table>
<thead>
<tr>
<th>Outlet ID</th>
<th>Outlet Name</th>
<th>Status</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>.AA1</td>
<td>DataServer_1</td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AA2</td>
<td>WebServer_1</td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AA3</td>
<td>FileServer_1</td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AA4</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AA5</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AA6</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AA7</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AA8</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AB1</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AB2</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AB3</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AB4</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AB5</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AB6</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AB7</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>.AB8</td>
<td></td>
<td>ON</td>
<td>OFF</td>
</tr>
</tbody>
</table>

More (Y/es N/o): y

Environmental Monitor .A trap configuration:

**Temperature/Humidity Sensor ** .A1

- **Name:** Temp_Humid_Sensor_A1
- **Status Trap:** ON
- **Temp Trap:** ON
  - Low: 31 Deg.F
  - High: 253 Deg.F
  - Delta: 5 Deg.F
- **Humid Trap:** ON
  - Low: 5 % RH
  - High: 100 % RH

**Temperature/Humidity Sensor ** .A2

- **Name:** T/H2_Florida_HQ_1
- **Status Trap:** ON
- **Temp Trap:** ON
  - Low: 32 Deg.F
  - High: 253 Deg.F
  - Delta: 2 Deg.F
- **Humid Trap:** ON
  - Low: 0 % RH
  - High: 100 % RH
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 LDAP support has been tested in the following environments:

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

### LDAP Command Summary

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

Setting the LDAP host address:

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

To set the LDAP host address:
At the Switched CDU: prompt, type set ldap, followed by host1 or host2 and the Directory Services server’s IP address or hostname. Press Enter.

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

Switched CDU: set ldap host1 98.76.54.32<Enter>

The following command sets the secondary Directory Services server hostname to ldap.servertech.com:

Switched CDU: set ldap host2 ldap.servertech.com<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 Switched CDU: 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:

Switched CDU: set ldap port 8888<Enter>

Enabling and disabling LDAP over TLS/SSL support:

The Set LDAP UseTLS command is used to enable or disable LDAP over TLS/SSL support.

To enable or disable LDAP over TLS/SSL support:
At the Switched CDU: prompt, type set ldap usetls, followed by yes or no and press Enter.

NOTE: If LDAP Over TLS/SSL is enabled, MD5 binding is disabled.
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 uses 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 20."

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 Switched CDU: prompt, type `set ldap bind`, followed by `simple` or `md5` and press Enter.

NOTE: If MD5 binding is enabled, LDAP over TLS/SSL is disabled.

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 Switched CDU: 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’:

Switched CDU: 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 Switched CDU: 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 Switched CDU: 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’:

Switched CDU: 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 Switched CDU: prompt, type `set ldap grouptype` followed by `DN` or `Name` and press `Enter`.

Example

The following sets group membership value to DN

```
Switched CDU:  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 Switched CDU: 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':

```
Switched CDU: 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 Switched CDU: 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’:

```
Switched CDU:  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 Switched CDU: 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 Switched CDU: prompt, type `show ldap` and press **Enter**.

**Example**

The following command displays the LDAP configuration information:

```
Switched CDU: show ldap
LDAP Configuration
    LDAP:    Enabled
    Host 1:  98.76.54.32
    Host 2:  ldap.servertech.com
    Port:    8888
    TLS/SSL: Yes
    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 58.

To set the DNS IP address:
At the Switched CDU: 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:

```
Switched CDU: 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 Switched CDU: 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:

```
Switched CDU: 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 Switched CDU: 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:

```
Switched CDU: create ldapgroup PowerUser<Enter>
```

Removing an LDAP group:
The Remove LDAPGroup command removes an LDAP group.

To remove an LDAP group:
At the Switched CDU: 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 level privileges; Admin, User, On-Only and View-Only. For more information on user access levels, see Changing a user’s access privilege level: on page 23.

To set the access level privilege for an LDAP group:
At the Switched CDU: 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:

Switched CDU: set ldapgroup access admin ldapadmin<Enter>

The following command sets the LDAP group access level for PowerUser to User:

Switched CDU: 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 Switched CDU: 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:

Switched CDU: 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 Switched CDU: prompt, type list ldapgroups and press Enter.

Example
The following command displays all LDAP groups with their access privilege level:

Switched CDU: list ldapgroups<Enter>

<table>
<thead>
<tr>
<th>LDAP Group Name</th>
<th>Access Level</th>
<th>Environmental Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAPAdmin</td>
<td>Admin</td>
<td>Allowed</td>
</tr>
<tr>
<td>PowerUser</td>
<td>User</td>
<td>Allowed</td>
</tr>
<tr>
<td>User</td>
<td>On-Only</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>Guest</td>
<td>View-Only</td>
<td>Not Allowed</td>
</tr>
</tbody>
</table>

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 Switched CDU: prompt, type add outlettolistap, optionally followed by an outlet name and a group name. Press Enter, or

Type add outlettolistap 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:

Switched CDU: add outlettolistap .a1 poweruser<Enter>
Switched CDU: add outlettolistap 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 Switched CDU: 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 grant outlet group access to an LDAP Group:
At the Switched CDU: 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:

```
Switched CDU: add grouptoldap servergroup_1 poweruser<Enter>
Switched CDU: 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 Switched CDU: 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 Switched CDU: 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 Switched CDU: prompt, type delete portfromldap console and a group name. Press Enter.
Displaying LDAP Group access:

The List LDAPGroup command displays all access rights for an LDAP group.

To display LDAP Group access:

At the Switched CDU: prompt, type list ldapgroup, optionally followed by a group name. Press Enter.

Example

The following command displays information about the LDAP group PowerUser:

```
Switched CDU: 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

LDAP Authentication Process

**Simple Bind Authentication Process**

<table>
<thead>
<tr>
<th>Client</th>
<th>LDAP Server</th>
<th>Sentry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate Sentry session</td>
<td>Prompt for login credentials</td>
<td></td>
</tr>
<tr>
<td>Authentication request with Username/Password</td>
<td>Simple bind using Search Bind DN &amp; Password</td>
<td></td>
</tr>
<tr>
<td>Username found?</td>
<td>Simple Bind using User FQDN and login password</td>
<td></td>
</tr>
<tr>
<td>Access Denied</td>
<td>Attribute name compared to Group Membership Attribute</td>
<td></td>
</tr>
<tr>
<td>Username found?</td>
<td>Username groups access rights compared against Sentry LDAP groups</td>
<td></td>
</tr>
<tr>
<td>Attribute match?</td>
<td>Group match?</td>
<td></td>
</tr>
<tr>
<td>Attribute name compared to Group Membership Attribute</td>
<td>Access Denied</td>
<td></td>
</tr>
<tr>
<td>Username found?</td>
<td>Attribute match?</td>
<td></td>
</tr>
<tr>
<td>Access Denied</td>
<td>Group match?</td>
<td></td>
</tr>
<tr>
<td>Access Granted</td>
<td>Username groups access rights compared against Sentry LDAP groups</td>
<td></td>
</tr>
<tr>
<td>Attribute name compared to Group Membership Attribute</td>
<td>Access Denied</td>
<td></td>
</tr>
<tr>
<td>Username found?</td>
<td>Attribute match?</td>
<td></td>
</tr>
<tr>
<td>Access Denied</td>
<td>Group match?</td>
<td></td>
</tr>
<tr>
<td>Access Granted</td>
<td>Username groups access rights compared against Sentry LDAP groups</td>
<td></td>
</tr>
</tbody>
</table>

**MD5 Bind Authentication Process**

<table>
<thead>
<tr>
<th>Client</th>
<th>LDAP Server</th>
<th>Sentry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate Sentry session</td>
<td>Prompt for login credentials</td>
<td></td>
</tr>
<tr>
<td>Authentication request with Username/Password</td>
<td>Simple bind using Search Bind DN &amp; Password</td>
<td></td>
</tr>
<tr>
<td>Username found?</td>
<td>Simple Bind using User FQDN and login password</td>
<td></td>
</tr>
<tr>
<td>Access Denied</td>
<td>Attribute name compared to Group Membership Attribute</td>
<td></td>
</tr>
<tr>
<td>Username found?</td>
<td>Username groups access rights compared against Sentry LDAP groups</td>
<td></td>
</tr>
<tr>
<td>Attribute match?</td>
<td>Group match?</td>
<td></td>
</tr>
<tr>
<td>Attribute name compared to Group Membership Attribute</td>
<td>Access Denied</td>
<td></td>
</tr>
<tr>
<td>Username found?</td>
<td>Attribute match?</td>
<td></td>
</tr>
<tr>
<td>Access Denied</td>
<td>Group match?</td>
<td></td>
</tr>
<tr>
<td>Access Granted</td>
<td>Username groups access rights compared against Sentry LDAP groups</td>
<td></td>
</tr>
<tr>
<td>Attribute name compared to Group Membership Attribute</td>
<td>Access Denied</td>
<td></td>
</tr>
<tr>
<td>Username found?</td>
<td>Attribute match?</td>
<td></td>
</tr>
<tr>
<td>Access Denied</td>
<td>Group match?</td>
<td></td>
</tr>
<tr>
<td>Access Granted</td>
<td>Username groups access rights compared against Sentry LDAP groups</td>
<td></td>
</tr>
<tr>
<td>Attribute name compared to Group Membership Attribute</td>
<td>Access Denied</td>
<td></td>
</tr>
<tr>
<td>Username found?</td>
<td>Attribute match?</td>
<td></td>
</tr>
<tr>
<td>Access Denied</td>
<td>Group match?</td>
<td></td>
</tr>
<tr>
<td>Access Granted</td>
<td>Username groups access rights compared against Sentry LDAP groups</td>
<td></td>
</tr>
</tbody>
</table>

**LDAPS (LDAP-over-TLS/SSL) Client Specifications**

Secure Sockets Layer (SSL) version 3
Transport Layer Security (TLS) version 1 (RFC 2246)
x.509 version 3 Server Certificates (RFC 2459) with RSA key sizes up to 4096 bits
Symmetric Cryptography Ciphers:
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (168-bit)
- TLS_RSA_WITH_DEX_CBC_SHA (56-bit)
- TLS_RSA_WITH_AES_128_CBC_SHA (128-bit)
- TLS_RSA_WITH_AES_256_CBC_SHA (256-bit)
Server certificates are accepted and used on-the-fly
A NULL client certificate is sent to the server if a client certificate is requested

---

Installation and Operations Manual

Advanced Operations • 89
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Authorder</td>
<td>Specifies the authentication order for each new session attempt</td>
</tr>
<tr>
<td>Set TACACS</td>
<td>Enables/disables TACACS support</td>
</tr>
<tr>
<td>Set TACACS Host</td>
<td>Sets the IP address or hostname of the TACACS server</td>
</tr>
<tr>
<td>Set TACACS Key</td>
<td>Sets the TACACS encryption key</td>
</tr>
<tr>
<td>Set TACACS Port</td>
<td>Sets the TACACS server port number</td>
</tr>
<tr>
<td>Show TACACS</td>
<td>Displays TACACS configurations</td>
</tr>
<tr>
<td>Add GroupToTACACS</td>
<td>Grants a TACACS account access to one or more groups</td>
</tr>
<tr>
<td>Add OutletToTACACS</td>
<td>Grants a TACACS account access to one or more outlets</td>
</tr>
<tr>
<td>Add PortToTACACS</td>
<td>Grants a TACACS account access to one or more serial ports</td>
</tr>
<tr>
<td>Delete GroupFromTACACS</td>
<td>Removes access to one or more groups for a TACACS account</td>
</tr>
<tr>
<td>Delete OutletToTACACS</td>
<td>Removes access to one or more outlets for a TACACS account</td>
</tr>
<tr>
<td>Delete PortFromTACACS</td>
<td>Removes access to one or more serial ports for a TACACS account</td>
</tr>
<tr>
<td>Set TacPriv Access</td>
<td>Sets the access level for a TACACS account</td>
</tr>
<tr>
<td>Set TacPriv Envmon</td>
<td>Grants or removes privileges to view input and environmental monitoring status</td>
</tr>
<tr>
<td>List TacPrvs</td>
<td>Displays access levels for all TACACS accounts</td>
</tr>
<tr>
<td>List TacPriv</td>
<td>Displays all accessible outlet/groups/ports for a TACACS account</td>
</tr>
</tbody>
</table>

### 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 Switched CDU: prompt, type `set tacacs`, followed by `enabled` or `disabled` and press Enter.
**Setting the TACACS+ server address:**
The Set TACACS Host command sets the IP address or hostname of the TACACS+ server.

*To set the TACACS+ server address:*
At the Switched CDU: prompt, type `set tacacs`, followed by `host1` or `host2` and the TACACS+ server’s IP address or hostname.  Press Enter.

**Examples**
The following command sets the primary TACACS+ server address to 98.76.54.32:
```
Switched CDU: set tacacs host1 98.76.54.32<Enter>
```
The following command sets the secondary TACACS+ server hostname to tacacs.servertech.com:
```
Switched CDU: set tacacs host2 tacacs.servertech.com<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 Switched CDU: prompt, type `set tacacs key` and press Enter.
At the TACACS+ Key: prompt, type an encryption key of up to 60 alphanumeric and other typed characters - (ASCII 33 to 126 decimal) are allowed; encryption keys are case sensitive. Press Enter. To specify no password, press Enter.
At the Verify TACACS+ Key: prompt, retype the key.  Press Enter. To verify no password, press Enter at the prompt.

**Example**
```
Switched CDU: 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.

**Changing the TACACS port:**
With TACACS support enabled, the Sentry sends TACACS requests to the default TACACS port number 49.  This port number may be changed using the Set TACACS Port command.

*To change the TACACS port:*
At the Switched CDU: prompt, type `set tacacs port`, followed by the port number and press Enter.

**Example**
The following changes the TACACS port number to 50:
```
Switched CDU: set tacacs port 50<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 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 Switched CDU: 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.

**To display the TACACS configuration information:**
At the Switched CDU: prompt, type `show tacacs` and press Enter.

**Example**
The following command displays the TACACS configuration information:

```
Switched CDU: show tacacs<Enter>
TACACS+ Configuration
    TACACS+:       Enabled
    Host 1:        98.76.54.32
    Host 2:        tacacs.servertech.com
    Port:          50
    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 23.

**To set the access level privilege for a TACACS+ account:**
At the Switched CDU: 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:

```
Switched CDU: set tacpriv access admin 14<Enter>
```

The following command sets the TACACS+ account access level for account 5 to User:

```
Switched CDU: 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 Switched CDU: 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:
```
Switched CDU: 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 Switched CDU: prompt, type list tacprvs and press Enter.

Example
The following command displays all TACACS+ account with their access privilege level:
```
Switched CDU: list tacprvs<Enter>
```

<table>
<thead>
<tr>
<th>TACACS</th>
<th>Access</th>
<th>Environmental</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>Level</td>
<td>Monitoring</td>
</tr>
<tr>
<td>TACAdmin</td>
<td>Admin</td>
<td>Allowed</td>
</tr>
<tr>
<td>PowerUser</td>
<td>User</td>
<td>Allowed</td>
</tr>
<tr>
<td>User</td>
<td>On-Only</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>Guest</td>
<td>View-Only</td>
<td>Not Allowed</td>
</tr>
</tbody>
</table>

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 Switched CDU: 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:
```
Switched CDU:add outlettotacacs .a1 5<Enter>
Switched CDU: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 Switched CDU: 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 Switched CDU: 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:

```
Switched CDU: add grouptotacacs servergroup_1 5<Enter>
Switched CDU: 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 Switched CDU: prompt, type `delete groupfromtacacs`, optionally followed by an 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 Switched CDU: 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 Switched CDU: prompt, type `delete portfromtacacs console` and a TACACS+ account number. Press Enter.

Displaying TACACS account access:

The List TacPriv command displays all access rights for a TACACS+ account.

To display TACACS account access:

At the Switched CDU: prompt, type `list tacpriv`, optionally followed by a TACACS+ account. Press Enter.

Example

The following command displays information about the TACACS+ account 1:

```
Switched CDU: list tacpriv 1<Enter>
TACACS+ Privilege Level: 1
Outlet    Outlet
ID        Name
A1        DataServer_1
A2        WebServer_1
Groups:
    ServerGroup_1
    ServerGroup_2
More (Y/es N/o): Y
Ports:
    Port ID    Port Name
    Console    Console
```

Members of the TACACS privilege level 1 account 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.
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_xxxxx’ (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_xxxxx’ (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.
The Sentry family of products supports the Remote Authentication Dial-in User Service (RADIUS) protocol. RADIUS provides a centralized network protocol to enable remote authentication and authorization, such as user names and passwords. With a central RADIUS 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 RADIUS server), a set of necessary RADIUS privilege levels and user access rights for each level.

RADIUS is also used in enterprise-wide networks because it provides the administrator with high performance, less memory usage, less CPU cycles on routers and switches, and an open standard that is easily interoperable within the network.

In addition to the protocol-required attributes, the RADIUS authentication process can be extended by using private vendor-specific attributes (VSA). This extension allows Server Technology to create its own proprietary attributes to support features and services using the Sentry CDU in the RADIUS authentication process.

### RADIUS Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Authorder</td>
<td>Specifies the authentication order for each new session attempt</td>
</tr>
<tr>
<td>Set RADIUS</td>
<td>Enables or disables RADIUS support</td>
</tr>
<tr>
<td>Set RADIUS … Server</td>
<td>Configures the address of the RADIUS server</td>
</tr>
<tr>
<td>Set RADIUS … Secret</td>
<td>Sets the shared secret for the RADIUS server</td>
</tr>
<tr>
<td>Set RADIUS … Port</td>
<td>Sets the port number of the RADIUS server</td>
</tr>
<tr>
<td>Set RADIUS … Timeout</td>
<td>Configures the timeout interval for the RADIUS server</td>
</tr>
<tr>
<td>Set RADIUS … Retries</td>
<td>Sets the number of retries for the RADIUS server</td>
</tr>
<tr>
<td>Show RADIUS</td>
<td>Displays RADIUS configuration settings</td>
</tr>
</tbody>
</table>

### Enabling and Setting Up RADIUS Support

The following configuration tasks are required to properly enable and set up RADIUS support on the primary and secondary RADIUS servers.

**Enabling and disabling RADIUS support:**

The Set RADIUS command enables or disables RADIUS support.

*To enable or disable RADIUS support:*

At the Switched CDU: prompt, type `set radius`, followed by `enabled` or `disabled`, and press 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 RADIUS server, and, if unsuccessful, then attempts authentication with the local user database on the Sentry device.

The Remote Only method attempts authentication only with the RADIUS server, and, if unsuccessful, access is denied.

*NOTE: With the Remote Only method, if authentication fails due to a communication failure with the RADIUS server automatic authentication fallback will occur to authenticate with the local user database on the Sentry device.*

*To set the authentication order:*

At the Switched CDU: 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 RADIUS has been fully configured and tested.*
Setting the RADIUS server address:
The Set RADIUS Server command sets the IP address or hostname of the primary or secondary server used for RADIUS authentication requests.

To set the RADIUS server address:
At the Switched CDU: prompt, type `set radius`, followed by `primary` or `secondary`, followed by `server`, and the RADIUS server’s IP address or hostname (maximum 63 characters). Press Enter.

Examples
The following command sets the primary RADIUS server address to 98.76.54.32:

```
Switched CDU: set radius primary server 98.76.54.32<Enter>
```

The following command sets the secondary RADIUS server address to radius.servertech.com:

```
Switched CDU: set radius secondary server radius.servertech.com<Enter>
```

Setting the RADIUS secret:
The Set RADIUS Secret command sets the shared secret for the server used for RADIUS authentication requests.

To set the shared secret:
At the Switched CDU: prompt, type `set radius`, followed by `primary` or `secondary`, and followed by `secret`. Press Enter. Enter the shared secret and press Enter. For security, shared secret characters are not displayed.

Changing the RADIUS port number:
The Set RADIUS Port command sets the server port number for RADIUS authentication requests.

To change the port number:
At the Switched CDU: prompt, type `set radius`, followed by `primary` or `secondary`, followed by `port`, and the port number (1-65535). Press Enter.

The default is 1812.

Example
The following command sets the secondary RADIUS server port number to 1855:

```
Switched CDU: set radius secondary port 1855<Enter>
```

Setting the RADIUS timeout value:
The Set RADIUS Timeout command sets the time interval to wait for a reply from the RADIUS server before resending the authentication request.

To set the timeout value:
At the Switched CDU: prompt, type `set radius`, followed by `primary` or `secondary`, followed by `timeout`, and the time interval in seconds (1-30). Press Enter.

Examples
The following command sets the primary RADIUS server timeout value to 15 seconds:

```
Switched CDU: set radius primary timeout 15<Enter>
```

The following command sets the secondary RADIUS server timeout value to 5 seconds:

```
Switched CDU: set radius secondary timeout 5<Enter>
```
Setting the number of RADIUS server retries:

The Set RADIUS Retries command specifies the number of times an authentication request is sent to the RADIUS server. The Sentry will attempt authentication with the primary server until the number of retries is reached, then will attempt authentication with the secondary server. If the Sentry does not receive a response from these attempts, the authentication request will be rejected.

To set the number of retries:

At the Switched CDU: prompt, type `set radius`, followed by `primary` or `secondary`, followed by `retries`, and followed by the number of retries (0-10). Press Enter.

Examples

The following command sets the retries for the primary RADIUS server to 5:

```
Switched CDU: set radius primary retries 5<Enter>
```

The following command sets the retries for the secondary RADIUS server to 2:

```
Switched CDU: set radius secondary retries 2<Enter>
```

Displaying RADIUS configuration information:

The Show RADIUS command displays RADIUS configuration information.

To display the RADIUS configuration information:

At the Switched CDU: prompt, type `show radius` and press Enter.

Example

The following command displays the RADIUS configuration information:

```
Switched CDU: show radius<Enter>
```

RADIUS Configuration

<table>
<thead>
<tr>
<th>RADIUS:</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Order:</td>
<td>Remote-&gt;Local</td>
</tr>
<tr>
<td>Primary Server:</td>
<td></td>
</tr>
<tr>
<td>Shared Secret:</td>
<td>****</td>
</tr>
<tr>
<td>Port:</td>
<td>1812</td>
</tr>
<tr>
<td>Timeout:</td>
<td>15 seconds</td>
</tr>
<tr>
<td>Retries:</td>
<td>5</td>
</tr>
</tbody>
</table>

Secondary Server:

| Shared Secret: |         |
| Port:          | 1855    |
| Timeout:       | 5 seconds |
| Retries:       | 2       |
Vendor-Specific Attributes (VSA):

Server Technology has defined and formatted RADIUS vendor-specific attributes (VSA) in the `dictionary.sti` file, which is available from Server Technology. The Sentry device is configured to recognize and use the configuration values in the file as specified by the network administrator, indicating to the RADIUS server that the defined attributes are based on Server Technology’s unique enterprise vendor code.

Using the format from in the `dictionary.sti` file, the Sentry RADIUS implementation supports the following vendor-specific attributes:

**Vendor-Specific Attribute (VSA) Descriptions**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STI-Access-Level</td>
<td>Indicates user access level for the Switched CDU; values are 1-6 as follows; a valid access level is required or access to the CDU is denied.</td>
</tr>
<tr>
<td></td>
<td>Valid Access Levels:&lt;br&gt;1 = Admin&lt;br&gt;2 = Power User&lt;br&gt;3 = User&lt;br&gt;4 = Reboot Only&lt;br&gt;5 = On Only&lt;br&gt;6 = View Only</td>
</tr>
<tr>
<td>STI-Env-Mon</td>
<td>Determines user access rights to environmental monitoring; values are Yes or No. For the STI-Access-Level value other than 1 (Admin), if STI-Env-Mon is not included for a user, default is no.</td>
</tr>
<tr>
<td>STI-Outlets</td>
<td>Specifies user access rights to outlets; values are space-delimited strings of absolute IDs, names, or the special keyword &quot;ALL&quot;. String values are case-sensitive and limited to 253 characters. This attribute can be repeated to append strings that declare additional access rights. For STI-Access Level values other than 1 (Admin) and 2 (Power User), if STI-Outlets is not included for a user, the default is no outlet.</td>
</tr>
<tr>
<td>STI-Groups</td>
<td>Specifies user access rights to groups of outlets; values are space-delimited strings of absolute IDs, names, or the special keyword &quot;ALL&quot;. String values are case-sensitive and limited to 253 characters. This attribute can be repeated to append strings that declare additional access rights. For STI-Access Level values other than 1 (Admin) and 2 (Power User), if STI-Groups is not included for a user, the default is no group.</td>
</tr>
<tr>
<td>STI-Ports</td>
<td>Specifies user access rights to ports; values are space-delimited strings of absolute IDs, names, or the special keyword &quot;ALL&quot;. String values are case-sensitive and limited to 253 characters. This attribute can be repeated to append strings that declare additional access rights. For STI-Access Level values other than 1 (Admin) and 2 (Power User), if STI-Ports is not included for a user, the default is no ports.</td>
</tr>
</tbody>
</table>

**NOTE:** User access levels must be configured using the `dictionary.sti` file. If the administrator does not use the `dictionary.sti` file to configure a user, the user will not have access rights to the Sentry CDU.

**Examples:**

**Administrator with full access and configuration rights:**

```
sti-admin Auth-Type := Local, User-Password == "admin"  
STI-Access-Level = Admin 
```

**Power user with environmental monitoring allowed and full outlet/group/port access rights:**

```
sti-power Auth-Type := Local, User-Password == "power"  
STI-Access-Level = Power-User, 
STI-Env-Mon = Yes 
```

**User with environmental monitoring not allowed and specific outlet/group/port access rights:**

```
sti-user Auth-Type := Local, User-Password == "user"  
STI-Access-Level = User, 
STI-Env-Mon = No, 
STI-Outlets = ".A1 .A2 Rtr1 Rtr2 Srvr1 Srvr2", 
STI-Outlets += ".A3 .A4 Rtr3 Rtr4 Srvr3 Srvr4", 
STI-Groups = "Routers Servers", 
STI-Ports = "Console" 
```

**View-only user with environmental monitoring allowed and all outlet and group access rights:**

```
sti-view Auth-Type := Local, User-Password == "view"  
STI-Access-Level = View-Only, 
STI-Env-Mon = Yes, 
STI-Outlets = "ALL", 
STI-Groups = "ALL" 
```
Logging

The Sentry family of products supports logging of system events both internally and externally. An internal log of more than 4000 events is automatically maintained and is reviewable by administrative users. For permanent/long-term log storage, Sentry supports the Syslog protocol. And for immediate notification, Sentry supports Email notifications.

Log entries include a sequential entry number, a date/time stamp and an event message. The event message is preceded with a message ‘type’ heading and if the event is tied to a user, the username will be included.

NOTE: For date/time stamp support, SNTP server support must be configured. For information on SNTP, see page 25.

The Sentry supports the following event message headers:

- **AUTH:** All authentication attempts.
- **POWER:** All power state change requests.
- **CONFIG:** All system configuration changes.
- **EVENT:** All general system events. Example: over/under threshold event.

Internal System Log

The internal system log is stored in the local memory and has support for up to 4097 continuously aging entries. The internal system log is only available to administrative users. For instructions on reviewing the internal log, see page 31.

Syslog

The Sentry’s Syslog support is RFC3164-compliant and enables off-Sentry viewing and storage of log messages. The Sentry supports external logging to up to two Syslog servers.

Syslog Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Syslog HostIP</td>
<td>Sets the IP address of the Syslog server</td>
</tr>
<tr>
<td>Set Syslog Port</td>
<td>Sets the Syslog server port number</td>
</tr>
<tr>
<td>Show Syslog</td>
<td>Displays all Syslog configuration information</td>
</tr>
</tbody>
</table>

Setting the Syslog server IP address:

The Set Syslog HostIP command sets the TCP/IP address of the Syslog server.

**To set the Syslog server IP address:**

At the Switched CDU: prompt, type `set syslog`, followed by `hostip1` or `hostip2` and the Syslog server’s IP address. Press Enter.

**Example**

The following command sets the primary Syslog server IP address to 56.47.38.29:

```
Switched CDU: set syslog hostip1 56.47.38.29<Enter>
```

Changing the Syslog server port:

With Syslog support enabled, the Syslog server watches and responds to requests on the default Syslog port number 514. This port number may be changed using the Set Syslog Port command.

**To change the Syslog port:**

At the Switched CDU: prompt, type `set syslog port`, followed by the port number and press Enter.

**Example**

The following changes the Syslog port number to 411:

```
Switched CDU: set syslog port 411<Enter>
```
Displaying Syslog configuration information:
The Show Syslog command displays Syslog configuration information.

To display the Syslog configuration information:
At the Switched CDU: prompt, type show syslog and press Enter.

Example
The following command displays the Syslog configuration information:

Switched CDU: show syslog<Enter>
SYSLOG Configuration
  Primary Syslog Server IP Address: 56.47.38.29
  Secondary Syslog Server IP Address: 0.0.0.0
  Syslog Server Port: 411

Email

Email Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Email</td>
<td>Enables or disables Email notification support</td>
</tr>
<tr>
<td>Set Email SMTP Host</td>
<td>Sets the SMTP Host IP address or hostname</td>
</tr>
<tr>
<td>Set Email SMTP Port</td>
<td>Sets the SMTP server port number</td>
</tr>
<tr>
<td>Set Email From</td>
<td>Sets the email 'From' address</td>
</tr>
<tr>
<td>Set Email PrimaryTo</td>
<td>Sets the primary recipient email address</td>
</tr>
<tr>
<td>Set Email SecondaryTo</td>
<td>Sets the secondary recipient email address</td>
</tr>
<tr>
<td>Set Email Event</td>
<td>Enables or disables notification of general system events</td>
</tr>
<tr>
<td>Set Email Auth</td>
<td>Enables or disables notification of all authentication attempts</td>
</tr>
<tr>
<td>Set Email Power</td>
<td>Enables or disables notification of power state change requests</td>
</tr>
<tr>
<td>Set Email Config</td>
<td>Enables or disables notification of configuration changes</td>
</tr>
<tr>
<td>Show Email</td>
<td>Displays all Email configuration information</td>
</tr>
</tbody>
</table>

Enabling or disabling Email notification Support:
The Set Email command enables or disables Email notification support.

To enable or disable Email notification support:
At the Switched CDU: prompt, type set email, followed by enabled or disabled and press Enter.

Setting the SMTP server address:
The Set Email Host command sets the IP address or hostname of the SMTP server.

To set the SMTP server address:
At the Switched CDU: prompt, type set email smtp host, followed by the SMTP server’s IP address or hostname and press Enter.

Examples
The following command sets the SMTP server address to 55.55.55.55:

Switched CDU: set email smtp 55.55.55.55<Enter>

The following command sets the SMTP server address to email.servertech.com:

Switched CDU: set email smtp email.servertech.com<Enter>
Changing the SMTP server port:
With SMTP support enabled, the Sentry sends SMTP requests to the default SMTP port number 25. This port number may be changed using the Set Email SMTP Port command.

To change the TACACS port:
At the Switched CDU: prompt, type **set email smtp port**, followed by the port number and press **Enter**.

*Example*
The following changes the SMTP port number to 5555:
```
Switched CDU: set email smtp port 5555<Enter>
```

Setting the ‘From’ email address:
The Set Email From command sets the ‘from’ email address. By default, this is set to ‘Sentry3_’ plus the last three octets of the unit’s MAC address. Example: ‘Sentry3_510c90@’

To set the ‘From’ email address:
At the Switched CDU: prompt, type **set email from**, followed by the originating email address and press **Enter**.

*Example*
The following command sets the ‘from’ email address to Rack14CDU1@servertech.com:
```
Switched CDU: set email from Rack14CDU1@servertech.com<Enter>
```

Setting the ‘To’ email address:
The Set Email PrimaryTo and Set Email SecondaryTo commands set the recipient email addresses.

To set the ‘To’ email address:
At the Switched CDU: prompt, type **set email**, followed by **primaryto** or **secondaryto** and the destination email address. Press **Enter**.

*Examples*
The following command sets the primary ‘to’ email address to DayAdmin@servertech.com:
```
Switched CDU: set email primaryto DayAdmin@servertech.com<Enter>
```
The following command sets the secondary ‘to’ email address to NiteAdmin@servertech.com:
```
Switched CDU: set email secondaryto NiteAdmin@servertech.com<Enter>
```

Enabling or disabling event notification types:
The Set Email Event, Set Email Auth, Set Email Power and Set Email Config commands enable or disable email notification of the event types as described on page 96.

To enable or disable event notification types:
At the Switched CDU: prompt, type **set email**, followed by **event**, **auth**, **power** or **config** and **enabled** or **disabled**. Press **Enter**.

*Examples*
The following command sets the enables email notification general system events:
```
Switched CDU: set email event enabled<Enter>
```
The following command sets the disables email notification authentications attempts:
```
Switched CDU: set email auth disable<Enter>
```
Displaying Email configuration information:
The Show Email command displays Email configuration information.

**To display the Email configuration information:**
At the Switched CDU: prompt, type **show email** and press **Enter**.

**Example**
The following command displays the Email configuration information:

```
Switched CDU: show email
Email Configuration
  Email Notifications: Enabled
  SMTP Host: email.servertech.com
  SMTP Port: 5555
  'From' Address: Rack14CDU1@servertech.com
  Primary 'Send To' Address: DayAdmin@servertech.com
  Secondary 'Send To' Address: NiteAdmin@servertech.com
  Include EVENT Messages: Enabled
  Include AUTH Messages: Disabled
  Include POWER Messages: Disabled
  Include CONFIG Messages: Disabled
```
Upload/Download

The Sentry family of product supports the ability to upload and download system configurations using a standard FTP client. This feature enables for backup and restoration of system configuration as well as upload of ‘template’ configurations to ease large initial equipment deployments.

Upload/Download Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set FTP Server</td>
<td>Enables or disables the FTP server</td>
</tr>
<tr>
<td>Show FTP</td>
<td>Displays FTP configuration information</td>
</tr>
</tbody>
</table>

Sentry Integrated FTP Server

The Sentry supports an integrated FTP Server which must be enabled for Upload/Download support. The Sentry FTP Server supports a single user at a time. Once an administrative user has authenticated with the Sentry FTP Server, standard FTP client commands may be used to upload or download Sentry configurations.


Enabling and disabling the FTP server:

The Set FTP Server command is used to enable or disable the integrated FTP server.

To enable or disable the FTP server:

At the Switched CDU: prompt, type set ftp server, followed by enabled or disabled and press Enter.

FTP Configuration Files

The Sentry FTP server supports upload/download of two configuration files: CONFIG.BIN and NETWORK.INI. These files may be uploaded or downloaded using FTP PUT and GET operations.

- **CONFIG.BIN** This file contains the entire configuration of the Sentry excluding TCP/IP settings, serial/factory-only configurations, the x.509 certificate (SSL) and SSH keys. This file in encoded to keep all data (including usernames, passwords etc.) out of plain view. This file is NOT editable.

- **FTP.INI** This file contains only the FTP settings (FTP Host, username, password, filepath, filename and automatic updates support). This file is user readable and editable ‘plain text’ file.

- **NETWORK.INI** This file contains only the TCP/IP settings (IP address, subnet mask, gateway, DNS1 and DNS2). This file is user readable and editable ‘plain text’ file.

- **SNTP.INI** This file contains only the SNTP settings (SNTP Hosts and GMT offset). This file is user readable and editable ‘plain text’ file.

NOTE: The CONFIG.BIN file while encoded is not encrypted and susceptible to decoding using simple tools. Server Technology recommends the secure storage of CONFIG.BIN backup images.
Upload/Download Process

GETting a configuration file (Download):

1. Open the FTP client.
   *In a Windows environment, in the Run window type `ftp` and press Enter.*

2. At the prompt, type `open`, followed by the IP address of the Sentry and press Enter.
   
   FTP> open 12.34.56.78<Enter>

3. Authenticate with the appropriate administrative username and password.

4. At the prompt, type `get`, followed by the filename and press Enter.
   
   FTP> get config.bin<Enter>

5. At the prompt, type `close` to close the connection to the Sentry.
   
   FTP> close

PUTting a configuration file (Upload):

NOTE: Uploading the CONFIG.BIN file takes considerably longer than the NETWORK.INI file. When uploading both, Server Technology recommends uploading the NETWORK.INI file first.

1. Open the FTP client.
   For Windows: in the Run window, type `ftp` and press Enter.

2. At the prompt, type `open`, followed by the IP address of the Sentry and press Enter.
   
   FTP> open 12.34.56.78<Enter>

3. Authenticate with the appropriate administrative username and password.

4. At the prompt, type `put`, followed by the filename and press Enter.
   
   FTP> put network.ini<Enter>

5. At the prompt, type `close` to close the connection to the Sentry and force a restart of the device.
   
   FTP> close
Remote Shutdown

The Sentry family of products supports the ability to initiate an orderly shutdown of remote servers, protecting open application files prior to the server being powered down. Shutdown signaling is initiated over the existing TCP/IP network and requires the use of a Remote Shutdown Agent.

With the Remote Shutdown Agent installed on the server and Shutdown configured on the Sentry, the Sentry will initiate an orderly shutdown of the server for all actions that would remove power from the outlet such as Off and Reboot commands.

1. Off or Reboot command received by the Sentry
2. Shutdown signal is sent to the Remote Shutdown Agent on the target server.
3. Remote Shutdown Agent initiates a graceful shutdown of the target server and includes the ability to execute user-defined scripts to perform custom activities, such as safely shutting down open databases.
4. Sentry removes power from the outlet.

NOTE: Remote Shutdown is also supported by the extended feature set of Sentry Smart Load-Shedding. Graceful shutdown is initiated by Smart Load-Shedding events such as high temperature, high infeed load and UPS ‘On Battery’ conditions. For additional information on Sentry Smart Load-Shedding, please contact your Server Technology Sales Representative.

Figure 4.1 Remote Shutdown Diagram

106 • Advanced Operations

Installation and Operations Manual
Supported Operating Systems

Remote Shutdown Agents are available for the following operating systems:

- **Windows**
  - 2000, 2003, XP

- **Linux**
  - Red Hat 7.3, 8.0
  - Red Hat Enterprise 2.1 ES (update 5), 3.0 ES (update 4)
  - Novell SUSE Linux Enterprise Server

- **Unix**
  - HP-UX 11.0, 11i v1, 11i v2
  - IBM AIX 4.3, 5.3
  - Sun Solaris 8, 9, 10

- **Novell Netware**
  - 6

The Remote Shutdown Agents are available for download from the [Server Technology website](http://www.servertechnology.com).

Shutdown Agent Installation

**Windows**

1. Browse to the location of the Remote Shutdown Agent install files.
2. Run `Setup.exe` by double-clicking on the icon.
3. Reply to the standard installation prompts.
4. For additional security, when prompted enter the IP address of the Sentry device that will be sending the shutdown signal.

   **NOTE:** If left blank, any Sentry device may send a shutdown signal to the server.

**Linux**

5. Browse to the location of the Remote Shutdown Agent install files.
6. Run `SetupRA`.
7. For additional security, when prompted enter the IP address of the Sentry device that will be sending the shutdown signal.

   **NOTE:** If left blank, any Sentry device may send a shutdown signal to the server.

**Unix**

8. Browse to the location of the Remote Shutdown Agent install files.
9. Run `Install`.
10. For additional security, when prompted enter the IP address of the Sentry device that will be sending the shutdown signal.

   **NOTE:** If left blank, any Sentry device may send a shutdown signal to the server.

**Netware**

12. From the NetWare system console, load the configuration module (`pmconfig.nlm`) using the default path.
13. For additional security, when prompted enter the IP address of the Sentry device that will be sending the shutdown signal.

   **NOTE:** If left blank, any Sentry device may send a shutdown signal to the server.
Enabling and Setting up Remote Shutdown Support

Remote Shutdown Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Outlet Host</td>
<td>Sets the target server Host IP address or hostname</td>
</tr>
<tr>
<td>Set Outlet Shutdown</td>
<td>Enables or disables Remote Shutdown</td>
</tr>
<tr>
<td>Set Outlet Shutdown Delay</td>
<td>Sets the outlet Remote Shutdown delay</td>
</tr>
<tr>
<td>Set Outlet Script</td>
<td>Enables or disables shutdown script delays</td>
</tr>
<tr>
<td>Set Outlet Script Delay</td>
<td>Sets the outlet shutdown script delay</td>
</tr>
<tr>
<td>Show Shutdown</td>
<td>Displays Remote Shutdown configuration information</td>
</tr>
</tbody>
</table>

Enabling or disabling Remote Shutdown support:

The Set Outlet Shutdown command enables or disables Remote Shutdown support for an outlet.

To enable or disable Remote Shutdown support:

At the Switched CDU: prompt, type `set outlet shutdown`, followed by `yes` or `no`, and the outlet ID. Press Enter.

Example

The following command enables Remote Shutdown from outlet .a1:

Switched CDU: `set outlet shutdown yes .a1<Enter>`

Setting the Remote Shutdown delay:

The Set Outlet Shutdown Delay command sets the Remote Shutdown delay for an outlet.

To set the Remote Shutdown delay:

At the Switched CDU: prompt, type `set outlet shutdown delay`, followed by the outlet ID, and a value from 30 to 900 (in seconds). Press Enter.

Example

The following command sets the Remote Shutdown delay for outlet .a2 to 120 seconds:

Switched CDU: `set outlet shutdown delay .a2 120<Enter>`

Setting the outlet host address:

The Set Outlet Host command set the IP address or hostname for an outlet. Hostnames may be up to 60 characters long.

To set the outlet host address:

At the Switched CDU: prompt, type `set outlet host`, followed by the outlet ID, and the IP address or hostname. Press Enter.

Example

The following command set the hostname for outlet .a1 to ‘Windows2003’:

Switched CDU: `set outlet host .a1 Windows2003<Enter>`

Enabling or disabling shutdown script support:

The Set Outlet Script command enables or disables shutdown script support for an outlet.

To enable or disable shutdown script support:

At the Switched CDU: prompt, type `set outlet script`, followed by `yes` or `no`, and the outlet ID. Press Enter.

Example

The following command enables Remote Shutdown from outlet .a1:

Switched CDU: `set outlet script yes .a1<Enter>`
Setting the shutdown script delay:
The Set Outlet Script Delay command sets the shutdown script delay for an outlet.

To set the shutdown script delay:
At the Switched CDU: prompt, type `set outlet script delay`, followed by the outlet ID, and a value from 1 to 15 (in minutes). Press Enter.

Example
The following command sets the shutdown script delay for outlet .a1 to 10 minutes:
Switched CDU: set outlet shutdown delay .a1 10<Enter>

Displaying Remote Shutdown information:
The Show Shutdown command displays all shutdown configuration information.
- Outlet ID and descriptive name
- Remote Shutdown settings
- Shutdown script setting

To display shutdown information:
At the Switched CDU: prompt, type `show shutdown` and press Enter.

Example
The following command displays all shutdown information:

```plaintext
Switched CDU: show shutdown
Outlet ID   Outlet Name & Hostname/IP            Shutdown/ Delay (sec)  Script/ Delay (min)
        .A1            DataServer_1               Yes/90      Yes/10
        .A2            WebServer_1                No/120       No/1
        .A3            FileServer_1               No/90        No/1
        .A4            TowerA_Outlet4             No/90        No/1
        .A5            TowerA_Outlet5             No/90        No/1
        .A6            TowerA_Outlet6             No/90        No/1
        .A7            TowerA_Outlet7             No/90        No/1
        .A8            TowerA_Outlet8             No/90        No/1
```
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 Web 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.

To reset to 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. |

From the Web interface

On the Restart page in the Tools section of the Web interface, select Restart and reset to factory defaults from the drop-down menu and press Apply.

From the command line

At the Switched CDU: prompt, type restart factory and press Enter.

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.

| NOTE: This method will NOT work if the reset button has been disabled by the administrator. |

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. |

To reset to factory defaults, except network settings

From the Web interface

On the Restart page in the Tools section of the Web interface, select Restart and reset to factory defaults, except network from the drop-down menu and press Apply.

From the command line

At the Switched CDU: prompt, type restart factory keepnet and press Enter.

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 Web interface. Upon initiating an FTP upload session, 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.

You must have administrator-level privileges to initiate an upload.

To initiate an FTP upload session from the Web interface

On the Restart page in the Tools section of the Web interface, select Restart and upload firmware via FTP from the drop-down menu and press Apply.

To initiate an FTP upload session from the command line

To initiate an FTP firmware upload session:

At the Switched CDU: prompt, type restart ftpload and press Enter.
## Appendix C: Technical Specifications

### Domestic Models

**POPS™ Switched CDU**

<table>
<thead>
<tr>
<th>Model</th>
<th>Rated Voltage</th>
<th>Input Cordset and Plug (10')</th>
<th>Outlets</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWG-16V2A313A1</td>
<td>208-240V 50/60Hz</td>
<td>IEC 60320 C20(^1)</td>
<td>4 / 12^2</td>
</tr>
<tr>
<td>CWG-16V2C313A1</td>
<td>208-240V 50/60Hz</td>
<td>NEMA L6-30P, 30A/208V locking</td>
<td>4 / 12^2</td>
</tr>
</tbody>
</table>

**POPS™ Expansion Module CDU**

<table>
<thead>
<tr>
<th>Model</th>
<th>Rated Voltage</th>
<th>Input Cordset and Plug (10')</th>
<th>Outlets</th>
</tr>
</thead>
<tbody>
<tr>
<td>CXG-16V2A313A1</td>
<td>208-240V 50/60Hz</td>
<td>IEC 60320 C20(^1)</td>
<td>4 / 12^2</td>
</tr>
<tr>
<td>CXG-16V2C313A1</td>
<td>208-240V 50/60Hz</td>
<td>NEMA L6-30P, 30A/208V locking</td>
<td>4 / 12^2</td>
</tr>
</tbody>
</table>

### International Models

**POPS™ Switched CDU**

<table>
<thead>
<tr>
<th>Model</th>
<th>Rated Voltage</th>
<th>Input Cordset and Plug (10')</th>
<th>Outlets</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWG-16VEA313A1</td>
<td>230V 50/60Hz</td>
<td>IEC 60320 C20(^1)</td>
<td>4 / 12^2</td>
</tr>
<tr>
<td>CWG-16VEK313A1</td>
<td>230V 50/60Hz</td>
<td>IEC 60309, 32A 3-pin 6Hr Blue</td>
<td>4 / 12^2</td>
</tr>
<tr>
<td>CWG-24V4K411A1</td>
<td>3/N/PE 400V 50/60Hz</td>
<td>IEC 60309, 32A 5-pin 6Hr Red</td>
<td>6 / 18^3</td>
</tr>
</tbody>
</table>

**POPS™ Expansion Module CDU**

<table>
<thead>
<tr>
<th>Model</th>
<th>Rated Voltage</th>
<th>Input Cordset and Plug (10')</th>
<th>Outlets</th>
</tr>
</thead>
<tbody>
<tr>
<td>CXG-16VEA313A1</td>
<td>230V 50/60Hz</td>
<td>IEC 60320 C20(^1)</td>
<td>4 / 12^2</td>
</tr>
<tr>
<td>CXG-16VEK313A1</td>
<td>230V 50/60Hz</td>
<td>IEC 60309, 32A 3-pin 6Hr Blue</td>
<td>4 / 12^2</td>
</tr>
<tr>
<td>CXG-24V4K411A1</td>
<td>3/N/PE 400V 50/60Hz</td>
<td>IEC 60309, 32A 5-pin 6Hr Red</td>
<td>6 / 18^3</td>
</tr>
</tbody>
</table>

\(^1\) Input cordset selected at time of purchase  
\(^2\) qty x IEC 60320 C13 / qty x IEC 60320 C19
## Power Ratings

### Domestic Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Voltage</th>
<th>Current</th>
<th>Voltage</th>
<th>Outlet</th>
<th>Branch Circuit</th>
<th>Phase</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>CxG-16/V2A311A1</td>
<td>208-240V</td>
<td>16</td>
<td>208-240V</td>
<td>12</td>
<td>xy</td>
<td>9.2</td>
<td>27.6</td>
</tr>
<tr>
<td>CxG-16/V2C311A1</td>
<td>208-240V</td>
<td>24</td>
<td>208-240V</td>
<td>12</td>
<td>yz</td>
<td>9.2</td>
<td>13.9</td>
</tr>
</tbody>
</table>

### International Models

1. All current ratings are in amperes. *Tous les indices de courant sont en ampères.*  
   2. IEC 60320 C13 / IEC 60320 C19

<table>
<thead>
<tr>
<th>Model</th>
<th>Voltage</th>
<th>Current</th>
<th>Voltage</th>
<th>Outlet</th>
<th>Branch Circuit</th>
<th>Phase</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>CxG-16/V2A311A1</td>
<td>208-240V</td>
<td>16</td>
<td>208-240V</td>
<td>xy</td>
<td>9.2</td>
<td>27.6</td>
<td></td>
</tr>
<tr>
<td>CxG-16/V2C311A1</td>
<td>208-240V</td>
<td>24</td>
<td>208-240V</td>
<td>yz</td>
<td>13.9</td>
<td>41.6</td>
<td></td>
</tr>
</tbody>
</table>

### Physical Specifications

<table>
<thead>
<tr>
<th>Operating</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>-40° to 185° F (-40° to 85° C)</td>
</tr>
<tr>
<td>Elevation (above MSL)</td>
<td>0 to 50,000 ft (0 to 15000m)</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>10 to 90%, non-condensing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dimensions (H x W x D)</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>CxG-16VxxM</td>
<td>10.2 lbs (4.6 kg)</td>
</tr>
<tr>
<td>CxG-24VxxM</td>
<td>17.5 lbs (7.9 kg)</td>
</tr>
</tbody>
</table>
Branch Circuit Protection

Always disconnect ALL power supply cords before opening to avoid electrical shock. Afin d’éviter les chocs électriques, débranchez TOUTES les cables électriques avant d’ouvrir. Vor dem Öffnen immer Netzleitung abziehen um elektrischen Schlag zu vermeiden.

Switched CDUs feature Branch Circuit protection on all outlets in the form of internal fuses. These fuses meet the strict safety requirements of UL/CSA 60950-1 for Branch Circuit Protection.

Time-Delay Fuses – Class G

<table>
<thead>
<tr>
<th>Amperes</th>
<th>Bussman Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>SC-20</td>
</tr>
</tbody>
</table>

CooperBussman product data-sheet #1024

Data Connections

RS-232 port

Switched CDUs 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.

<table>
<thead>
<tr>
<th>Pin</th>
<th>DTE Signal Name</th>
<th>Input/Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Request to Send</td>
<td>RTS</td>
</tr>
<tr>
<td>2</td>
<td>Data Terminal Ready</td>
<td>DTR</td>
</tr>
<tr>
<td>3</td>
<td>Transmit Data</td>
<td>TD</td>
</tr>
<tr>
<td>4</td>
<td>Signal Ground</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Signal Ground</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Receive Data</td>
<td>RD</td>
</tr>
<tr>
<td>7</td>
<td>Data Set Ready</td>
<td>DSR</td>
</tr>
<tr>
<td>8</td>
<td>Clear to Send</td>
<td>CTS</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Pin</th>
<th>DCE Signal Name</th>
<th>Input/Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Receive Data</td>
<td>RD</td>
</tr>
<tr>
<td>3</td>
<td>Transmit Data</td>
<td>TD</td>
</tr>
<tr>
<td>4</td>
<td>Data Terminal Ready</td>
<td>DTR</td>
</tr>
<tr>
<td>5</td>
<td>Signal Ground</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Data Set Ready</td>
<td>DSR</td>
</tr>
<tr>
<td>7</td>
<td>Request to Send</td>
<td>RTS</td>
</tr>
<tr>
<td>8</td>
<td>Clear to Send</td>
<td>CTS</td>
</tr>
</tbody>
</table>

LED Indicators

Input/Branch/Phase Current

Units are equipped with 7-segment LEDs for reporting of input, branch or phase current loading. Loading is reported in amperes and is displayed in ½ amp increments under 10A and whole amp increments at and above 10A. Additionally, the LED may display codes for events detected by the system for immediate local notification.

<table>
<thead>
<tr>
<th>Behavior/Code</th>
<th>Event description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking</td>
<td>On 3-phase devices – Indicates that phase loads exceed out-of-balance threshold</td>
</tr>
<tr>
<td>FE</td>
<td>Sentry has detected a removed/blown fuse</td>
</tr>
</tbody>
</table>

Outlets

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 operated 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 exigencies 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

Products with the following mark comply with the RoHS Directive (2002/95/EC) issued by the Commission of the European Community.
Japanese Notification

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

本製品に同梱または付属しております電源コードは、本製品専用です。本製品以外の製品ならびに他の用途に使用しないで下さい。

Chinese Notification

关于符合中国《电子信息产品污染控制管理办法》的声明

产品中有毒有害物质的名称及含量

<table>
<thead>
<tr>
<th>部件名称 (Parts)</th>
<th>有毒有害物质或元素 (Hazardous Substance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>机箱组件 (Chassis Subassembly)</td>
<td>铅 (Pb)</td>
</tr>
<tr>
<td>印刷板组件 (PCAs)</td>
<td>X</td>
</tr>
</tbody>
</table>

O 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006 标准规定的限量要求以下。

Indicates that this hazardous substance contained in all homogeneous materials of this part is below the limit requirement in SJ/T 11363-2006.

X 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006 标准 规定的限量要求。

Indicates that this hazardous substance contained in at least one of the homogeneous materials of this part is above the limit requirement in SJ/T 11363-2006.

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.
Appendix D: Warranty, Product Registration and Support

Warranty
For the Server Technology warranty information, please see our Website at www.servertech.com

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 at www.servertech.com

Technical Support

Experience Server Technology’s FREE SMARTER 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 a.m. to 5 p.m. PST, Monday through Friday. After-hours service is provided to ensure your requests are handled quickly no matter what time zone or country you are located in.

Server Technology, Inc.
1040 Sandhill Drive              Tel: 775.284.2000          Web: www.servertech.com
Reno, Nevada 89521 USA          Fax: 775.284.2065          Email: 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, please review Server Technology’s Return Merchandise Authorization process on our website at www.servertech.com