



# Intelligent IPM

## Installation and Operations Manual



### Instructions

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



### Dangerous Voltage

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



### Protective Grounding Terminal

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

## Life-Support Policy

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

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

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

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

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

## Notices

301-0113-1 Rev K (052016)

Copyright © 2005-2016 Server Technology, Inc. All rights reserved.

1040 Sandhill Drive

Reno, Nevada 89521 USA

### All Rights Reserved

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

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

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

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, Sentry, Switched CDU, CDU, PRO2, PIPS, POPS, PDU Power Pivot, and StartUp Stick are trademarks of Server Technology, Inc., registered in the US. EZip is a trademark of Server Technology.

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

<b>CHAPTER 1: INTRODUCTION</b>	<b>4</b>
Quick Installation Checklist.....	4
Technical Support.....	4
PDU Power Pivot®.....	5
Equipment Overview.....	6
IPv6 and Sentry Products.....	7
Installation.....	10
Standard Accessories.....	10
Optional Accessories.....	10
Safety Precautions.....	11
Installing the Power Input Retention Bracket.....	12
Attaching Safety Earth Ground Connection.....	13
Connecting to the Power Source.....	14
Connecting Devices.....	14
Connecting the Sensors.....	14
Connecting to the Unit.....	14
<b>CHAPTER 2: OPERATIONS</b>	<b>15</b>
Interfaces.....	16
Web Interface.....	17
Command Line Interface.....	41
<b>CHAPTER 3: ADVANCED OPERATIONS</b>	<b>75</b>
SSL.....	76
SSH.....	78
SNMP/Thresholds.....	79
LDAP.....	91
TACACS+.....	101
Logging.....	106
Upload/Download.....	110
<b>CHAPTER 4: APPENDICES</b>	<b>112</b>
Appendix A: Resetting to Factory Defaults.....	112
Appendix B: Uploading Firmware.....	113
Appendix C: Technical Specifications.....	114
Appendix D: Product Support Information.....	119

# Chapter 1: Introduction

## Quick Installation Checklist

The following steps are recommended to quickly install and configure the Intelligent IPM for use in your data center equipment cabinet.

1. Mount the Intelligent IPM.
2. Connect to the power source.
3. Connect the devices.
4. Connect the sensors.
5. Connect to the PDU.
6. Configure the PDU.
  - Login as the predefined Administrator (admin/admin).
  - Configure the network settings.
  - Create new administrative user account.
  - Configure location and PDU names.
  - Configure sensor names.
  - Configure new user account(s).
  - Remove the predefined Administrator.
7. Connect the PDU to the network.

## Technical Support



### Experience Server Technology's FREE Technical Support

Server Technology understands<sup>®</sup> 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: 1-800-835-1515

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

Reno, Nevada 89521 USA

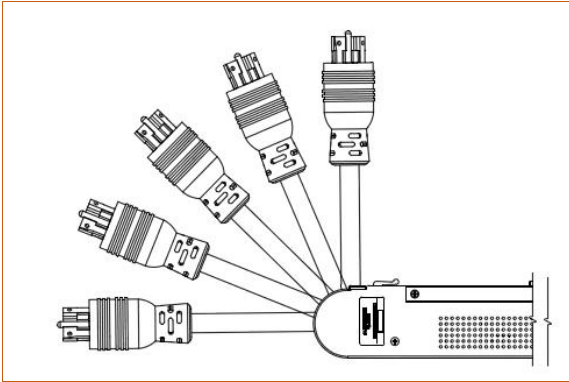
Fax: 775-284-2065

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

## PDU Power Pivot®

Server Technology's PDU Power Pivot® flexible infeed provides a simplified power cord routing to the PDU with a design that eliminates bend radius issues.

As illustrated below, the PDU Power Pivot capability can deliver a solution for several types of PDU installations and mountings, setting the correct cord angle for overhead power, offset overhead power, concrete floor, raised floor, and intra-rack power.



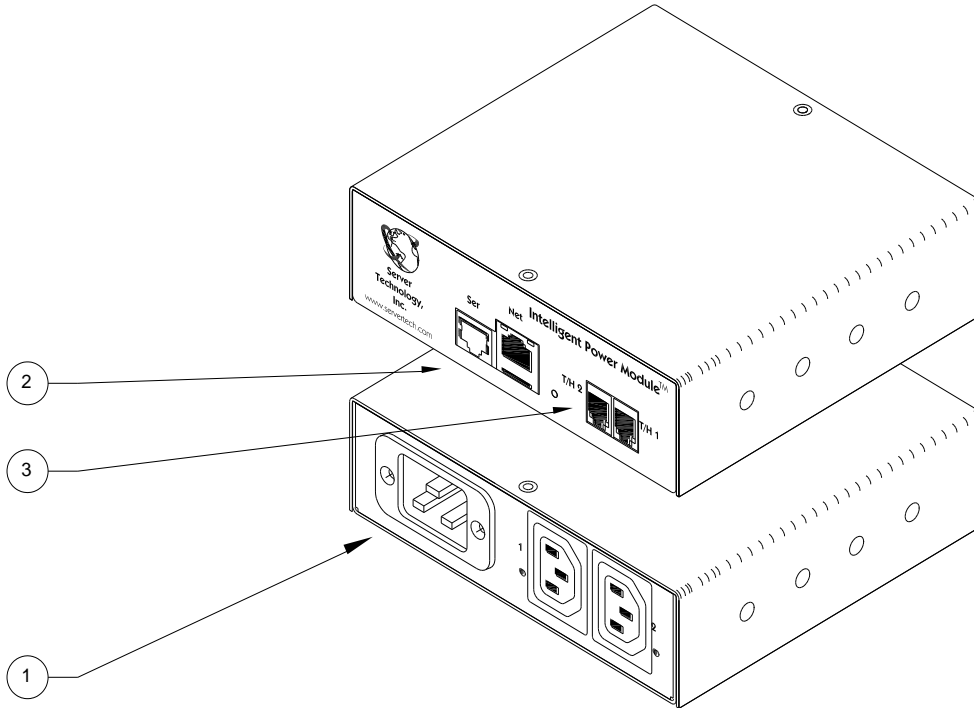
**PDU Power Pivot – Flexible Cord Design**

To learn more about PDU Power Pivot and watch a brief video that animates the PDU Power Pivot mounting angles in the equipment rack, see the Server Technology website at: <http://info.servertech.com/PDUpowerpivot>

## Equipment Overview

1. The power inlet/cord(s) connects the Intelligent IPM to the electrical power source.
2. Two RJ45 connectors for Serial (RS-232) and Ethernet connection.
3. Two mini RJ11 connectors for Temperature/Humidity sensors.

A number is printed above each outlet, and these numbers can be used in commands that require an outlet name.



**Intelligent IPM Views**

## IPv6 and Sentry Products

Server Technology is introducing IPv6 “dual stack” support to the PDU product line. IPv6 has been designed to succeed IPv4 as the dominant communications protocol for internet traffic, to avoid depletions of the IPv4 address space, and to allow more IP address growth. Many devices already in use support IPv6.

IPv6 has several new operational methods:

- Static IPv6 Address: The IPv6 equivalent of Static IPv4.
- DHCPv6 Address: The IPv6 equivalent of a DHCP IPv4 address, also known as a “stateful” auto-configuration of DHCPv6.
- IPv6 Stateless Auto-Configured Address – (RFC 4862): An automatically-generated unique link-local IPv6 address used for client based configurations. This address is always present in the Server Technology dual stack and cannot be disabled.
- DHCPv6 Stateless Auto-Configured Address – (RFC 3736): A “stateless” Dynamic Host Configuration Protocol (DHCP) service for IPv6 (DHCPv6). This address is used by nodes to obtain configuration information, such as addresses of DNS recursive name servers that do not require the maintenance of any dynamic state for individual clients.

### **Firmware – Protocol Support**

#### **IPv6 and IPv4 Protocols:**

The firmware supports the following network IPv6 and IPv4 protocols:

- DNS Ping
- FTP (or SFTP) Server SNMPv1/2/3
- FTP (or SFTP) Updates SNTP
- HTTP or HTTPS
- SMTP
- Static IPv6 DHCPv6 (stateless and stateful)
- Syslog SNMPv1/2/3 Traps
- Telnet SSH

#### **IPv4-Only Protocols:**

The firmware supports the following network IPv4-only protocols:

- Cisco EnergyWise
- LDAP
- Load Shedding \*
- RADIUS \*
- TACACS+

\* = may work with IPv6 addresses, but not tested.

## Network-Enabled Modes

---

### NOTES:

- For all network-enabled modes described below, the PDU will set an auto-configured IPv6 address, and if IPv6 router announcements are active, a stateless DHCP IPv6 address will also be set. Further, in all network-enabled modes, at least one IPv4 or one IPv6 address will be active.
  - For maximum backward compatibility, the default network mode is “IPv4 only”.
- 

- Network disabled – No IPv4 or IPv6 addresses available.
- IPv4 only, DHCP disabled (static IPv4) – If the IPv4 Static Address and Net Mask of the PDU are valid, they will be set.
- IPv4 only, DHCP enabled (DHCP IPv4) – The PDU will try to resolve an IPv4 DHCP address. If a DHCP address cannot be obtained after 90 seconds, the PDU can: (1) optionally fall back to its static IPv4 settings, or (2) indefinitely wait to acquire an address based on DHCP configuration settings. **This setting is the default.**
- Dual IPv6/IPv4, DHCP disabled (static IPv6/IPv4) – If the IPv6 Static Address and prefix of the PDU are valid, they will be set. Otherwise, the PDU will attempt to use DHCPv6 to obtain an IPv6 address.

In addition, if the IPv4 Static Address and Net Mask of the PDU are valid, they will be set.

- Dual IPv6/IPv4, DHCP enabled (DHCP IPv6/IPv4) – The PDU will try to resolve both its IPv6 and IPv4 addresses by DHCP. If both DHCP requests are answered, the primary DNS server of the PDU will become the primary IPv6 DNS server, and the secondary DNS server of the PDU will become the primary IPv4 DNS server. If only one of the DHCP requests is answered, the DNS servers of the PDU will map to the primary and secondary DNS server from that request.

If a DHCP address cannot be obtained after 90 seconds, the PDU can: (1) optionally fall back to its static IPv4 and/or IPv6 settings, or (2) indefinitely wait to acquire an address based on DHCP configuration settings.



## Viewing Network Status

You can obtain the IPv6 network status through the firmware Web Interface or Command Line Interface (CLI). For the CLI, use the **show network** command as follows:

```
Switched CDU: show network
Network Settings
  State: DHCP IPv6/IPv4 Network: Dual IPv6/IPv4
  Link: Up Negotiation: Auto
  Speed: 100 Mbps Duplex: Full

  AutoCfg IPv6: FE80::20A:9CFF:FE52:4104/64
  IPv6 Address: FD01::1:B51A:E03C/64
  IPv4 Address: 10.1.6.230 Subnet Mask: 255.255.0.0
  IPv4 Gateway: 10.1.1.1
  DNS1: FD01::A01:585
  DNS2: 10.1.5.133

Static IPv4/IPv6 Settings
  IPv6 Address: FD01::A01:353/64
  IPv6 Gateway: ::
  IPv4 Address: 10.1.2.253 Subnet Mask: 255.255.0.0
  IPv4 Gateway: 10.1.1.1
  DNS1: 10.1.5.133
  DNS2: 10.1.5.134

DHCP Settings
  DHCP: Enabled
  FQDN: Enabled [sentry3-524104]
  Boot Delay: Enabled
  Static Fallback: Enabled

Network Services
  Telnet: Enabled Port: 23
  SSH: Enabled Port: 22 Auth: Password, Kb-Int
  HTTP: Enabled Port: 80
  SSL: Enabled Port: 443 Installed Cert: User Encrypted
  Access: Optional Stored Files: Cert & Key
  User Cert: Enabled User Passphrase: <set>
  SNMPv1/2: Enabled Port: 161 TrapPort: 162
  SNMPv3: Disabled Port: 161 TrapPort: 162
  FTP Server: Enabled Port: 21
  SPM Access: Enabled

Command successful
```

---

**NOTE:** The fields IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway, DNS1, and DNS2 are equivalent to existing PDU IPv4 settings except that current network settings and static settings are displayed separately. This allows you to view both static configuration settings and active network settings that can be obtained using DHCP. The DNS addresses may be in IPv4 or IPv6 (based on RFC4291) format at this time.

---

## Installation

Before installing your Intelligent IPM, 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














- RJ45 to RJ45 crossover cable.
- RJ45 to DB9F serial port adapter (for connection to standard DB9M DTE serial port).
- Outlet retention clips (208-240V models).
- Separate power input cord (typically sold as a separate line item).
- Power input retention bracket hardware (**can** be installed):
  - Two removable T-brackets with two 40mm screws.

### Optional Accessories

- Temperature/Humidity sensors
- Rack mounting hardware

## Safety Precautions

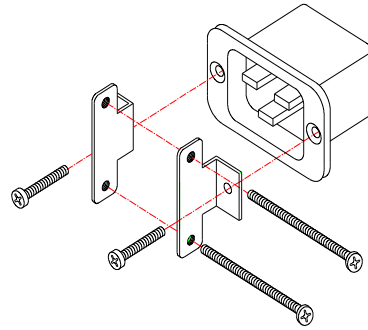
This section contains important safety and regulatory information that **must be reviewed** before installing and using the Intelligent IPM.

	Only for installation and use in a Restricted Access Location in accordance with the following installation and use instructions.  <b>This equipment should only be installed by trained personnel.</b>	Destiné à l'installation et l'utilisation dans le cadre de Restricted Access Location selon les instructions d'installation et d'utilisation.  <b>Cet équipement est uniquement destiné à être installé par personnel qualifié.</b>	Nur für Installation und Gebrauch in eingeschränkten Betriebszonen gemäß der folgenden Installations-und Gebrauchsanweisungen.  <b>Dieses Gerät ist nur für den Einbau durch Personal vorgesehen.</b>
	This equipment is designed to be installed on a dedicated circuit. The power supply cord shall be a minimum of 1.5m (4.9ft) and a maximum of 4.5m (15ft). If using an extension power cord, the total length shall also be no more than the maximum allowed. The plug is considered the disconnect device and must be easily accessible.	Cet équipement a été conçu pour être installé que un circuit dédié. Le cordon d'alimentation doit être d'au moins 1,5M et un maximum de 4,5m. Si vous utilisez un cordon de rallonge, la longueur totale est également plus que le maximum autorise. La prise est considérée comme un dispositif de coupure et doit être facilement accessible.	Die Geräte sind für eine Installation an einer fest zugeordneten Leitung ausgelegt. Die Stromzuleitung hat eine Mindestlänge von 1,5m, und höchstens 4,5m. Sollten Sie ein Verlängerungskabel, der Gesamtlänge auch nicht mehr als die maximal zulässige sein. Der Stecker dient zur Trennung vom Netz und muss einfach erreichbar sein.
	The dedicated circuit must have circuit breaker or fuse protection. PDUs 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 PDU must be provided and must meet all applicable codes and regulations. In North America, protection must have a 10,000A interrupt capacity.	Le circuit spécialisé doit avoir un disjoncteur ou une protection de fusible. PDU ont été conçus sans disjoncteur général ni fusible pour éviter que cela devienne 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.	Der feste Stromkreis muss mit einem Schutzschalter oder einem Sicherungsschutz versehen sein. PDUs verfügt über keinen Hauptschutzschalter bzw. über keine Sicherung, damit kein einzelner Fehlerpunkt entstehen kann. Der Kunde ist dafür verantwortlich, den Stromkreis sachgemäß zu schützen. Der Kapazitätsschutz entspricht der aktuellen Stromstärke der Geräte und muss alle relevanten Codes und Bestimmungen erfüllen. Für Installation in Nordamerika müssen Ausschalter bzw. Sicherung über 10.000 A Unterbrechungskapazität verfügen.
	Models with unterminated power cords: Input connector must be installed by qualified service personnel. Input connector rating must meet all applicable codes and regulations.	Modèles avec cordons d'alimentation non terminés: Le connecteur d'entrée doit être installé par un personnel qualifié. Entrée cote de raccordement doit respecter tous les codes et règlements électriques applicables.	Modelle mit nicht abgeschlossenen Netzkabel: Der Eingangsstecker darf nur von qualifiziertem Wartungspersonal installiert werden. Eingangsanschluss Bewertung müssen alle geltenden und verbindlichen Normen und Vorschriften entsprechen.
	Do not block venting holes when installing this product. Allow for maximum airflow at all times.	Ne bloquez pas les orifices d'aération lors de l'installation de ce produit. Permettre une circulation d'air maximale à tout moment.	Achten Sie darauf, dass keine Belüftungslöcher bei der Installation dieses Produkts. Damit für maximalen Luftstrom zu allen Zeiten.
	Installation Orientation: Vertical units are designed to be installed in vertical orientation.	Installation Orientation: Les unités vertical sont conçues pour être installées dans une orientation verticale.	Installationsausrichtung: Vertical Einheiten sind zur vertikalen Installation vorgesehen.
 	Always disconnect the power supply cord before servicing to avoid electrical shock. For products with two input power cords, both must be disconnected before servicing.	Toujours débrancher le cordon d'alimentation avant de l'ouverture pour éviter un choc électrique. Pour les produits avec deux cordons d'alimentation d'entrée, les deux doivent être déconnectés avant l'entretien.	Trennen Sie das Netzkabel, bevor Sie Wartungsarbeiten Öffnung einen elektrischen Schlag zu vermeiden. Für Produkte mit zwei Eingangsstromkabel, sowohl, müssen vor der Wartung abgeschaltet werden.
	WARNING! High leakage current! Earth connection is essential before connecting supply!	ATTENTION! Haut fuite très possible! Une connection de masse est essentielle avant de connecter l'alimentation !	ACHTUNG! Hoher Ableitstrom! Ein Erdungsanschluss ist vor dem Einschalten der Stromzufuhr erforderlich!
 	WARNING! Cx-xxE-x units double pole/neutral fusing	ATTENTION! Les unités Cx-xxE-x Double Pôle/Fusible sur le Neutre	ACHTUNG!: Cx-xxE-x Zweipolige bzw. Neutralleiter-Sicherung
	ATTENTION! Observe precautions for handling Electrostatic Sensitive Devices.	Attention ! Respecter les mesures de sécurité en manipulant des dispositifs sensibles aux décharges électrostatiques.	Achtung! Vorsichtshinweise zur Handhabung elektrostatisch empfindlicher Geräte beachten.
	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.	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 correspond.	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.

## Installing the Power Input Retention Bracket

### To install the power input retention bracket:

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



**Retention Bracket Assembly**

## Attaching Safety Earth Ground Connection


Server Technology PDUs are supplied with an external safety ground connection to provide an alternate ground path for fault currents, and to maintain the same ground reference between it and the equipment rack.

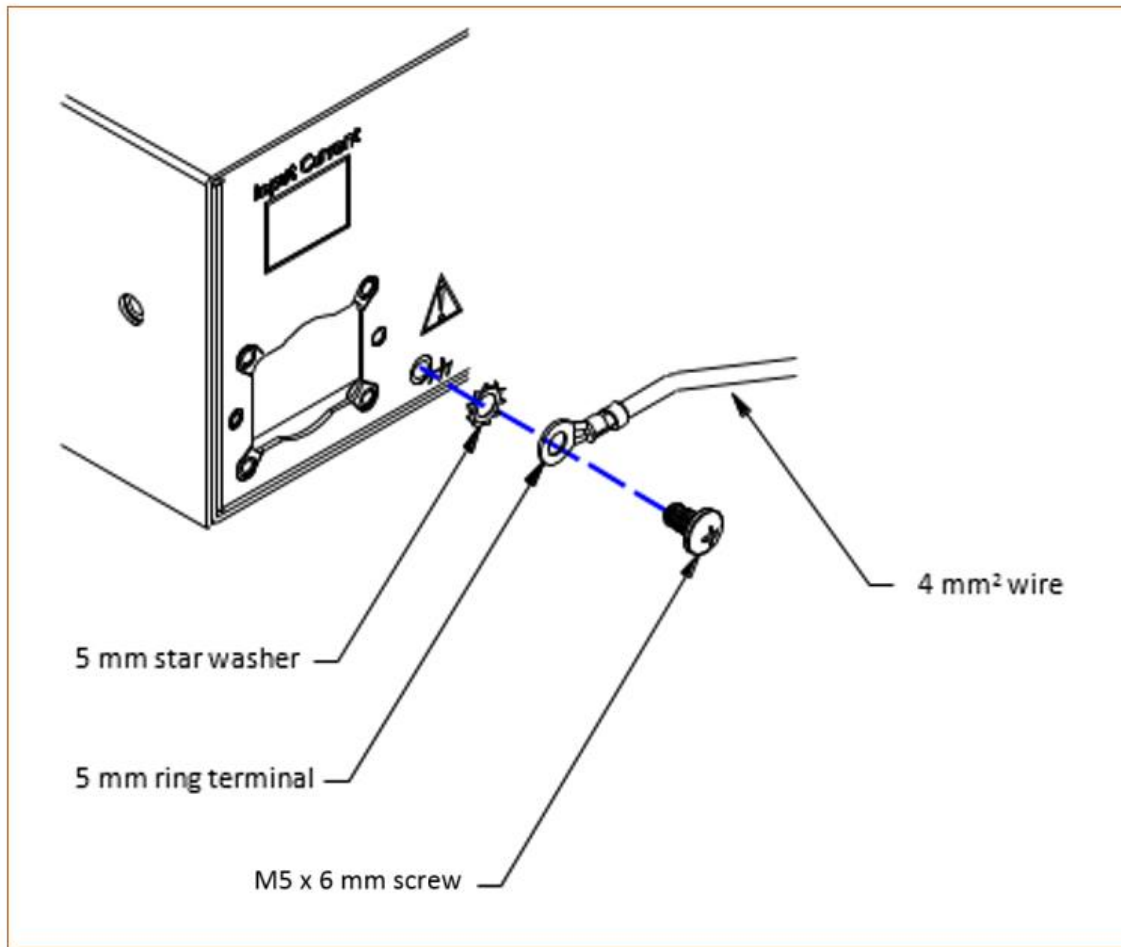
**NOTE:** The auxiliary external ground location may vary. Most PDUs will have it located near the power cord entry located near the  symbol.

### User-supplied materials:

- One 5 mm internal (or external) tooth star washer;
- One 4.0 mm<sup>2</sup> (10 AWG) wire with 5 mm ring terminal;
- One metric M5 x 6 mm coarse pitch screw.

### Instructions:

1. Connect one end of the ground wire to the equipment cabinet or local ground.
2. Locate the PDU external ground near the  symbol.
3. Connect the other end with a ring terminal and a M5 screw to the PDU external ground. To ensure proper grounding to the chassis, use a star washer between the ring terminal and the PDU.



## Connecting 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

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 Intelligent IPM outlets.

---

**NOTE:** Server Technology recommends even distribution of attached devices across all available outlets to avoid exceeding the outlet, branch or phase limitations.

---



---

Always disconnect ALL power supply cords before opening to avoid electrical shock.  
Afín d'éviter les chocs électriques, débranchez TOUTES les cables électrique avant d'ouvrir.  
Immer ALLE Netzleitungen auskuppeln vor den Aufmachen um elektrischen Schlag zu vermeiden.

---

## Connecting the Sensors

The Intelligent IPM 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 Intelligent IPM 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.

### Ethernet port

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

The Intelligent IPM 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 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

## Chapter 2: Operations

<b>INTERFACES</b>	<b>16</b>
Outlet Naming and Grouping	16
Usernames and Passwords	16
<b>WEB INTERFACE</b>	<b>17</b>
Logging In	17
System Summary	18
Outlet Control	21
<i>Individual</i> .....	21
<i>Group</i> .....	21
Environmental Monitoring	22
<i>Sensors</i> .....	22
Configuration	22
<i>System</i> .....	22
<i>Network</i> .....	25
<i>Telnet/SSH</i> .....	26
<i>HTTP/SSL</i> .....	26
<i>Serial Ports</i> .....	28
<i>Groups</i> .....	29
<i>Users</i> .....	29
<i>FTP</i> .....	31
<i>SNTP/Syslog</i> .....	32
<i>SNMP/Thresholds</i> .....	33
<i>LDAP</i> .....	35
<i>TACACS+</i> .....	37
<i>RADIUS</i> .....	38
<i>SMTP/Email</i> .....	39
Features	40
Tools	40
<i>Ping</i> .....	40
<i>Change Password</i> .....	40
<i>Firmware</i> .....	40
<i>View Log</i> .....	40
<i>Restart</i> .....	40
<b>COMMAND LINE INTERFACE</b>	<b>41</b>
Logging In	41
Operations Commands	45
Administration Commands	49
<i>User Administration</i> .....	49
<i>Outlet Administration</i> .....	53
<i>Group Administration</i> .....	55
<i>Environmental Monitor Administration</i> .....	56
<i>Serial Port Administration</i> .....	56
<i>System Administration</i> .....	58
<i>Feature Administration</i> .....	60
<i>TCP/IP Administration</i> .....	67
<i>HTTP Administration</i> .....	70
<i>Sentry Power Manager (SPM) Administration</i> .....	70
<i>Telnet Administration</i> .....	71
<i>FTP Administration</i> .....	71
<i>SNTP Administration</i> .....	73

## Interfaces

The Intelligent IPM 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**

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

Absolute names are specified by a period (.) followed by a tower letter and outlet number. The tower letter for the Intelligent IPM is A.

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

### **Usernames and Passwords**

The Intelligent IPM 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 can perform operations such as creating/removing user accounts and command privileges, changing passwords and displaying user information. An administrator can also view the status of all sensors and power inputs.

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



## Web Interface

The Web Interface provides web-based access to the Firmware. The interface is designed with three major sections, illustrated below.

1. System Header: Shows PDU description and location, IP address, and user/access.
2. Navigation Bar: Provides access to PDU configuration, control action, or status page.
3. Details Window: Current control/status information based on the page selected from the navigation bar.

**NOTE:** The blinking of the PDU location string (IP address) in the System Header section may not work with all web browsers.

This example shows the **Outlet Control > Individual** page:

The screenshot displays the 'Sentry Switched CDU' web interface. The system header shows 'Location: IP Address: 10.1.1.74' and 'User: admn Access: Admin'. The navigation bar on the left includes 'System', 'Outlet Control', 'Individual', 'Group', 'Power Monitoring', 'Environmental Monitoring', 'Smart Load Shedding', 'Configuration', and 'Tools'. The main content area is titled 'Outlet Control - Individual' and 'Individual Outlet Control'. It features a table with columns for 'Outlet ID', 'Outlet Name', 'Outlet Status', 'Control State', and 'Control Action'. The table lists outlets A1 through B8, all with 'On' status and 'Wake On' control state. A 'Global Control Action' dropdown is set to 'None'. Three callout boxes are present: '1' points to the system header, '2' points to the navigation bar, and '3' points to the row for TowerA\_Outlet3.

Outlet ID	Outlet Name	Outlet Status	Control State	Control Action
A1	TowerA_Outlet1	On	Wake On	None
A2	TowerA_Outlet2	On	Wake On	None
A3	TowerA_Outlet3	On	Wake On	None
A4	TowerA_Outlet4	On	Wake On	None
A5	TowerA_Outlet5	On	Wake On	None
A6	TowerA_Outlet6	On	Wake On	None
A7	TowerA_Outlet7	On	Wake On	None
A8	TowerA_Outlet8	On	Wake On	None
B1	TowerB_Outlet1	On	Wake On	None
B2	TowerB_Outlet2	On	Wake On	None
B3	TowerB_Outlet3	On	Wake On	None
B4	TowerB_Outlet4	On	Wake On	None
B5	TowerB_Outlet5	On	Wake On	None
B6	TowerB_Outlet6	On	Wake On	None
B7	TowerB_Outlet7	On	Wake On	None
B8	TowerB_Outlet8	On	Wake On	None

Example of Firmware Web Interface

## Logging In

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

### To log in by the Web interface:

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.

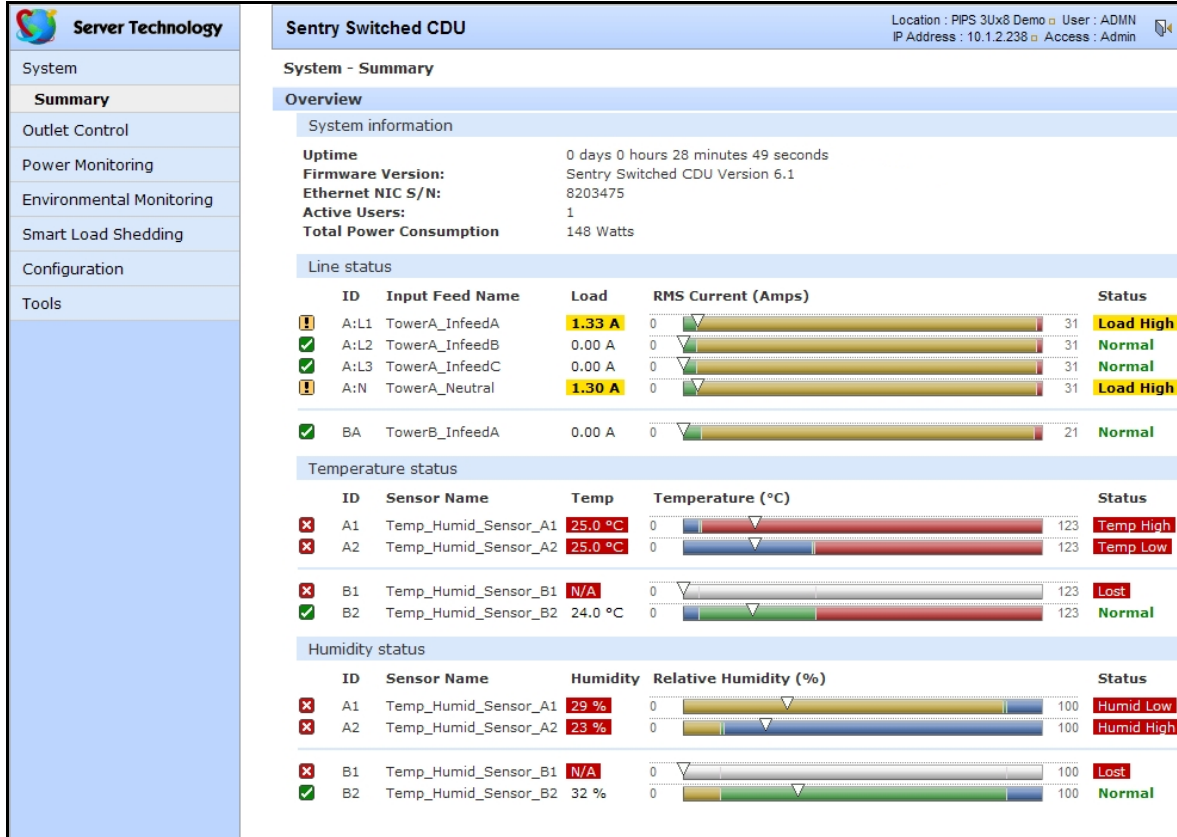
**NOTE:** The default PDU username/password is admn/admn.

## System Summary

The System Summary is typically displayed as the default page at user login to the firmware Web Interface. If you do not have environmental monitor access for a PDU, your default page at login will be the Outlet Control page (shown in Figure 3 above).

Both the System Summary page and the Outlet Control page display automatically at login and do not require enabling.

The System Summary page contains general system, line, humidity, and temperature status information. The color-coded sensor graphs shown in the example below provide a quick and efficient real-time view for monitoring environmental conditions in your PDU network.



### Example of System Summary Page

The System Summary page displays precise current and system power consumption in your PDU network. Dynamic updates (without a full page refresh) allow you to assess critical system statistics with close to instantaneous feedback. This performance is useful for monitoring new installation or power distribution changes in high-density computing environments. Power system administrators can also quickly identify thermal and humidity concerns that might otherwise escalate into costly infrastructure repairs if left unchecked.

As long as the System Summary page is active, the sensor graphs are continually updating system statistics and threshold values. The data with the most impact on the system is displayed to reduce your analysis and troubleshooting time. You can quickly analyze and correct a PDU if a sudden operating condition affects your device network.

**NOTE:** Because the System Summary page continually requests updated status information from the PDU, the page does not time-out. You will need to navigate to another page or manually log off.

## System Information

**Uptime:** Displays the cumulative time the PDU has been up and running since the last unit restarted. Uptime shows continuous, real-time system updates with an approximate 5-second automatic refresh. A manual refresh of the System Summary page is not required.

**Firmware Version:** Shows the current firmware version.

**Ethernet NIC S/N:** Displays the PDU serial number derived from the Ethernet NIC.

**Active Users:** Displays the number of active user sessions accessing the firmware. These sessions include serial, TELNET, SSH, and Web sessions. Active Users also shows sessions that an unauthorized user may be attempting to access. The number shown in Active Users changes instantly as the number of active user sessions change. A total of 4 concurrent web user sessions are allowed (HTTP or HTTPS).

---

**NOTE:** Depending on your web browser, multiple web accesses from the same machine are often treated as one user.

---

**Total Power Consumption:** Displays the total system power (in Watts) being distributed by the current PDU configuration.

## Line Status

The Line Status graph displays a blinking warning (yellow), whenever the total input load on an infeed exceeds the present user set threshold. If an overload occurs, a blinking error condition (red) is displayed. The unit continues to display these yellow and red states until the condition changes or the problem has been resolved.

The default input feed high load threshold is 80% of the input feed maximum load capacity.

---

**NOTE:** The input feed high threshold is user-defined. You must configure this threshold value on the SNMP/Thresholds page or the Command Line Interface (CLI).

---

## Temperature Status

The Temperature Status graph displays a blinking error whenever temperature exceeds the low or high threshold. The PDU will continue to display this state until the condition changes or the problem has been resolved.

For the temperature sensor, the default range of low/high temperature values is 5°-45° C (41°-115° F).

Up to four sets of dual temperature/humidity sensors can be displayed in this graph for a total of eight possible temperature sensor graphs. A thin blue line separates each set based on the tower or environmental monitor.

---

**NOTE:** The temperature threshold values are user-defined. You must configure these threshold values on the SNMP/Thresholds page or the Command Line Interface (CLI).

---

## Humidity Status

The Humidity Status graph displays a blinking error whenever humidity exceeds the low or high threshold. The PDU will continue to display this state until the condition changes or the problem has been resolved.

For the humidity sensor, the default range of low/high humidity percentage is 0-100% (relative humidity).

Up to four sets of dual temperature/humidity sensors can be displayed in this graph for a total of eight possible humidity sensor graphs. A thin blue line separates each set based on the tower or environmental monitor.




---

**NOTE:** The humidity threshold values are user-defined. You must configure these threshold values on the SNMP/Thresholds page or the Command Line Interface (CLI).

---

## Field Descriptions


The following fields and icons are viewed left to right for Line Status, Temperature Status, and Humidity Status:


**Icon:** Provides quick viewing of current operational state: Information , Warning  and Critical .


**ID:** Device input feed or sensor identifier.

**Name:** Descriptive, user-defined name for each input infeed or sensor.

**Load, Temp, Humidity:** Current state of the reported input load (in amps), current temperature, or current percentage of relative humidity.










**Low Limit:** Displays the user-defined low limit of the load, temperature, or humidity graph. These values depend on the sensor limited and cannot be set by the user. For example, a 0°C low limit would be displayed as  for a temperature sensor graph in Celsius.

**Sensor Graph and Level Indicator:** The horizontal sensor graph shows current operating conditions in color-coded segments. See the section below, “Sensor Graph Color Coding” for details. The level indicator  appears across the graph to indicate the relative position of the current data value with respect to the minimum (low limit) and maximum (high limit) values displayed at the left and right of the graph.

**High Limit:** Displays the high limit of the load, temperature, or humidity graph. These values depend on the sensor limits and cannot be set by the user. For example, a 100°C high limit would be displayed as  100 for a temperature sensor graph in Celsius.

**Status:** One of several operating conditions:

### System Summary – Status Descriptions

Icon	Status	Description
	Reading	Unit is reading a new or restored sensor.
	Normal	Indicates normal operation.
	Load High	Infeed current load exceeds present High threshold.
	Over Load	Infeed current load exceeds the measurable range for the infeed.
	Temp Low	Current temperature falls below present Low threshold.
	Temp High	Current temperature exceeds present High threshold.
	Humid Low	Current percentage of relative humidity falls below present Low threshold.
	Humid High	Current percentage of relative humidity exceeds present High threshold.
	Lost	The connection was lost to a sensor that was previously detected and the sensor is pulled from the original environment monitoring statistics. There is no data to report, the graph is meaningless, and the threshold settings remain displayed but are grayed.

### Sensor Graph Color-Coding

The following colors change dynamically on the sensor graphs to communicate operating conditions:

#### *Line (Load) Status:*

Green = Normal

Yellow = High load (load configured by user)

Red = Overload (based on device characteristics)

User configures load capacity at **Configuration > SNMP/Thresholds > Input Feed Traps and Thresholds**

#### *Temperature Status:*

Blue = cold; low temperature (threshold configured by user)

Green = acceptable temperature range

Red = hot; high temperature (threshold configured by user)

User configures low/high temperature thresholds at **Configuration > SNMP/Thresholds > Sensor Traps and Thresholds**

#### *Humidity Status:*

Blue = wet; high humidity (threshold configured by user)

Green = acceptable percentage of relative humidity

Yellow = dry; low humidity (threshold configured by user)

User configures low/high relative humidity thresholds at **Configuration > SNMP/Thresholds > Sensor Traps and Thresholds**

## Logical Group Separators

Logical groups are separated by a thin blue line on the System Summary page as shown in the following example between Tower A\_InfeedA and Tower B\_InfeedA:

Line status						
	ID	Input Feed Name	Load	RMS Current (Amps)		Status
✓	AA	TowerA_InfeedA	0.00 A	0		21 Normal
✓	BA	TowerB_InfeedA	0.25 A	0		21 Normal

This grouping includes master/link units in addition to some branched units.

Up to three blue line dividers can be displayed on the System Summary page between all sensor groups.

## 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 PDU by the outlet, the current Control State being applied by the PDU, and the outlet load in amperes.

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

### Individual

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

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

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

## Outlet State/Control State Field Values

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

## Environmental Monitoring

### Sensors

The Sensors page displays:

- Absolute and descriptive names of the temperature/humidity sensor
- Temperature/humidity sensor readings and percentage of relative humidity

Monitor pages (like the Sensors page) refresh occasionally to reflect current PDU status.

### Temperature/Humidity Sensor Status

Status	Description
Found	The PDU found the sensor and connection is established.
Not Found	On a fresh reboot, the PDU does not find a sensor.
Lost	The connection to a previously found sensor is now lost.
No Comm	Communication loss occurred due to a hardware issue (not loss of communication with the probes). <sup>1</sup>

<sup>1</sup> = The ENV part of the sensor supports two Temperature/Humidity (T/H) probes as part of the master unit, two T/H probes as part of the link unit, and the optional EMCU-1-1 (which can support two T/H probes, four contact-closure monitoring points, and one water sensor). The “No Comm” sensor status is not loss of communication with probes themselves.

## 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 can be used for the location description only.

## Creating a pre-login banner:

Click the **Login Banner** link. On the subsequent Login Banner page, type pre-login banner text and click **Apply**.

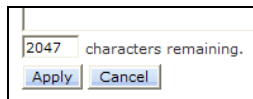
---

### NOTES:

- The pre-login banner can be up to 2069 characters in length and is displayed prior to the login prompt. If left blank, a system banner will not be displayed prior to the login prompt.
- For an SSH connection, the banner length is truncated to 1500 bytes in SSH packets to avoid failure of the SSH connection when configured with a long login banner.

---

The Login Banner displays the following Characters Remaining box to show you in real-time as you type how many of the 2069 maximum characters are still available for you to complete your banner. The box adjusts dynamically as you type or delete characters.



If you reach the maximum 2069 characters, the box displays “-1”. To clear your entry and start over, click **Cancel**.

## 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 click **Apply**.

## Configuring the LED display orientation:

From the Display Orientation drop-down list, select **Normal** or **Inverted**, and click **Apply**.

---

### NOTES:

- Only specific PDU models are equipped with an accelerometer chip that senses device orientation. If equipped, your PDU automatically aligns the LED display orientation (depending on its current direction), and the option “Auto” displays in the Display Orientation drop-down list by default. In addition, the actual mounting of the unit, such as “<Normal> or <Inverted>”, appears to the right of the “Auto” option. However, even if your PDU model does have the sensor for device orientation, you can still select the Normal or Inverted option from the list to override the capability of the hardware.
- If your PDU model does not have the accelerometer chip, you will need to configure the LED display orientation by selecting Normal or Inverted.

---

## 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 configuration reset button:

Select **Enabled** or **Disabled** from the Configuration 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**.

## 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**.

### Setting the temperature scale:

Select **Celsius** or **Fahrenheit** from the Temperature Scale drop-down menu and click **Apply**.

### Setting the system area (footprint):

Enter a system area value in the Area (Footprint) field and click **Apply**.

### Setting the system area unit of measure:

Select Square Feet or Square Meters from the Area (Footprint) drop-down menu and click **Apply**.

### Setting the power factor:

The Power Factor value calculates the power usage displayed in the Power Monitoring pages.

Type a numeric value in the Power Factor field (from 0.50 to 1.00) and click **Apply**.

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

The threshold (percentage) specified determines when the current on the lines of a 3-phase system are out-of-balance between the three phases of power. If the alerting feature is enabled, an alert will be sent when an out-of-balance condition occurs.

In the 3-Phase Load Out-of-Balance Threshold field, type a value from 0 to 100%, and click **Apply**.

### Setting the 3-phase load out-of-balance alerting:

This setting enables/disables the sending of an alert when the current on the lines of a 3-phase system are past a pre-set threshold (percentage) and are out-of-balance between the three phases of power.

From the 3-Phase Load Out-of-Balance Alerting drop-down menu, select **Enabled** or **Disabled**, and click **Apply**.

---

#### NOTES:

- When a device with 3-phase input voltage is out-of-balance, efficiency is reduced and the unit is prevented from reaching maximum capacity. When an alert for the out-of-balance condition is received (if the alerting feature is enabled), it may be necessary to adjust distribution of the loads.
  - For 3-phase systems, if the Out-of-Balance Alerting feature is enabled, and the system goes into a load out-of-balance condition, the Tower Status field on the “Power Monitoring – System” web page will display the alert “3ph Out-of-Balance”, unless there is a higher priority tower error state to report.
- 

### Configuring the Command Line Interface (CLI) session timeout:

Enter a timeout period (in minutes) in the CLI Session Timeout field, and click **Apply**.

The valid timeout range is 1 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 outlet name:

Click on the **Outlet Names** link which will open the Outlets configuration page.

### Creating a descriptive serial port name:

Click on the **Serial Port Names** link which will open the Serial Ports configuration page.

### 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 can configure the IP address, subnet mask, gateway address, DNS addresses as well as view the link status, speed and duplex value.

The PDU 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.

---

### Enabling or disabling Dynamic Host Configuration Protocol (DHCP) support:

To enable DHCP, check the Enable checkbox. To disable DHCP, uncheck the checkbox. Click **Apply**.

### Enabling Dynamic Host Configuration Protocol (DHCP):

To enable DHCP, check the Enable checkbox. To disable DHCP, uncheck (clear) the checkbox.

Click **Apply**.

### Setting the Fully-Qualified Domain Name (FQDN):

To enable FQDN, check the Enable checkbox and accept the default name “sentry3-521384” (or type a different name). To disable FQDN, uncheck (clear) the checkbox.

Click **Apply**.

### Enabling the DHCP boot delay:

To enable the boot delay, check the Enable checkbox. To disable the boot delay, uncheck (clear) the checkbox.

Click **Apply**.

- Enabling the Boot Delay option gives the PDU approximately 100-seconds to establish a connection through a DHCP server. This interval allows various network component activities to occur as the CDU powers up (such as obtaining SNTP time stamps for logging). This is the default state.
- Disabling the Boot Delay option forces the CDU to boot after approximately 5-seconds regardless of the DHCP acquisition state. This speeds up a boot when a DHCP server is connected to one of the outlets in the CDU. In this configuration, SNMP traps, SNTP, and other protocols will not be available until a DHCP address has been resolved.

---

#### NOTES:

- The Boot Delay option executes only when DHCP is enabled.
  - The firmware can detect network link integrity and will wait for network connection. This means that if the network is not currently connected, the enabled Boot Delay option will be ignored.
- 

### Enabling static address fallback:

---

**NOTE:** The Static Address Fallback option executes only when DHCP is enabled.

---

To enable static address fallback, check the Enable checkbox. To disable, uncheck (clear) the checkbox.

Click **Apply**.

- Enabling the Static Address Fallback option informs the PDU to automatically fall back to a static address if a DHCP server does not respond after 100-seconds. This is the default state.
  - Disabling the Static Address Fallback option generates DHCP server requests until the PDU obtains a dynamic address.
- 

**NOTE:** If the DHCP server boot time is excessive, you may need to disable the DHCP Static Address Fallback option.

---

## 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.

### Enabling or disabling Telnet or SSH support:

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

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

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

### Enabling or disabling SSH server authentication methods:

The SSH server supports the Password and the Keyboard-Interactive authentication methods for security.

Password is an authentication method in which 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 in which 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 used 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 click **Apply**.

## HTTP/SSL

The HTTP/SSL page configures HTTP server options, SSL options (including user-defined certificates), and determines settings for the PDU Power Manager (SPM) enterprise software product.

### Enabling or disabling HTTP or SSL support:

From the HTTP or SSL Server drop-down menu, select **Enabled** or **Disabled**, and click **Apply**.

---

**NOTE:** SSL-encrypted (HTTPS) must be used for secure website connections.

---

### Setting SSL secure access:

SSL allows either optional or required connections. The default secure access is optional.

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

From the Secure Access drop-down menu, select **Optional** or **Required**, and click **Apply**.

### Changing the HTTP server or SSL port number:

In the HTTP or SSL section of the page, in the Port field, type the port number, and click **Apply**. The HTTP default port number is 80; the SSL default port number is 443.

### Uploading a custom user certificate:

#### *Enabling and disabling user certificates:*

In the User Certificate drop-down menu, select Enabled. Provide a passphrase (0-47 characters) for the new certificate. To change the passphrase, type a new passphrase and check the Change checkbox. Click **Apply**.

The Stored Files section displays a message to confirm the upload status of the user certificate and its related public key.

## Custom User Certificate Messages

Message	Description and Valid Values/Range
Cert & Key	Both the user certificate and its key were uploaded successfully.
Cert	User certificate was uploaded without a key.
No Cert	User certificate was not uploaded.
Factory Encrypted	User certificate was encrypted and uploaded at product assembly.
None	Neither the user certificate nor its key were uploaded.

### *Uploading the certificate:*

**NOTE:** You can enable user certificates and provide a passphrase using either the firmware Web interface or the Command Line Interface (CLI). However, the uploading of a custom user certificate can only be done using the Web interface – there are no equivalent commands for uploading user certificates.

To upload a user certificate, click the **Upload** link. The Upload window displays. Type the certificate filename (or key filename) and click the **Upload** button. The upload status is displayed in the Stored Files section as described above.

### *Removing a certificate:*

To remove a user certificate, click the **Remove** link. A message displays to confirm the removal of the certificate.

## Setting the PDU Power Manager (SPM) options:

The PDU Power Manager (SPM) is Server Technology's enterprise management software product for the data center. The configuration options provided allow you to enable/disable SPM and reset the SPM password to its default.

**NOTE:** The SPM options apply only if you are currently using Server Technology's SPM software.

### *SPM Secure Access:*

If your operation does not currently use SPM software, you can disable SPM Secure Access. However, if disabled, the PDU will not be able to use the SPM suite of secure network capabilities or the advanced remote configuration.

Select **Enabled** or **Disabled** from the SPM Secure Access drop-down menu and click **Apply**.

**NOTE:** Both HTTP and SSL must be enabled or the SPM Secure Access option will not be permitted. When SPM Secure Access is permitted, the default is **Enabled**.

### *SPM Password:*

Each PDU has a default unique SPM password that is used to communicate between SPM and the PDU. When SPM discovers a PDU in the network, SPM changes this password into a different unique password for added security. The SPM then continues to manage or alter these passwords as required for system security.

If a PDU is relocated or swapped from the system after a password was generated, SPM may not be able to re-establish a connection to the unit. The Set SPM Reset Password command allows you to reset to the internal default password of the PDU so SPM can re-discover the device and add it to the system. Once the unit has been acquired by SPM, no further action is necessary.

To reset the password, check SPM Password and click **Apply**.

**NOTE:** Do not reset the password if SPM communication has already been established.

## **Serial Ports**

The Serial Ports configuration page allows maintenance to the serial port.

---

**NOTE:** Pass-Thru connections can 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 click **Apply**.

### **Setting the serial port timeout value:**

The Serial Port Timeout Value sets the serial port inactivity timeout period for individual ports. The timeout period defines the maximum period of inactivity before automatically closing the Pass-Thru session.

The valid range for the timeout is 0 to 60 (in minutes). The default timeout is 5 minutes. Setting the timeout value to “0” disables the timeout.

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

Type the timeout minutes in the Connection Timeout field and click **Apply**.

### **Creating a descriptive serial port name:**

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

On the following Serial Ports 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 following Serial Ports Edit page, select **On** or **Off** from the DSR Check drop-down menu and click **Apply**.

### **Enabling or disabling the Command Line Interface (CLI):**

This option enables or disables availability of the CLI for issuing action commands to the PDU. If disabled, only the Firmware Web user interface will be available.

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

On the following Serial Ports Edit page, select **Enabled** or **Disabled** from the CLI drop-down menu and click **Apply**.

### **Enabling or disabling the Serial Command Protocol (SCP):**

This option allows SCP functions to be enabled or disabled for a specific serial port.

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

On the following Serial Ports Edit page, select **Enabled** or **Disabled** from the SCP drop-down menu and click **Apply**.

---

#### **NOTES:**

- Upon a coldboot of the system, if the Coldboot Alert feature is enabled, the system will send a ½ second RS-232 break out to any SCP-enabled serial ports.
  - The SCP option must be enabled to use the Bluetooth Android solution.
- 

### **Enabling or disabling the Serial Command Protocol (SCP) emulation:**

This option notifies SCP of an MRV device on a specific serial port.

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

On the following Serial Ports Edit page, select **None** or **MRV** from the SCP Emulation drop-down menu and click **Apply**.

### **Enabling or disabling the RFTAG option:**

This option makes RF Code sensor tags available for the Server Technology wireless monitoring solution.

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

On the following Serial Ports Edit page, select **Enabled** or **Disabled** from the RFTAG drop-down menu and click **Apply**.

## Configuring the Bluetooth™ options:

If the PDU has been equipped for the mobile monitoring solution using Bluetooth® technology, several Bluetooth parameters will be available for editing on the Serial Ports configuration page.

Click the **Edit** link in the Action column to configure the following parameters.

Provide a value as described for each parameter field, and click **Apply**.

### Firmware Bluetooth Parameters

Parameter	Description and Valid Values/Range
Bluetooth Name	Descriptive name of the Bluetooth module that displays in the list of discovered modules on the Android device. The default module name is "ST Eye". The name cannot be blank; maximum Valid range is 1-31 characters.
Bluetooth Discoverability	Settings that determine the current status of the pushbutton on the Bluetooth module. <ul style="list-style-type: none"><li>• Always – The Bluetooth module is discoverable, even without pressing the pushbutton.</li><li>• Limited – (Default). The pushbutton on the Bluetooth module must be pressed to make the module discoverable for 60-seconds.</li><li>• Never – The Bluetooth module is never in discoverable mode.</li></ul>
Bluetooth Pin Code	The pin code is available for legacy Bluetooth modules that require a pin to pair the module. Although not used in current Bluetooth modules, the pin code is supported if needed. Default is 9611; must be 4-digits; range is 0000 to 9999.
Bluetooth Transmission Power	Designated transmission power (dbm) for the Bluetooth module. Note that lowering the transmission power reduces the effective range of the module. Default is 0; range is -6 to 4 dbm.

## Groups

The Groups configuration page allows you to create and delete groups and to assign 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 click **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 click **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 PDU 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 can also grant administrative privileges to other user accounts allowing the unit to have more than one administrative-level user.

---

**NOTE:** You cannot remove administrative privileges from the default **admin** user unless you have already granted administrative access to another user account.

---

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 click **Apply**.

## Granting or removing environmental monitoring access:

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 click **Apply**.

---

**NOTE:** Granting access to environmental monitoring (temperature/humidity/sensors) to a non-admin user also grants that user access to power monitoring (outlets, infeeds, towers – all the environmental data of the PDU).

---

## 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 click **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 click **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 click **Apply**.

## **FTP**

The FTP configuration page allows you to set up and maintain all settings required to perform an FTP firmware upload, configure automatic FTP updates, or system configuration uploads/downloads.

---

### **NOTES:**

The FTP page accepts both IPv4 and IPv6 formats in the Host field.

- Secure File Transport Protocol (SFTP) is also supported for encrypted SSH transport over the network.
- 

### **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 PDU features the ability to schedule automatic firmware updates. When enabled and configured, the PDU 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 PDU features the ability to upload and download system configuration files to ease implementation across multiple Sentry devices.

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 page sets the options for the SNTP server, time zone, Daylight Saving Time (DST) automatic clock adjustment, and Syslog server.

### ***About Daylight Saving Time(DST)***

Support for DST is disabled by default. When enabled, the date and time are automatically adjusted forward one hour between the starting and ending dates and times (which can be configured).

---

**NOTE: If Daylight Saving Time (DST) is enabled, all system time displays will be shown with the current DST start/end date/time settings.**

---

The default time zone is set for the United States until at least 2015.

The time zone format is: **mo.w.d/h:m:s**, as follows:

**mo** = month from January to December (1-12)  
**w** = week number (1-4) or the last week (5)  
**d** = day of week from Sunday to Saturday (0-6)  
**h** = hour (0-23)  
**m** = minute (0-59)  
**s** = second (0-59)

### **Setting the local date/time:**

The Date/Time (Local) field shows the current DST settings. To increment the settings – based on updates to the start/end day/time options – click **Update**.

### **Setting the SNTP primary/secondary server address:**

The Primary/Secondary Host fields contact the SNTP server; the fields are populated with the external NTP pool time zones “2.servertech.pool.ntp.org” and “1.servertech.pool.ntp.org” as default for new PDUs that have not yet been time set.

Enter the IP address or hostname in the Primary Host and/or Secondary Host field and click **Apply**.

### **Setting the Local GMT offset (hours/minutes):**

The GMT offset supports all standard international time zones from -12:59 to +14:59. The GMT offset can be set in minutes to accommodate partial-hour time zones.

Select the local offset from GMT value from the drop-down menu and click **Apply**.

### **Enabling or disabling Daylight Saving Time (DST):**

Select **Enabled** or **Disabled** from the SNMPv3 Agent drop-down menu and click **Apply**.

### **Setting Daylight Saving Time (DST) start/end date/time options:**

Select the week/day/month and hour/minute/second for the start date/time and end date/time from the drop-down menus and click **Apply**.

### **Setting the Syslog server address:**

Enter the IP address or hostname in the Primary and/or Secondary Host field, and click **Apply**.

---

**NOTE: Both IPv4 and IPv6 formats are accepted in the Primary/Secondary Host fields.**

---

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

In the Syslog Port field, enter the port number and click **Apply**.



## **SNMP/Thresholds**

The SNMP/Thresholds configuration page allows setup and maintenance of all SNMP agent settings required to enable SNMP. The page also provides access to the trap configuration pages for towers, input feed, environmental monitor, and sensors.

---

**NOTE:** Traps are generated according to a hierarchical architecture; for example, 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.

---

### **About SNMP versions:**

The firmware supports SNMP versions 1, 2, and 3.

SNMP version 3 supports authentication and encryption on a per user basis. Authentication types are None and MD5. Encryption types are None and DES. If you use authentication, you must use encryption.

Two SNMPv3 users are supported: one user with read-write (RW) access, and one user with read-only (RO) access. Both users have the same configuration parameters, and you can configure each user independently.

SNMPv2 and SNMPv3 can be enabled or disabled independently. You can have SNMPv2 and/or SNMPv3, or none.

### **Enabling or disabling SNMP v3 support:**

Select **Enabled** or **Disabled** from the SNMPv3 Agent drop-down menu and click **Apply**.

---

**NOTE:** The default for SNMP support is **Enabled**. When Server Technology products are shipped, the default SNMP configuration for the GET community string is set to “**public**” and the SET community string is left **blank**.

---

### **Setting the SNMPv3 read-write (RW) user or read-only (RO) user:**

Enter the Read-Write User or Read-Only User username and click **Apply**. A valid username can be set to any value between 1-31 characters.

### **Configuring the SNMPv3 read-write (RW) user or read-only (RO) user authentication type:**

From the Read-Write User or Read-Only User Authentication Type drop-down menu, select None or MD5, and click **Apply**. To clear the password, check **Change Password**.

### **Setting the SNMPv3 read-write (RW) user or read-only (RO) user authentication password:**

Enter the Read-Write (RW) User or Read-Only (RO) User Password and, and click **Apply**. To clear the password, check **Change Password**. A valid authentication password can be set to any value between 1-39 characters. A blank password will clear the string.

### **Configuring the SNMPv3 read-write (RW) user or read-only (RO) user privacy type:**

From the Read-Write User or Read-Only User Privacy Type drop-down menu, select None or DES, and click **Apply**. To clear the password, check **Change Password**.

### **Setting the SNMPv3 read-write (RW) user or read-only (RO) user privacy password:**

Enter the Read-Write User or Read-Only User privacy password and, and click **Apply**. To clear the password, check **Change Password**. A valid password can be set to any value between 1-31 characters.

### **Setting the SNMPv3 trap username:**

The optional trap username displays on SNMP activity logs to identify user actions.

Type a name in the Trap Username field and click **Apply**. The trap username can be 1-31 alphanumeric characters; spaces are allowed; and the name is case sensitive.

## Configuring general parameters for any SNMP version:

### *Setting trap destinations:*

Type an IP address or hostname as necessary in the trap destination field(s) and click **Apply**.

---

**NOTE:** Both IPv4 and IPv6 formats are accepted in the “Trap Destination 1” and “Trap Destination 2” fields.

---

### *Setting the error trap repeat time:*

Type a time value in the Error Trap Repeat Time field and click **Apply**. The valid range is 1 to 65535 (in seconds).

### *Setting the trap format version:*

The SNMP Trap Format configures the SNMP trap format version. The trap format can be SNMP v1, v2, or v3. The default is v1, regardless of the versions that are enabled for the agent.

From the Trap Format drop-down menu, select the v1, v2, or v3 option and click **Apply**.

### *Setting IP restrictions:*

From the IP Restrictions drop-down menu, select the No Restrictions or Trap Destinations Only option and click **Apply**.

---

**NOTE:** When the Trap Destinations Only option is selected, SNMP Manager Get and Set requests are allowed only from the IP address of the defined trap destinations.

---

### *Setting the SNMP SysName, SysLocation or SysContact objects:*

In the appropriate field, enter the SysName, SysLocation or SysContact objects and click **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 click **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 click **Apply**.

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

### *Configuring Temperature and Humidity Recovery Delta (Hysteresis):*

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 (hysteresis), in the Recovery Delta field for “Temp”, type a value (in degrees) and click **Apply**. Valid range is 0-30 Celsius or 0-54 Fahrenheit.

To configure a humidity recovery delta (hysteresis), in the Recovery Delta field for “Humid”, type a value (in percent) and click **Apply**. Valid range is 0-20%.

---

**NOTE:** The default value for the Recovery Delta field is 1 degree Celsius and 2 degrees Fahrenheit.

---

### ***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 click **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.

### **Enabling or disabling LDAP support:**

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

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

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

---

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

---

### **Setting the LDAP server address:**

Enter the IP address or hostname in the Primary and/or Secondary Host field and click **Apply**.

---

**NOTE:** Both IPv4 and IPv6 formats are accepted in the Primary/Secondary Host fields.

---

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

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

### **Setting the LDAP bind type:**

The PDU supports three standard LDAP bind methods:

**Simple:** Uses unencrypted delivery of username-password over the network to the LDAP server for authentication, showing user credentials in plain text.

**TLS/SSL:** (LDAP over TLS/SSL) Uses a trusted authority certificate to provide encryption of LDAP authentication.

**MD5:** Provides strong protection using 1-way hash encoding that does not transmit the username-password over the network.

From the Bind Type drop-down menu, select Simple, TLS/SSL, or MD5, and click **Apply**.

---

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

---

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

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

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

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

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

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

### **Setting the user search filter:**

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

### **Setting the group membership attribute:**

Enter the group membership attribute in the Group Membership Attribute field and click **Apply**.

### Enabling or disabling group search:

Select **Enabled** or **Disabled** from the Group Search drop-down menu and click **Apply**.

### Setting the group search base Distinguished Name (DN):

The Group Search Base DN indicates where the LDAP group search will start.

Enter the Base DN in the Group Search Base DN field and click **Apply**.

### Setting the user membership attribute name:

The User Membership Attribute is a comma-delimited string of up to two attribute names whose values in the search results are the users that are members of the group. Maximum numbers of characters is 61.

Enter the user membership attribute name(s) in the User Membership Attribute field and click **Apply**.

---

**NOTE:** The user membership option allows the searching of directory entries of groups for a user membership attribute to find the groups for which the user is a member.

---

### Setting the DNS IP address:

For information about how to set the DNS IP address, see the [Network](#) section.

### 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 click **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 click **Apply**.

#### *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 click **Apply**.

---

**NOTE:** Granting access to environmental monitoring (temperature/humidity/sensors) to a non-admin user also grants that user access to power monitoring (outlets, infeeds, towers – all the environmental data of the PDU).

---

#### *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 click **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 click **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 click **Apply**.

## **TACACS+**

The TACACS+ configuration page is used for setup and maintenance of all settings required to enable TACACS+ support.

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

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

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

Enter the IP address or hostname in the Primary and/or Secondary Host field and click **Apply**.

---

**NOTE:** Both IPv4 and IPv6 formats are accepted in the Primary/Secondary Host fields.

---

### **Changing the TACACS+ server port:**

Enter the port number in the Port field and click **Apply**.

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

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

For more information about remote authentication order, see the “Setting the authentication order” section.

---

**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 click **Apply**.

#### ***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 click **Apply**.

---

**NOTE:** Granting access to environmental monitoring (temperature/humidity/sensors) to a non-admin user also grants that user access to power monitoring (outlets, infeeds, towers – all the environmental data of the PDU).

---

#### ***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 click **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 click **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 click **Apply**.

## **RADIUS**

The Remote Authentication Dial-in User Service (RADIUS) configuration allows you to set up and maintain the settings required to enable RADIUS support.

### **Enabling or disabling RADIUS support:**

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

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

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

For more information about remote authentication order, see the “Setting the authentication order” section.

---

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

---

### **Changing the RADIUS server address:**

Enter the IP address or hostname in the Primary and/or Secondary Server field and click **Apply**.

---

**NOTE:** Both IPv4 and IPv6 formats are accepted in the Primary/Secondary Host fields.

---

### **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 click **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 click **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.

Type the timeout value (in seconds) in the Primary and/or Secondary Timeout field and click **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 PDU will attempt authentication with the primary server until the number of retries is reached, then will attempt authentication with the secondary server. If the PDU does not receive a response from these attempts, the authentication request will be rejected.

#### ***Setting the number of retries:***

Type the number of retries in the Primary and/or Secondary Retries field and click **Apply**.

The valid retries range is 0-10; default is 2.

## **SMTP/Email**

The SMTP/Email page allows the configuration of Simple Mail Transfer Protocol (SMTP) and Email options.

### **Enabling or disabling Email support:**

Select **Enabled** or **Disabled** from the Email Notifications drop-down menu and click **Apply**.

### **Setting the SMTP server address:**

Enter the IP address or hostname in the SMTP Host field and click **Apply**.

---

**NOTE:** Both IPv4 and IPv6 formats are accepted in the Host field.

---

### **Changing the SMTP server port:**

Enter the port number in the SMTP Port field and click **Apply**.

### **Setting the SMTP authentication type:**

---

#### **NOTES:**

- SMTP authentication allows the mail client in the PDU to login to the mail server during the process of sending a mail. The mail server may require this login to relay mail to another mail server.
  - Supported SMTP authentication types are: None (default, no SMTP authentication); Digest-MD5; CRAM-MD5; Login; and Plain. SMTP authentication occurs with a configured username and password, or you can use the address in the 'From' Address field in place of the username.
- 

From the SMTP Authentication drop-down menu, select an authentication method. From the "with" drop-down menu, select "SMTP Username" or "From Address". Click **Apply**.

### **Setting the Email SMTP authentication username:**

In the Username field, type the desired Email SMTP username and click **Apply**. Spaces are not allowed.

### **Setting the Email SMTP authentication password:**

The Set Email SMTP Password command sets the password for SMTP authentication with the username.

In the Password field, type a password of 1-16 alphanumeric and other characters (ASCII 33 to 126 decimal) are allowed; passwords are case sensitive. Click **Apply**.

To change the password, type over it, check the Change checkbox, and click **Apply**.

### **Setting the 'From' email address:**

Enter the 'from' email address in the 'From' Address field and click **Apply**.

### **Setting the 'Send To' email address:**

Enter the 'send to' email address in the Primary or Secondary 'Send To' Address field and click **Apply**.

If the primary 'send to' address fails, the system then attempts to send the email to the secondary 'send to' address.

### **Setting the subject ID:**

From the Subject ID drop-down menu, select the default "Sentry3\_524640" option or the "Location" option to specify the email subject line. Click **Apply**.

### **Enabling or disabling event type notifications:**

Check the type of event message to enable, and click **Apply**. Options are Event Messages, Authentication Messages, power Messages, and Configuration Messages.

### **Sending a test email:**

After providing information in the Email/SMTP web page, click the **Test** button to send a test email to the target email destinations.

## **Features**

The Features configuration page allows you to activate and maintain the special features purchased from Server Technology. From this page you can review all activated features and activate new purchased features.

### **To activate a special feature:**

In the Feature Key Value field, enter the activation key provided by Server Technology and click **Apply**.

---

**NOTE:** A restart of the PDU 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 tests the ability of the PDU to contact an IP address for another Ethernet-enabled device. For LDAP support, Ping tests the configuration of the Domain Name Server (DNS) IP address by testing for proper name resolution.

---

**NOTE:** Both IPv4 and IPv6 formats are accepted in the Ping Host Name/IP Address field.

---

### **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**.

### **Firmware**

The Firmware page allows the uploading of a system firmware (.bin) file. Click Browse to locate the .bin firmware file, and then click Upload. A confirmation message is displayed.

### **View Log**

The View Log feature enables viewing of the internal system log. This feature 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 more information about configuration requirements, see the “Logging” section.

---

**NOTE:** Only system administrators can view the system log.

---

### **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 click **Apply**.

---

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

---

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

For more information about resetting a PDU to factory defaults from the Web interface, see Appendix A.

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

For more information about uploading new firmware from the Web interface, see Appendix B.

#### **Generating a new SSL X.509 certificate:**

Select the **Restart and generate a new X.509 certificate** from the Action drop-down menu and click **Apply**.

#### **Computing new SSH security keys:**

Select the **Restart and compute new SSH keys** from the Action drop-down menu and click **Apply**.



## Command Line Interface

**IMPORTANT:** The Command Line Interface (CLI) was modified to allow both IPv4 and IPv6 settings.

### 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 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. For more information, see the “Creating a location description” section.

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

#### Operations Command Summary

Command	Description
Connect	Connects to a serial/Pass-Thru port
Envmon	Displays the status of the integrated Environmental Monitor
IStat	Displays the status of the infeeds
List Group	Lists all assigned outlets for a group name
List Groups	Lists all accessible groups for the current user
List Outlets	Lists all accessible outlets for the current user
List Ports	Lists all accessible serial/Pass-Thru ports for the current user
Login	Ends the current session and brings up the Username: prompt
Logout	Ends a session
Off	Turns one or more outlets off
On	Turns one or more outlets on
Password	Changes the password for the current user
Quit	Ends a session
Reboot	Reboots one or more outlets
Status	Displays the on/off status of one or more outlets
UPSStat	Displays the status of the associated UPSs
Add Grouptouser	Grants a user access to one or more groups
Add Outlettogroup	Adds an outlet to a group name
Add Outlettouser	Grants a user access to one or all outlets
Add Porttouser	Grants a user access to one or all serial/Pass-Thru ports
Create Group	Adds a group name
Create UPS	Adds a UPS association

## Administrative Command Summary

---

Create User	Adds a user account
Delete Groupfromuser	Removes access to one or more groups for a user
Delete Outletfromgroup	Deletes an outlet from a group name
Delete Outletfromuser	Removes access to one or all outlets for a user
Delete Portfromuser	Removes access to one or all serial/Pass-Thru ports
List User	Displays all accessible outlets/groups/ports for a user
List Users	Displays privilege levels for all users
Remove Group	Deletes a group name
Remove UPS	Deletes a UPS association
Remove User	Deletes a user account
Restart	Performs a warm boot
Set Banner	Set the pre-login banner text
Set Bluetooth Discover	Determines the current status of the pushbutton on the Bluetooth module
Set Bluetooth Name	Configures the name of the discovered Bluetooth module on the Android device
Set Bluetooth Pincode	Pin code value for legacy Bluetooth modules that require a pin to pair the module
Set Bluetooth Transpwr	Designated transmission power (dbm) for the Bluetooth module.
Set DHCP	Enables or disables DHCP support
Set DHCP Boot Delay	Enables or disables a 100-second boot delay between PDU and DHCP server
Set DHCP Static Address Fallback	Enables or disables DHCP fallback to a static IP address
Set DNS	Sets the IP address of the Domain Name server
Set EnergyWise	Enables or disables the Cisco EnergyWise network
Set EnergyWise Domain	Sets the Cisco EnergyWise domain name
Set EnergyWise Port	Sets the Cisco EnergyWise port number
Set EnergyWise Refresh	Rate (in seconds) at which information is pushed to the EnergyWise manager
Set EnergyWise Secret	Sets the Cisco EnergyWise secret
Set Envmon Name	Specifies a descriptive field fro the integrated Environmental Monitor
Set Envmon THS Name	Specifies a descriptive field for a temperature-humidity sensor
Set FTP Autoupdate Day	Sets the automatic FTP update day
Set FTP Autoupdate Hour	Sets the automatic FTP update hour
Set FTP Autoupdate	Enables or disables automatic FTP update support
Set FTP Directory	Specifies the directory for the file to be uploaded
Set FTP Filename	Specifies the file to be uploaded via FTP
Set FTP Host	Sets the FTP Host IP address or hostname
Set FTP Password	Sets the password for the FTP Host
Set FTP Test	Validates that the PDU can login to the FTP server and verify/download the firmware file
Set FTP Server	Enables or disables the FTP server
Set FTP Username	Sets the username for the FTP Host
Set Gateway	Sets the gateway of the PDU
Set HTTP	Enables or disables HTTP access and sets the HTTP target port.
Set HTTP Port	Specifies the target port for HTTP access
Set Infeed Loadmax	Specifies the maximum load capacity for the infeed
Set Infeed Name	Specifies a descriptive field for the infeed
Set Infeed Voltage	Specifies the nominal input voltage for the infeed
Set IP Address	Sets the IP address of the PDU
Set LDAP UseTLS	Enables or disables LDAP over TLS/SSL support

## Administrative Command Summary (continued...)

Set Location	Specifies a descriptive field for the Web control screen and login banner
Set Net	Determines the acquisition method for the protocol stack and IPv4/IPv6 addresses
Set Option Button	Enables or disables the external configuration reset button
Set Option Coldboot Alert	Enables or disables the Coldboot Alert feature using a serial protocol
Set Option Display	Sets the LED orientation for external Current displays
Set Option More	Enables or disables the 'more' prompt
Set Option Outlet Sequence	Configures outlet power-on sequence order as normal or reversed
Set Option Prompt	Configures a custom CLI prompt
Set Option StrongPasswords	Enables or disables strong password requirements
Set Option Tempscale	Sets the Environmental Monitor temperature scale
Set Option CLI Timeout	Sets the Command Line Interface (CLI) session timeout period
Set Option Web Timeout	Sets the web session (Web Interface) timeout period
Set Outlet Locked	Locks or unlocks a single outlet (no control) in its current state
Set Outlet Name	Specifies a descriptive field for a device attached to an outlet
Set Outlet PostOnDelay	Sets the Post-On delay for an outlet
Set Outlet RebootDelay	Sets the reboot delay for all outlets
Set Outlet SeqInterval	Sets the sequencing interval for all outlets
Set Outlet Wakeup	Sets the wakeup state for an outlet
Set Port CLI	Enables or disables availability of the Command Line Interface (CLI)
Set Port DSR Check	Sets the DSR active signal checking for a serial/Pass-Thru port
Set Port Name	Specifies a descriptive field for a serial/Pass-Thru port
Set Port SCP	Enables or disables Serial Command Protocol (SCP) functions
Set Port SCP Emulate	Notifies the Serial Command Protocol (SCP) of an MRV device on a specific serial port
Set Port Speed	Set the connection speed for all serial/Pass-Thru ports
Set Port Timeout	Sets the inactivity timeout period for a serial port before closing the pass-thru session
Set Port RFTag	Enables or disables RF Code sensor tags for the wireless monitoring solution
Set SCPAuth	Enables or disables Serial Command Protocol (SCP) authentication
Set SCPAuth User	Sets the username and password for Serial Command Protocol (SCP) authentication
Set SNMP IP Restrict	Allows SNMP Get and Set requests only from defined trap destinations
Set SNTP	Sets the IP address or hostname of the SNTP servers
Set SNTP DST	Enables or disables Daylight Saving Time (DST)
Set SNTP DST End	Specifies the settings for DST day/time end parameters
Set SNTP DST Start	Specifies the settings for DST day/time start parameters
Set SNTP GMTOffset	Sets the local GMT offset applied to the SNTP date/time
Set SPM	Enables/disables secure access of Sentry Power Manager (SPM)
Set SPM Reset Password	Resets the SPM password on the PDU to its internal default password
Set Subnet	Sets the subnet mask of the PDU
Set System Area	Specifies to total system area for the system
Set System Area Unit	Specifies the system area (footprint) unit of measure
Set System Balance	Sets the percentage as load out-of-balance threshold for 3-phase systems
Set System Balance Alert	Enables/disables alert when load out-of-balance threshold is reached for 3-phase systems
Set System PF	Sets the power factor used in the total system power calculation
Set Telnet Port	Sets the Telnet server port number
Set Telnet	Enables or disables Telnet access
Set Tower 3Phase	Specifies the AC voltage type for the tower
Set Tower Model	Specifies the model number for the tower
Set Tower Name	Specifies a descriptive field for the tower

## **Administrative Command Summary (continued...)**

Set Tower ProdSN	Specifies the serial number for the tower
Set Tower	Specifies the AC or DC voltage type for the tower
Set UPS AddInfeed	Adds an infeed association to a UPS
Set UPS DelInfeed	Deletes an infeed association from a UPS
Set UPS GETComm	Sets the UPS 'get' community string
Set UPS Host	Sets the UPS Host IP address or hostname
Set UPS Port	Specifies the target port for a UPS
Set UPS Type	Sets the UPS type
Set UPS VPoll	Enables or disables UPS voltage polling
Set User Access	Sets the access level for a user
Set User Envmon	Grants or removes user access to environmental monitoring
Set User Password	Changes the password for a user
Show EnergyWise	Displays Cisco EnergyWise network configuration information
Show FTP	Displays FTP configuration information
Show Infeeds	Displays infeed configuration information
Show Network	Displays network configuration information for all IPv4 and IPv6 settings
Show Options	Displays system option information
Show Outlets	Displays configuration information for all outlets
Show Ports	Displays serial/Pass-Thru port configuration information
Show SNMP	Displays SNMP configuration information
Show System	Displays system configuration information
Show System Status	Displays system power and tower configuration information
Show Towers	Displays tower configuration information
Show UPS	Displays UPS configuration information
Version	Displays the firmware version

### **To display the names of commands that you can 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 PDU environment and control session operations.

### **Turning outlets on:**

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

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

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

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

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

#### ***Examples***

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

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

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

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

### **Turning outlets off:**

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

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

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

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

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

#### ***Examples***

The following command turns off the outlet named FileServer\_1:

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

The following command turns off all outlets:

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

### **Rebooting outlets:**

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

---

**NOTE:** It is necessary to reissue the Status command to verify that the outlets have rebooted.

---

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

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

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

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

#### ***Example***

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

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

## Displaying outlet status:

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

This display includes the outlet absolute and descriptive names, the Outlet State reported to the PDU by the outlet and the current Control State being applied by the PDU. 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.

---

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

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

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

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

### **Examples**

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

```
Sentry: status WebServer_1<Enter>
Outlet  Outlet      Outlet  Control
ID      Name           State   State
.A2     WebServer_1     On      On
```

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

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

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

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

## Displaying accessible outlets:

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

### *To display accessible outlets:*

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

### **Example**

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

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

## Displaying accessible groups:

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

### *To display accessible groups:*

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

### **Example**

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

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

## Displaying outlets assigned to a group:

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

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

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

### **Example**

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

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

## Displaying accessible serial ports:

The List Ports command displays accessible serial ports for the current user.

### *To display accessible serial ports:*

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

### **Example**

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

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

## Displaying infeed status:

The Istat command displays the status of one or more infeeds.

This display includes the infeed absolute and descriptive names and the Input Status.

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

Type **istat** and press **Enter**.

### **Example**

The following command displays the infeed status:

```
Sentry: istat
Input      Input      Input
Feed ID   Feed Name   Status
.AA       HQ_1_Infeed_A  On
```

## 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**.

---

**NOTE:** The Connect command will not immediately disconnect when issued from an SSH session that was established while another Telnet or SSH session already existed.

---

### *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 can 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 Sentry: prompt, type **envmon** and press **Enter**.

### **Example**

The following command displays the status of the Environmental Monitor.

```
Sentry: 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.

### *To change a password:*

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



## Ending a session:

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

### *To end a session:*

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

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

## Displaying UPS status:

The UPSStat command displays the status of one or more UPS devices associated with the PDU.

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.

---

## Administration Commands

Administration commands can 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.

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

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

At the Password: prompt, type a password of 1-16 alphanumeric and other typed characters - (ASCII 32 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:

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

For security, password characters are not displayed.

#### Removing a user account:

The Remove User command removes a user account.

---

**NOTE:** You can remove the default user account **adm** only if you have already granted administrative access to another user account using the Set User Admnpriv command.

---

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

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

## Changing a password:

The Set User Password command changes a user's password. For security, when you type a password, the characters are not displayed on the screen.

### *To change a password:*

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

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

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

### *Example*

The following command changes the password for the user JohnDoe:

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

For security, password characters are not displayed.

## Setting user access level privileges:

The Set User Access command sets the access level privileges for a user. The PDU has the following defined access privilege levels; Admin, Power User, User, Reboot-Only, On-Only and View-Only.

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

---

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

---

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

At the Sentry: prompt, type **set user access**, followed by **admin**, **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:

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

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

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

## Granting and removing environmental monitoring viewing privileges:

The Set User Envmon command grants or removes Environmental Monitoring viewing privileges to/from a user.

### *To grant or remove environmental monitoring viewing privileges for a user:*

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

### *Example*

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

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

## Displaying user access level:

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

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

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

### **Example**

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

```
Sentry: list users<Enter>
  User          Privilege      Environmental
  Name          Level          Monitoring
  JOHNDOE       Admin          Allowed
  JILLDOE       Power-User     Allowed
  JANEDOE       User           Allowed
  JAKEDOE       Reboot-Only   Not Allowed
  JOSEYDOE      On-Only       Not Allowed
  JOEDOE        View-Only     Not Allowed
```

## Adding outlet access to a user:

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

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

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

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

### **Examples**

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

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

## Deleting outlet access for a user:

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

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

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

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

## Adding group access to a user:

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

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

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

### **Examples**

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

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

## Deleting group access for a user:

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

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

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

### Adding serial 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 Sentry: 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 Sentry: 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 Sentry: prompt, type **list user**, optionally followed by a username. Press **Enter**.

#### **Example**

The following command displays information about the user JaneDoe:

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

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

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

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

#### *To create an outlet name:*

At the Sentry: prompt, type **set outlet name** followed by the absolute outlet name, 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:

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

### **Setting the outlet wakeup state:**

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

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

#### *To set the wakeup state:*

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

#### **Example**

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

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

### **Setting the outlet post-on delay:**

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

---

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

---

#### *To set the outlet post-on delay*

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

#### **Example**

The following command set the Post-On delay for outlet .a2 to 90 seconds:

```
Sentry: set outlet postondelay .a2 90<Enter>
```

## Displaying outlet information:

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

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

### *To display outlet information:*

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

### **Example**

The following command displays all outlet information:

```
Sentry: show outlets<Enter>
Outlet  Outlet      Wakeup      Post-On
ID      Name           State        Delay (seconds)
.A1     TowerA_Outlet1 Off          0
.A2     TowerA_Outlet2 On           90
More (Y/es N/o):
Outlet Options:
  Sequence Interval:  2 seconds
  Reboot Delay:      15 seconds
```

## Group Administration

### Creating a group name:

The Create Group command creates a new group name.

#### *To create a group name:*

At the Sentry: prompt, type **create group** optionally followed by a descriptive name of up to 24 alphanumeric and other 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:

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

### Removing a group name:

The Remove Group command removes a group name.

#### *To remove a group name:*

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

#### *Example*

The following command removes group name ServerGroup\_1:

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

### Adding an outlet to a group:

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

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

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

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

#### *Examples*

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

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

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

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

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

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

### Deleting an outlet from a group:

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

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

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

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

## **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 Evmmon command is issued.

#### ***To create an Environmental Monitor name:***

At the Sentry: prompt, type **set envmon name** followed by the absolute Environmental Monitor 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 the Environmental Monitor:

```
Sentry: 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 Evmmon command is issued.

#### ***To create an temperature/humidity sensor name:***

At the Sentry: prompt, type **set envmon ths name** followed by the absolute name of the temperature/humidity sensor, 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 T/H2\_Florida\_HQ\_1 to the second temperature/humidity sensor:

```
Sentry: 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 can use this name in commands that require a port name as an alternative to using the port's absolute name.

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

At the Sentry: prompt, type **set port name** followed by the absolute outlet name, 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:

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

### **Setting the serial ports data-rate:**

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

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

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

#### ***Example***

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

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

### **Enabling or disabling active signal checking for serial 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 Sentry: prompt, type **set port dsrcheck console, on or off**, and press **Enter**.



## Setting the serial port timeout value:

The Set Port Timeout command sets 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 timeout is 0 to 60 (in minutes). The default timeout is 5 minutes. The command can be used to set individual ports by ID or name.

---

### NOTES:

- Setting the timeout value to “0” disables the timer.
  - Only a numeric value is accepted.
- 

#### *To set the serial port timeout value for an individual port:*

At the Switched CDU: prompt, **type set port timeout**, followed by the port ID or name, followed by a timeout value from 0 to 60 (in minutes), and press **Enter**.

## Configuring the Bluetooth™ options:

If the PDU has been equipped for the mobile monitoring solution using Bluetooth® technology, several Bluetooth parameters will be available for editing on the Serial Ports configuration page.

#### *To set the Bluetooth™ module name:*

The Bluetooth™ module name displays in the list of discovered modules on the Android device. The default is “ST Eye”, and the module name cannot be blank.

At the Switched CDU: prompt, type **set bluetooth name**, followed by 1-31 characters of a descriptive name for the module, and press **Enter**.

#### *To set the Bluetooth™ discoverability:*

Three discoverability settings determine the current status of the pushbutton on the Bluetooth module:

- Always - The Bluetooth module is discoverable, even without pressing the pushbutton.
- Limited (Default) - The pushbutton on the Bluetooth module must be pressed to make the module discoverable for 60-seconds.
- Never - The Bluetooth module is never in discoverable mode.

At the Switched CDU: prompt, type **set bluetooth discover**, followed by **always**, **limited**, or **never**, and press **Enter**.

#### *To set the Bluetooth™ pin code:*

The pin code is available for legacy Bluetooth modules that require a pin to pair the module. Although not used in current Bluetooth modules, the pin code is supported if needed. The default is 9611.

At the Switched CDU: prompt, type **set bluetooth pincode**, followed by 4-digits from 0000 to 9999, and press **Enter**.

#### *To set the Bluetooth™ transmission power:*

This setting is the designated transmission power (dbm) for the Bluetooth module. Note that lowering the transmission power reduces the effective range of the module. Default is 0

At the Switched CDU: prompt, type **set bluetooth transpwr**, followed by a value from -6 to 4 (dbm), 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
- Bluetooth™ parameter settings settings, if applicable

### *To display serial port information:*

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

### **Example**

The following command displays all serial port information:

```
Switched CDU: show ports<Enter>
Serial Port Configuration
  Port ID: Console          Port Name: CONSOLE
  DSR Check: ON            CLI: Enabled    SCP: Disabled  RFTAG: Enabled
  Data Rate: 9600         Connection Timeout: 5 minute<s>

  Port ID: Aux             Port Name: AUX
  DSR Check: ON            CLI: Enabled    SCP: Enabled
  Data Rate: 115200       Connection Timeout: 5 minute<s>

Bluetooth Settings:
  Name:                    ST Eye - 10.1.2.77
  Discoverability:         LIMITED
  Pin code:                9611
  Transmission pwr:       0 <dbm>
```

## **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 2069 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.

---

#### **NOTES:**

##### *For SSH sessions only:*

- The “keyboard-interactive” authentication method must be used for the banner to display.
  - Banner length is truncated to 1500 bytes in SSH packets to avoid failure of SSH connection when configured with a long login banner.
- 

### *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**.

### **Setting the system area:**

The Set System Area command is used to set the total area for the system. This value is used for total system power calculations.

### *To set the system area:*

At the Switched CDU: prompt, type **set system area**, followed by the system area (in square feet) and press **Enter**.

### **Example**

The following command sets the total system area to 6.3 square feet:

```
Switched CDU: set system area 6.3<Enter>
```

### **Setting the system area unit of measure:**

The Set System Area Unit command sets the value for the system area footprint 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 areaunit**, 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 determines when the current on the lines of a 3-phase system are out-of-balance between the three phases of power.

#### *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 20%.

```
Switched CDU: set system balance 20<Enter>
```

### Setting the 3-phase load out-of-balance alert:

The Set System Balance Alert command enables or disables the sending of an alert when the current on the lines of a 3-phase system are past a pre-set threshold (percentage) and are out-of-balance between the three phases of power.

At the Switched CDU: prompt, type **set system balancealert**, followed by **enabled** or **disabled**, and press **Enter**.

#### **Example:**

The following command enables the load out-of-balance alert:

```
Switched CDU: set system balancealert enabled<Enter>
```

---

#### **NOTES:**

- When a device with 3-phase input voltage is out-of-balance, efficiency is reduced and the unit is prevented from reaching maximum capacity. When an alert for the out-of-balance condition is received (if the alerting feature is enabled), it may be necessary to adjust distribution of the loads.
  - For 3-phase systems, if the Out-of-Balance Alerting feature is enabled, and the system goes into a load out-of-balance condition, the System Status command will display the alert “3ph Out-of-Balance” in the Tower Status section, unless there is a higher priority tower error state to report.
- 

### 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 Sentry: 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:

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

The following command deletes any previously specified location description:

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

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

## **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 IPM is required after activating new special features.

---

### **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 Sentry: prompt, type **set option strong password**, followed by **enabled** or **disabled** and press **Enter**.

### **Displaying system power status:**

The System Status command displays system power and tower 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
Tower Status
Tower      Tower      Tower
ID         Name       Status
.A         TowerA    Normal
.B         TowerB    Normal

Command successful
```

---

**NOTE:** For 3-phase systems, if the Out-of-Balance Alerting feature is enabled, and the system goes into a load out-of-balance condition, the System Status command will display the alert "3ph Out-of-Balance" in the Tower Status section, unless there is a higher priority tower error state to report.

---

## 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 PDU configurations from being reset locally.

---

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

---

### *To enable or disable the configuration reset button:*

At the Sentry: 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 Sentry: 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 PDU will report in.

### *To set the temperature scale:*

At the Sentry: prompt, type **set option tempscale**, followed by **celsius** or **fahrenheit** and press **Enter**.

## 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.

### *To create a tower name:*

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

### **Example**

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

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

## Displaying tower information:

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

### *To display tower information:*

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

### **Example**

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

## Creating a descriptive infeed name:

The Set Infeed Name command assigns a descriptive name to an infeed. This descriptive name is displayed when the Show Traps command is issued

### *To create a infeed name:*

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

### **Example**

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

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

## Displaying infeed information:

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

### *To display tower information:*

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

### **Example**

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

### 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>
```

### Customizing the CLI prompt:

The Set Option Prompt command customizes the CLI prompt.

#### *To customize the CLI prompt:*

At the Switched CDU: prompt, type **set option prompt** and press **Enter**. Then type the custom prompt and press **Enter**.

To reset the custom prompt to the default prompt, type **set option prompt** and press **Enter**. When prompted, leave blank and press **Enter**.

The maximum length of the custom prompt is 31 characters. Spaces and special characters are allowed.

#### **Example:**

The following command sets the default CLI prompt to “My Prompt”:

```
Switched CDU: set option prompt<Enter>
Custom prompt <blank for default>: My Prompt:
Command successful
My Prompt:
```

### Enabling or Disabling StartUp Stick®:

The Set Option Startupstick command enables or disables the StartUp Stick tool for PDU mass configuration of operating parameters.

#### *To enable or disable StartUp Stick:*

At the Switched CDU: prompt, type **set option startupstick**, followed by **enabled** or **disabled** and press **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**.

## To enable or disable the Serial Command Protocol (SCP) authentication:

The Set SCP Authentication command enables or disables SCP Authentication.

### *To enable or disable SCP:*

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

## To set the Serial Command Protocol (SCP) authentication user:

The Set SCPAuth User command sets the username and password for SCPAuthentication.

### *To set SCP username:*

At the Switched CDU: prompt, type **set scpauth user**, followed by user name, and press **Enter**. You will be prompted to enter and verify a password.

## Displaying the Firmware version:

The Version command displays the Firmware version.

### *To display the firmware version:*

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

## Performing a warm boot:

The Restart command performs a warm boot of the PDU.

---

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

---

### *To perform a warm boot:*

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

## Displaying system options:

The Show Options command displays settings for all system options.

### *To display system option information:*

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

### **Example**

```
Sentry: show options
System Options
  Display Orientation:      AUTO <Normal>
  Outlet Sequence Order:   NORMAL
  Strong Passwords:        DISABLED
  Configuration Reset Button:  ENABLED
  More Prompt:             ENABLED
  Temperature Scale:        CELSIUS
  CLI Custom Prompt:        <none>
  CLI Session Timeout:      10 minutes
  Web Session Timeout:      10 minutes
  Coldboot Alert <SCP>:     ENABLED
```

---

**NOTE:** The display of "<SCP>" after the Coldboot Alert parameter in the Show Options command (as indicated above) shows a relationship between the Serial Command Protocol (SCP) and the Coldboot Alert feature. Upon a coldboot of the system, if the Coldboot Alert feature is enabled, the system will send a ½ second RS-232 break out to to any SCP-enabled serial ports.

---



## Enabling or disabling the Cisco EnergyWise network:

---

**NOTE:** Only commands through the CLI are supported for the Cisco EnergyWise network. There is no firmware web-based interface for EnergyWise. Enabling EnergyWise requires a system restart.

---

The Set EnergyWise command enables or disables the EnergyWise network support:

### *To enable or disable EnergyWise:*

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

### *Example*

```
Switched CDU: set energywise enabled
Command successful -- restart required
```

## Setting up PDUs in the Cisco EnergyWise network:

---

**NOTE:** To use EnergyWise, you must first configure domain name, port, and secret.

---

The Set EnergyWise Domain command configures the EnergyWise domain the PDU belongs to. The limit of the Domain Name is 64 characters.

### *To set the EnergyWise domain name:*

At the Switched CDU: prompt, type **set energywise domain**, followed by the domain name, and press **Enter**.

### *Example*

```
Switched CDU: set energywise domain 10.1.2.120
Command successful
```

### *To set the EnergyWise port:*

The default port number is 43440; the valid range for port numbers is 1-65535.

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

### *Example*

```
Switched CDU: set energywise port
Port [666]: 700
Command successful
```

### *To set the EnergyWise secret:*

The limit of the Secret field is 64 characters. A blank secret is also acceptable.

At the Switched CDU: prompt, type **set energywise secret**, then verify the secret, and press **Enter**.

### *Example*

```
Switched CDU: set energywise secret
Secret: *****
VerifySecret: *****

Command successful
```

### ***To set a blank EnergyWise secret:***

A blank secret is acceptable.

At the Switched CDU: prompt, type **set energywise secret**, do not type in the Secret field, and press **Enter** twice (to bypass the Secret field and then VerifySecret field.)

### ***Example of a blank secret***

```
Switched CDU: show energywise
EnergyWise Configuration
  Endpoint:      Enabled *
  Port:          666
  Domain:        (undefined)
  Refresh Rate:  60
  Secret:        (Blank)
Command successful
```

### ***To set the EnergyWise refresh rate:***

The EnergyWise refresh rate is the rate (in seconds) at which new information is pushed to the EnergyWise manager. Valid range is 30-600 seconds; default is new data sent to the EnergyWise manager every 3 minutes.

At the Switched CDU: prompt, type **set energywise refresh**, followed by a rate (in seconds) from 30-600, and press **Enter**.

## **Viewing Cisco EnergyWise network parameters:**

---

**NOTE:** A change in any value (shown in the example below) requires a restart of the system.

---

### ***To view EnergyWise network parameters:***

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

### ***Example***

```
Switched CDU: show energywise
EnergyWise Configuration
  Endpoint:      Enabled*
  Port:          666
  Domain:        <undefined>
  Refresh Rate:  55
  Secret:        *****
Command successful
```

## **TCP/IP Administration**

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**.

### **Enabling or disabling DHCP boot delay:**

The Set DHCP Boot Delay command enables or disables the DHCP boot delay option.

- Enabling the Boot Delay option gives the PDU approximately 100-seconds to establish a connection through a DHCP server. This interval allows various network component activities to occur as the PDU powers up (such as obtaining SNTP time stamps for logging or allowing SNMP traps to be sent as switched outlets power up). This is the default state.
- Disabling the Boot Delay option forces the PDU to boot after approximately 5-seconds regardless of the DHCP acquisition state. This speeds up a boot when a DHCP server is connected to one of the PDU's outlets. In this configuration, SNMP traps, SNTP and other protocols will not be available until a DHCP address has been resolved.

### ***To enable the boot delay:***

At the Switched CDU: prompt, type **set dhcp**, followed by **bootdelay**, followed by **enabled** or **disabled**, and press **Enter**.

---

#### **NOTES:**

- The Boot Delay option executes only when DHCP is enabled.
- The firmware can detect network link integrity and will wait for network connection. This means that if the network is not currently connected, the enabled Boot Delay option will be ignored.

---

### **Enabling or disabling DHCP static address fallback:**

**NOTE:** DHCP must be enabled to activate the DHCP Static Address Fallback option.

The Set DHCP Static Address Fallback command enables or disables the DHCP static address fallback option.

Enabling the Static Address Fallback option informs the PDU to automatically fall back to a static address if a DHCP server does not respond after 100-seconds. This is the default state.

Disabling the Static Address Fallback option generates periodic DHCP server requests until the PDU obtains a dynamic address.

### ***To enable the static address fallback:***

At the Switched CDU: prompt, type **set dhcp**, followed by **staticfallback**, followed by **enabled** or **disabled**, and press **Enter**.

**NOTE:** If the DHCP server boot time is excessive, you may need to disable the DHCP Static Address Fallback option.

---

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

**NOTE:** Both IPv4 and IPv6 IP address formats are accepted.

---

### ***Example***

The following command sets the IP address to 12.34.56.78:

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

### Setting the subnet mask:

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

#### *To set the subnet mask:*

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

#### **Example**

The following command sets the subnet mask to 255.0.0.0

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

### Setting the gateway:

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

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

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

#### **Example**

The following command set the gateway IP address to 12.34.56.1:

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

### Setting the DNS IP address:

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

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

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

---

**NOTE:** Both IPv4 and IPv6 formats are accepted for DNS IP address.

---

#### **Example**

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

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

## Displaying network configuration information:

The Show Network command displays TCP/IP, Telnet, SSH, Web, SSL, SNMP, and DHCP options (when DHCP is enabled) configuration information. The Show Network command also displays all IPv4 and IPv6 settings.

- Network configuration: IP address, subnet mask, gateway and DNS IP addresses (both IPv4 and IPv6 formats are displayed). (both IPv4 and IPv6 formats are displayed).
- Enabled-disabled status and port numbers for Telnet, SSH, HTTP, SSL, SNMP, and FTP Server support.
- Network status: Link, speed, duplex, and negotiation.
- DHCP boot delay and DHCP static address fallback options (when DHCP is enabled).
- Enabled-disabled status of Sentry Power Manager (SPM).

### *To display network configuration information:*

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

### **Example**

The following command displays the network configuration information:

```
Switched CDU: show network
Network Settings
  State: DHCP IPv6/IPv4 Network: Dual IPv6/IPv4
  Link: Up Negotiation: Auto
  Speed: 100 Mbps Duplex: Full

  AutoCfg IPv6: FE80::20A:9CFF:FE52:4104/64
  IPv6 Address: FD01::1:B51A:E03C/64
  IPv4 Address: 10.1.6.230 Subnet Mask: 255.255.0.0
  IPv4 Gateway: 10.1.1.1
  DNS1: FD01::A01:585
  DNS2: 10.1.5.133

Static IPv4/IPv6 Settings
  IPv6 Address: FD01::A01:353/64
  IPv6 Gateway: ::
  IPv4 Address: 10.1.2.253 Subnet Mask: 255.255.0.0
  IPv4 Gateway: 10.1.1.1
  DNS1: 10.1.5.133
  DNS2: 10.1.5.134

DHCP Settings
  DHCP: Enabled
  FQDN: Enabled [sentry3-524104]
  Boot Delay: Enabled
  Static Fallback: Enabled

Network Services
  Telnet: Enabled Port: 23
  SSH: Enabled Port: 22 Auth: Password, Kb-Int
  HTTP: Enabled Port: 80
  SSL: Enabled Port: 443 Installed Cert: User Encrypted
  Access: Optional Stored Files: Cert & Key
  User Cert: Enabled User Passphrase: <set>
  SNMPv1/2: Enabled Port: 161 TrapPort: 162
  SNMPv3: Disabled Port: 161 TrapPort: 162
  FTP Server: Enabled Port: 21
  SPM Access: Enabled

Command successful
```

---

**NOTE:** The fields IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway, DNS1, and DNS2 are equivalent to existing PDU IPv4 settings except that current network settings and static settings are displayed separately. This allows you to view both static configuration settings and active network settings that can be obtained using DHCP. The DNS addresses can be in IPv4 or IPv6 (based on RFC4291) format at this time.

---

## HTTP Administration

---

**NOTE:** A restart is required after setting or changing any Telnet/Web configurations.

---

### **Enabling and disabling HTTP support:**

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

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

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

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

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

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

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

#### **Example**

The following changes the HTTP port number to 2048:

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

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

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

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

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

## Sentry Power Manager (SPM) Administration

The PDU Power Manager (SPM) is Server Technology's enterprise management software product for the data center. The configuration options provided allow you to enable/disable SPM and reset the SPM password to its default.

---

**NOTE:** The SPM options apply only if you are currently using Server Technology's SPM software product.

---

### **Enabling and disabling SPM Secure Access:**

The Set SPM command enables or disables support for Sentry Power Manager (SPM). If your operation does not currently use SPM software, you can disable SPM Secure Access. However, if disabled, the PDU will not be able to use the SPM suite of secure network capabilities or the advanced remote configuration.

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

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

---

**NOTE:** Both HTTP and SSL must be enabled or the SPM Secure Access option will not be permitted. When SPM Secure Access is permitted, the default is Enabled.

---

### **Resetting the SPM Password:**

The Set SPM Reset Password command resets the SPM password on the PDU to its internal default password.

Each PDU has a default unique SPM password that is used to communicate between SPM and the PDU. When SPM discovers a PDU in the network, SPM changes this password into a different unique password for added security. The SPM then continues to manage or alter these passwords as required for system security.

If a PDU is relocated or swapped from the system after a password was generated, SPM may not be able to re-establish a connection to the unit. The Set SPM Reset Password command allows you to reset to the internal default password of the PDU so SPM can re-discover the device and add it to the system. Once the unit has been acquired by SPM, no further action is necessary.

#### *To reset the SPM password:*

At the Switched CDU: prompt, type **set spm**, followed by **resetpw** and press **Enter**.

---

**NOTE:** Do not reset the password if SPM communication has already been established.

---

## Telnet Administration

---

**NOTE:** A restart of the IPM is required after setting or changing any Telnet/Web configurations.

---

### **Enabling and disabling Telnet support:**

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

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

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

### **Changing the Telnet port:**

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

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

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

#### **Example**

The following changes the Telnet port number to 7001:

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

## FTP Administration

You can upload new versions of firmware into the PDU 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 PDU for an FTP firmware upload.

---

**NOTE:** Secure File Transport Protocol (SFTP) is also supported for encrypted SSH transport over the network.

---

### **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 Sentry: prompt, type **set ftp host**, followed by the IP address or hostname and press **Enter**.

---

**NOTE:** Both IPv4 and IPv6 formats are accepted for IP address or hostname.

---

#### **Examples**

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

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

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

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

#### **Example**

The following command sets the FTP username to Guest:

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

### Setting the FTP Password:

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

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

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

#### **Example**

The following command sets the FTP password to OpenSesame:

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

### Setting the filename to be uploaded:

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

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

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

#### **Example**

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

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

### Setting the 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 Sentry: 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 Sentry: 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:

```
Sentry: set ftp autoupdate day sunday<Enter>
```

### Setting the automatic update scheduled hour:

The Set FTP Autoupdate Hour command is used to hour of the day when automatic updates occur.

#### *To set the automatic update hour:*

At the Sentry: 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:

```
Sentry: set ftp autoupdate hour 12am<Enter>
```

The following command sets the automatic update hour to 3 PM:

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

### **Example**

The following command displays the FTP configuration information:

```
Sentry: show ftp<Enter>
FTP Configuration
Host:      ftp.servertech.com
Username:  guest
Password:  OpenSesame
Directory: ftp://sentry
Filename:  snb_s52a.bin
FTP Automatic Updates Configuration
Automatic Updates: 12.34.56.99
Scheduled Day:     Sunday
Scheduled Hour:    3 PM
```

## **SNTP Administration**

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

### *About Daylight Saving Time(DST)*

Support for DST is disabled by default. When enabled, the date and time are automatically adjusted forward one hour between the starting and ending dates and times (which can be configured).

---

**NOTE:** If Daylight Saving Time (DST) is enabled, all system time displays will be shown with the current DST start/end date/time settings.

---

The default time zone is set for the United States until at least 2015.

The time zone format is: **mo.w.d/h:m:s**, as follows:

- mo** = month from January to December (1-12)
- w** = week number (1-4) or the last week (5)
- d** = day of week from Sunday to Saturday (0-6)
- h** = hour (0-23)
- m** = minute (0-59)
- s** = second (0-59)

## **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 sntp**, followed by **primary** or **secondary**, and the SNTP server IP address or hostname. Press **Enter**.

---

### **NOTES:**

- The primary/secondary IP addresses contact the SNTP server; these addresses are populated with the external NTP pool time zones "2.servertech.pool.ntp.org" and "1.servertech.pool.ntp.org" as default for new PDUs that have not yet been time set.
  - Both IPv4 and IPv6 formats are accepted for primary/secondary IP address or hostname.
- 

### **Examples**

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

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

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

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

## Setting the local GMT offset (hours/minutes):

The Set SNTP GMTOffset command is used to set the offset from GMT for the date/time returned by SNTP.

The GMT offset supports all standard international time zones from -12:59 to +14:59. The GMT offset can be set in minutes to accommodate partial-hour time zones.

---

**NOTE:** The IPM does not support automatic adjustment for Daylight Saving Time (DST).

---

### *To set the local GMT offset:*

At the Sentry: prompt, type **set sntp gmtoffset**, followed by the offset value, and press **Enter**.

### **Examples**

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

```
Sentry: set sntp gmtoffset -12<Enter>
```

## Displaying SNTP configuration information:

The Show SNTP command displays all SNTP configuration information.

### *To display SNTP configuration information*

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

### **Example**

The following command displays the SNTP configuration information:

```
Switched CDU: show sntp <Enter>
Date/Time:      2013-04-13 15:21:18
Primary Host:   204.152.184.72
Secondary Host: 1.servertech.pool.ntp.org
Local GMT Offset: -8
Use DST:        Enabled
Start Date:     1st Wednesday in April
Start Time:     04:18:06
End Date:       1st Sunday in November
End Time:       02:00:00
```

## 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 IPM is required after activating new special features.

---

## Chapter 3: Advanced Operations

<b>SSL</b>	<b>765</b>
Enabling and Setting up SSL Support	765
SSL Technical Specifications	765
<b>SSH</b>	<b>78</b>
Enabling and Setting up SSH Support	78
SSH Technical Specifications	78
<b>SNMP</b>	<b>79</b>
MIB, OID and Support	79
Enabling and Setting up SNMP Support	81
SNMP Traps	85
Configuring Traps	87
<b>LDAP</b>	<b>91</b>
Enabling and Setting up LDAP Support	91
Configuring LDAP Groups	97
LDAP Technical Specifications	100
<b>TACACS+</b>	<b>101</b>
Enabling and Setting up TACACS+ Support	101
Configuring TACACS+ Privilege Levels	103
TACACS+ Technical Specifications	105
<b>LOGGING</b>	<b>106</b>
Internal System Log	106
Syslog	106
Email	107
<b>UPLOAD/DOWNLOAD</b>	<b>110</b>
Sentry Integrated FTP Server	110
FTP Configuration Files	110
Upload/Download Process	111

## SSL

Secure Socket Layers (SSL) 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 PDU's SSL Certificate enables the client to verify the PDU's authenticity and to communicate with the PDU securely via an encrypted session, protecting confidential information from interception and hacking.

### SSL Command Summary

Command	Description
Set SSL	Enables/disables SSL support
Set SSL Access	Sets SSL access as optional or required
Set SSL Port	Configures the SSL port number
Set SSL User Certificate	Enables/disables custom user certificates
Set SSL User Passphrase	Passphrase to control login access for user certificates

### Enabling and Setting up SSL Support

**NOTE:** A restart of the IPM is required after setting or changing any SSL configurations.

#### Enabling or disabling SSL support:

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

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

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

#### Setting SSL access level:

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

##### *To change the access level:*

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

##### **Example**

The following changes the access level to required:

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

#### Enabling or disabling custom user certificates:

The Set SSL User Certificate command enables or disables uploading of custom user certificates.

##### *To enable or disable user certificates:*

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

#### Setting the custom user certificate passphrase:

The Set SSL User Passphrase command sets the user-defined passphrase for authentication of uploaded custom user certificates.

##### *To set the user certificate passphrase:*

At the Switched CDU: prompt, type **set ssl userpass** and press **Enter**. You will be prompted to provide the passphrase. Press **Enter**.

**NOTE:** A restart of the PDU is required after setting the user certificate passphrase.

## **SSL Technical Specifications**

Secure Socket Layer (SSL)

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

SSL/TLS-enabled HTTPS server (RFC 2818)

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

Asymmetric Cryptography:

1024-bit RSA Key Exchange

Symmetric Cryptography Ciphers:

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

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

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

TLS\_RSA\_WITH\_DES\_CBC\_SHA

## SSH

Secure Shell (SSH) version 2 enables secure network terminal sessions between a 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 PDU for configuration and power management, the SSH session can be used for secure Pass-Thru connections to attached devices.

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

### SSH Command Summary

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

### Enabling and Setting up SSH Support

---

**NOTE:** A restart of the PDU is required after setting or changing any SSH configuration

---

#### Enabling or disabling SSH support:

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

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

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

#### Changing the SSH server port:

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

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

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

#### **Example**

The following changes the SSH port number to 65535:

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

### SSH Technical Specifications

Secure Shell (SSH) version 2

Asymmetric Cryptography:

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

Symmetric Cryptography:

AES256-CBC	RIJNDAEL256-CBC	3DES-192-CBC
AES192-CBC	RIJNDAEL192-CBC	
AES128-CBC	RIJNDAEL128-CBC	

Message Integrity:

HMAC-SHA1-160  
HMAC-MD5-128

Authentication:

Username/Password

Session Channel Break Extension (for RS232 Break)

## SNMP/Thresholds

The PDU 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 unit includes an SNMP v2c agent supporting standard MIB 1 and MIB 2 objects. A private enterprise MIB extension (Sentry3 MIB) is also supported to provide remote power control.

### **About SNMP Versions**

The firmware supports SNMP versions 1, 2, and 3.

SNMP version 3 supports authentication and encryption on a per user basis. Authentication types are None and MD5. Encryption types are None and DES. If you use authentication, you must use encryption.

Two SNMPv3 users are supported: one user with read-write (RW) access, and one user with read-only (RO) access. Both users have the same configuration parameters, and you can configure each user independently.

SNMPv2 and SNMPv3 can be enabled or disabled independently. You can have SNMPv2 and/or SNMPv3, or none.

#### ***SNMP CLI Commands:***

- All SNMP v3 specific configuration settings use the CLI command SET SNMP V3.
- All SNMP v1/v2 specific configuration settings use the CLI command SET SNMP V2.
- All SNMP configuration settings common to any SNMP version use the CLI command SET SNMP.

---

#### **NOTES:**

- If you use SNMP v1 or SNMP v2, all SET SNMP CLI commands (and the SHOW command) require the “V2” keyword.
- SNMP v1/v2 CLI commands are documented immediately below in this section showing the required “V2” keyword. All CLI commands that follow the SNMP v1/v2 section in this manual assume SNMP v3.

---

### **SNMP v1/v2 Command Summary**

Command	Description
Set SNMP IP Restrict	Allows SNMP Get and Set requests only from defined trap destinations
Set SNMP Trap Format	Configures the SNMP trap format version
Set SNMP V2	Enables or disables SNMP v1/v2 support
Set SNMP V2 Getcomm	Sets the 'get' community string
Set SNMP V2 Setcomm	Sets the 'set' community string
Show SNMP	Displays all SNMP configuration information

### **Enabling and Setting Up SNMP v1/v2 Support**

SNMP v1/v2 support must be enabled and configured for access to Sentry3 MIB objects and generation of all Sentry3 traps.

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

The SNMP Set command is used to enable or disable SNMP v1/v2 support.

#### ***To enable SNMP v1/v2 support:***

At the Switched CDU: prompt, type **set snmp v2**, followed by **enabled** or **disabled** and press **Enter**.

---

**NOTE:** A restart of the IPM is required after enabling or disabling SNMP support.

---

## Setting the Get/Set community strings:

**NOTE:** The default for SNMP support is **Enabled**. When Server Technology products are shipped, the default SNMP configuration for the Get community string is set to “**public**” and the Set community string is left **blank**.

The PDU supports two SNMP community strings (Set and Get) that provide varying levels of access to objects defined in the PDU3 MIB. Valid community strings are 1 to 24 characters.

### *Set Community String:*

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

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

At the Switched CDU: prompt, type **set snmp v2 setcomm**, followed by the string, and press **Enter**.

### *Get Community String:*

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 v2 getcomm**, followed by the string, and press **Enter**.

## Displaying SNMP v1/v2 configuration information:

The Show SNMP V2 command displays all SNMP v1/v2 configuration information, including:

- SNMP support status
- SNMP community strings
- Trap timer value
- Trap destinations (both IPv4 and IPv6 formats can be displayed.)

### *To display SNMP v1/v2 configuration information:*

At the Switched CDU: prompt, type **show snmp v2** and press **Enter**.

### **Example**

The following command displays the SNMP configuration information:

```
Switched CDU: show snmp v2<Enter>
SNMP Configuration
  SNMPv2 Agent:                Enabled
    GET Community <RO>:        public
    SET Community <RW>:        <undefined>
    TRAP Community:            trap

  SNMPv3 Agent:                Disabled
    Engine ID                   800006B6020000000000000000000000FFFF0A010249
    RW Username:                <undefined>
    RW Auth Type:               None <password not set>
    RW Privacy Type:            None <password not set>
    RO Username:                <undefined>
    RO Auth Type:               None <password not set>
    RW Privacy Type:            None <password not set>
    Trap Username               <undefined>
    Trap Destination 1:         <undefined>
    Trap Destination 2:         <undefined>
    Trap format:                v3
    IP Restrictions:            No Restrictions
    Error Trap Repeat Time:     60 second<s>

  SysName:                     Sentry3_524640
  SysLocation:                  No Location
  SysContact:                   No Contact

Command successful
```



## SNMP v3 Command Summary

Command	Description
Set SNMP IP Restrict	Allows SNMP Get and Set requests from defined trap destinations only
Set SNMP Trap Format	Configures the SNMP trap format version
Set SNMP V3	Enables or disables SNMP v3 support
Set SNMP V3 RO Username	Sets the SNMP V3 read-only username.
Set SNMP V3 RO Auth Type	Sets the SNMP V3 read-only authentication type
Set SNMP V3 RO Auth Password	Sets the SNMP V3 read-only authentication password
Set SNMP V3 RO Priv Type	Sets the SNMP V3 read-only privacy type
Set SNMP V3 RO Priv Password	Sets the SNMP V3 ready-only privacy password
Set SNMP V3 RW Username	Sets the SNMP V3 read-write username
Set SNMP V3 RW Auth Type	Sets the SNMP V3 read-write authentication type
Set SNMP V3 RW Auth Password	Sets the SNMP V3 read-write authentication password
Set SNMP V3 Trap Username	Sets the SNMP V3 trap username for display on SNMP activity logs
Set SNMP V3 RW Priv Type	Sets the SNMP V3 read-write privacy type
Set SNMP V3 RW Priv Password	Sets the SNMP V3 ready-write privacy password
Show SNMP	Displays all SNMP configuration information

### MIB, OID and Support

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

<ftp://ftp.servertech.com/pub/SNMP/sentry3>

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

For SNMP Support, email: [mibmaster@servertech.com](mailto:mibmaster@servertech.com)

### Enabling and Setting up SNMP Support

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

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

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

#### *To enable SNMP support:*

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

---

**NOTE:** A restart of the IPM is required after enabling or disabling SNMP support.

---

#### **SNMPv3 Engine ID:**

The local engine ID is the unique identifier for the SNMPv3 engine and is displayed for viewing.

#### **Setting the SNMP v3 read-only (RO) username :**

The Set SNMP RO Username command sets the read-only username for SNMP v3. A valid username can be set to any value between 1-32 characters.

#### *To set the RO username:*

At the Switched CDU: prompt, type **set snmp v3 rousername**, and press **Enter**.

---

**NOTE:** You can set a blank username but doing so will clear the string and disallow any read-only user access.

---

#### **Setting the SNMP v3 read-only (RO) authentication type :**

The Set SNMP RO Auth Type command sets the SNMP v3 RO authentication type.

#### *To set the RO authentication type:*

At the Switched CDU: prompt, type **set snmp v3 roauthtype**, followed by **none** or **md5**, and press **Enter**.

### Setting the SNMP v3 read-only (RO) authentication password:

The Set SNMP RO Auth Password command sets the SNMP v3 RO authentication password. A valid authentication password can be set to any value between 1-40 characters. A blank password will clear the string.

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

At the Switched CDU: prompt, type **set snmp v3 roauthpass**, and press **Enter**.

### Setting the SNMP v3 read-only (RO) privacy type :

The Set SNMP RO Priv Type command sets the SNMP v3 RO privacy type.

#### *To set the RO privacy type:*

At the Switched CDU: prompt, type **set snmp v3 roprivtype**, followed by **none** or **des**, and press **Enter**.

### Setting the SNMP v3 read-only (RO) privacy password:

The Set SNMP RO Priv Password command sets the SNMP v3 RO privacy password. A valid privacy password can be set to any value between 1-32 characters. A blank password will clear the string

#### *To set the RO privacy password:*

At the Switched CDU: prompt, type **set snmp v3 roprivpass**, and press **Enter**

### Setting the SNMP v3 read-write (RW) username :

The Set SNMP RW Username command sets the read-write username for SNMP v3. A valid username can be set to any value between 1-32 characters.

To set the RW username:

At the Switched CDU: prompt, type **set snmpv3 rwusername**, and press **Enter**.

---

**NOTE:** You can set a blank username but doing so will clear the string and disallow any read-write user access.

---

### Setting the SNMP v3 read-write (RW) authentication type :

The Set SNMP RW Auth Type command sets the SNMP v3 RW authentication type.

#### *To set the RW authentication type:*

At the Switched CDU: prompt, type **set snmp v3 rwauthtype**, followed by **none** or **md5**, and press **Enter**.

### Setting the SNMP v3 read-write (RW) authentication password:

The Set SNMP RW Auth Password command sets the SNMP v3 RW authentication password. A valid authentication password can be set to any value between 1-40 characters. A blank password will clear the string

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

At the Switched CDU: prompt, type **set snmp v3 rwauthpass**, and press **Enter**.

### Setting the SNMP v3 read-write (RW) privacy type :

The Set SNMP RW Priv Type command sets the SNMP v3 RW privacy type. A valid password can be set to any value between 1-40 characters.

#### *To set the RW privacy type:*

At the Switched CDU: prompt, type **set snmp v3 rwprivtype**, followed by **none** or **des**, and press **Enter**.

### Setting the SNMP v3 read-write (RW) privacy password:

The Set SNMP RW Priv Password command sets the SNMP v3 RW privacy password. A valid privacy password can be set to any value between 1-32 characters. A blank password will clear the string

#### *To set the RW privacy password:*

At the Switched CDU: prompt, type **set snmp v3 rwprivpass**, and press **Enter**.

### Setting the SNMP v3 trap username:

The Set SNMP Trap Username command sets an optional username for display on SNMP activity logs to identify user actions.

At the Switched CDU: prompt, type **set snmp v3 trapusername**, and press **Enter**. The trap username can be 1-31 alphanumeric characters; spaces are allowed; and the name is case sensitive.

### Setting the error trap repeat timer:

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

#### *To set the error trap repeat 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 PDU: set snmp traptime 180<Enter>
```

### Setting the SNMP trap format version:

The SNMP Trap Format configures the SNMP trap format version. The trap format can be SNMP v1, v2, or v3.

#### *To set the trap format version:*

At the Switched CDU: prompt, type **set snmp trapformat**, followed by **1**, **2**, or **3**, and press **Enter**. The default is v1, regardless of the versions that are enabled for the agent.

#### **Example**

The following sets the trap format version to SNMP v3:

```
Switched CDU: set snmp trapformat 3<Enter>
```

### Setting IP restrictions:

The Set SNMP IP Restrictions command supports SNMP Manager Get and Set requests to only be allowed from the IP address of the defined trap 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 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. The PDU supports a maximum of two trap destinations; one must be defined to enable trap generation.

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

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

#### **Examples**

The following sets the trap destination 1 to 64.42.31.208:

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

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

```
Sentry: set snmp trapdest2 snmp.servertech.com<Enter>
```

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

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

### Setting the trap timer:

The Set 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 Sentry: prompt, type **set traptime**, followed by the timer period and press **Enter**.

#### *Example*

The following sets the timer period to 180 seconds:

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

### Setting the Get/Set community strings:

The Switched CDU supports two SNMP community strings that provide varying levels of access to objects defined in the PDU3 MIB.

Community strings can be 1 to 24 characters.

#### *Setcomm:*

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

#### *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 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**.

## Displaying SNMP configuration information:

The Show SNMP command displays all SNMP configuration information.

- SNMP version (v2/v3) support status (enabled/disabled)
- SNMP community strings
- Read-Only (RO) or Read-Write (RW) username, authentication type, privacy type (if SNMPv3)
- Trap username
- Trap destination(s)
- IP restrictions setting
- Error trap repeat time (in seconds)
- Sysname, syslocation, and syscontact

### 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
SNMPv2 Agent:                Enabled
    GET Community <RO>:      public
    SET Community <RW>:      <undefined>
    TRAP Community:          trap

SNMPv3 Agent:                Disabled

    Engine ID                800006B6020000000000000000000000FFFF0A010249
    RW Username:             <undefined>
    RW Auth Type:            None <password not set>
    RW Privacy Type:         None <password not set>

    RO Username:             <undefined>
    RO Auth Type:            None <password not set>
    RW Privacy Type:         None <password not set>

    Trap Username            <undefined>
    Trap Destination 1:      <undefined>
    Trap Destination 2:      <undefined>
    Trap format:              v3

    IP Restrictions:         No Restrictions
    Error Trap Repeat Time:  60 second<s>

    SysName:                 Sentry3_524640
    SysLocation:              No Location
    SysContact:               No Contact

Command successful
```

## SNMP Traps

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

### Trap Summary

Name	Level(s)	Description
Status	T, I, O, E, S	Operational status change
Change	O	Control status change
Temp	S	Temperature is out of range
Humid	S	Relative Humidity is out of range

All traps include the Location of the PDU 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 PDU 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**

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

### **Infeed Status traps**

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

### **Outlet Status traps**

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

### **Environmental Monitor Status traps**

<b>Status</b>	<b>Error</b>	<b>Description</b>
Normal		Environmental Monitor is working correctly
NoComm	x	Communication to the Environmental Monitor has been lost

### **Temperature/Humidity Sensor Status traps**

<b>Status</b>	<b>Error</b>	<b>Description</b>
Found		The sensor has been detected
NotFound		No sensor has been detected
Lost	x	Sensor initially detected but communication to the sensor has been lost
NoComm	x	Communication to the sensor has been lost

**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 PDU, and identifier and name of the affected outlet. For descriptions of the outlet status types, see the previous 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 PDU, 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**

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

## **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 PDU, 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**

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

## **Configuring Traps**

### **SNMP Trap Command Summary**

<b>Command</b>	<b>Description</b>
Set Trap Tower Status	Enables or disables the Tower Status trap
Set Trap Infeed Status	Enables or disables the Infeed Status trap off
Set Trap Outlet Change	Enables or disables the Outlet Change trap
Set Trap Outlet Status	Enables or disables the Outlet Status trap
Set Trap EM Status	Enables or disables the Environmental Monitor Status trap
Set Trap THS Status	Enables or disables a temperature/humidity sensor Status trap
Set Trap THS Temp	Enables or disables a temperature/humidity sensor Temp trap
Set Trap THS Temphigh	Sets a temperature/humidity sensor Temp trap high limit
Set Trap THS Templow	Sets a temperature/humidity sensor Temp trap low limit
Set Trap THS Humid	Enables or disables a temperature/humidity sensor Humid trap
Set Trap THS Humidhigh	Sets a temperature/humidity sensor Humid trap high limit
Set Trap THS Humidlow	Sets a temperature/humidity sensor Humid trap low limit
Show Traps	Displays trap configurations

## Enabling or Disabling a Status Trap:

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

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

At the Sentry: prompt, type **set trap (tower, infeed, 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:

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

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

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

---

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

---

## Enabling or Disabling a Change Trap:

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

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

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

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

### *Example*

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

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

## 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 Sentry: 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:

```
Sentry: 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 Sentry: prompt, type **set trap ths, templow** or **temphigh**, followed by the sensor name and a value from 0 to 127 in degrees Celsius. Press **Enter**.

### *Example*

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

```
Sentry: set trap ths temphigh .a2 95<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 Sentry: 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:

```
Sentry: 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 Sentry: 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:

```
Sentry: set trap ths humidlow .a1 5<Enter>
```

## Configuring Temperature Recovery Delta (Hysteresis):

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

### *To configure the temperature recovery delta:*

At the Switched CDU: prompt, type **set trap ths tempdelta**, followed by the sensor name, the number of degrees for the recovery delta, and press **Enter**. Valid range is 0-30 C or 0-54 F.

### **Example**

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

```
Switched CDU: set trap ths tempdelta temp_humid_sensor_A1 2<Enter>
```

## Configuring Humidity Recovery Delta (Hysteresis):

The Humidity Recovery Delta command allows configuration of the percentage of change needed to recover from a humidity alarm.

---

**NOTE:** After exceeding a low or high humidity threshold (thus entering an error condition), the humidity value must return past the threshold by the configured recovery delta amount to clear the error condition. Default of humidity recovery delta is 2% relative humidity.

---

### *To configure the humidity recovery delta:*

At the Switched CDU: prompt, type **set trap ths humiddelta**, followed by the sensor name, the percentage for the recovery delta, and press **Enter**. Valid range is 0-20%.

### *Example*

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

```
Switched CDU: set trap ths humiddelta temp_humid_sensor_A1 2<Enter>
```

## Displaying Trap Configuration Information:

The Show Traps command displays information about all traps.

### *To display trap information:*

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

### *Example*

The following command requests trap configuration information:

```
Sentry: show traps <Enter>
Tower trap configuration:
  Tower      Tower      Status
  ID         Name         Trap
  .A         Florida_HQ_1  ON
More (Y/es N/o): y
Input feed trap configuration:
  Input      Input      Status
  Feed ID    Feed Name   Trap
  .AA        HQ_1_Infeed_A  ON
More (Y/es N/o): y
Outlet trap configuration:
  Outlet      Outlet      Change  Status
  ID          Name         Trap     Trap
  .AA1        DataServer_1  OFF      ON
  .AA2        WebServer_1  OFF      ON
More (Y/es N/o): y
Environmental Monitor .A trap configuration:
Name: Florida_HQ_1
Status Trap: ON
Temperature/Humidity Sensor .A1      Temperature/Humidity Sensor .A2
Name: Temp_Humid_Sensor_A1          Name: T/H2_Florida_HQ_1
Status Trap: ON                     Status Trap: ON
Temp Trap: ON                       Temp Trap: ON
  Low: 0   Deg.C                    Low: 0   Deg.C
  High: 127 Deg.C                   High: 95 Deg.C
Humid Trap: ON                      Humid Trap: ON
  Low: 5   % RH                     Low: 0   % RH
  High: 100 % RH                    High: 100 % RH
```

## LDAP

The PDU 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

Command	Description
Add GrouptoLDAP	Grants an LDAP group access to one or more groups
Add OutlettoLDAP	Grants an LDAP group access to one or more outlets
Add PorttoLDAP	Grants an LDAP group access to one or more serial ports
Create LDAPGroup	Adds an LDAP group name
Delete GroupfromLDAP	Removes access to one or more groups for an LDAP group
Delete OutlettoLDAP	Removes access to one or more outlets for an LDAP group
Delete PortfromLDAP	Removes access to one or more serial ports for an LDAP group
List LDAPGroup	Displays all accessible outlet/groups/ports for an LDAP group
List LDAPGroups	Displays privilege levels for all LDAP groups
Ping	Verifies proper DNS configuration by name resolution
Remove LDAPGroup	Deletes an LDAP group name
Set Authorder	Specifies the authentication order for each new session attempt
Set DNS	Sets the IP address of the Domain Name server
Set LDAP Bind	Specifies the LDAP bind request
Set LDAP BindDN	Specifies the user account Fully-Qualified Distinguished Name (FQDN) for binds
Set LDAP BindPW	Specifies the user account password for binds
Set LDAP GroupAttr	Specifies the user class distinguished name (DN) or names of groups a user is a member of
Set LDAP GroupType	Specifies the data type for the Set LDAP GroupAttr command
Set LDAP Host	Sets the IP address or hostname of the Directory Services server
Set LDAP Port	Sets the LDAP server port number
Set LDAP UserBaseDN	Sets the base distinguished name (DN) for the username search at login
Set LDAP UserFilter	Sets the filter used for the username search at login
Set LDAP UseTLS	Enables/disables LDAP over TLS/SSL support
Set LDAP	Enables/disables LDAP support
Set LDAPGroup Access	Sets the access level for an LDAP group
Set LDAPGroup Envmon	Grants or removes access to environmental monitoring
Show LDAP	Displays LDAP configurations
Show Network	Displays network configuration information for all IPv4 and IPv6 settings

## **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 IPM must match.

---

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

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

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

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

### **Setting the LDAP host address:**

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

---

**NOTE:** Both IPv4 and IPv6 formats are accepted for hostname.

---

#### ***To set the LDAP host address:***

At the Sentry: 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:

```
Sentry: set ldap host1 98.76.54.32<Enter>
```

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

```
Sentry: set ldap host2 ldap.servertech.com<Enter>
```

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

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

#### ***To change the LDAP server port:***

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

#### ***Example***

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

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

### **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:** When LDAP Over TLS/SSL is enabled, MD5 binding is disabled.

---

## Setting the LDAP bind type:

The Set LDAP Bind command specifies the LDAP bind request that authenticates a client with the LDAP server.

The PDU supports three standard LDAP bind methods:

**Simple:** Uses unencrypted delivery of username-password over the network to the LDAP server for authentication, showing user credentials in plain text.

**LDAP over TLS/SSL:** Uses a trusted authority certificate to provide encryption of LDAP authentication.

**MD5:** Provides strong protection using 1-way hash encoding that does not transmit the username-password over the network.

### *To set the bind type:*

At the Switched CDU: prompt, type **set ldap bind**, followed by **simple**, **TLS**, 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 Sentry: prompt, type **set ldap binddn**, and press **Enter**. At the following prompt, type the FQDN and press **Enter**.

### **Example**

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

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

The User Membership Attribute is a comma-delimited string of up to two attribute names whose values in the search results are the users that are members of the LDAP group. Maximum number of characters is 61.

---

**NOTE:** The user membership attribute option allows the searching of group directory names by a user membership attribute to find the groups for which the user is a member.

---

### *To set user membership attribute:*

At the Switched CDU: prompt, type **set ldap groupsearch userattr** and press **Enter**.

Then at the following prompt, type the group membership attribute and press **Enter**.

### **Example**

The following sets the user membership attribute to Test

```
Switched CDU: set ldap groupsearch userattr<Enter>
Enter Group Member Attribute <61 character max>
Test<Enter>
```

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

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

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

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

## Setting the group membership attribute:

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

### *To set Group Membership Attribute:*

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

### **Example**

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

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

## Setting the group membership value type:

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

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

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

### **Example**

The following sets group membership value to DN

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

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

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

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

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

### **Example**

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

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

## Setting the user search filter:

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

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

(searchfilter=%s)

where 'searchfilter' is the name of the attribute in the user class which has a value that represents the user's login name. In this string, the '%s' will be replaced by the entered username. Maximum string length is 100 characters.

### *To set the user search filter:*

At the Sentry: prompt, type **set ldap userfilter** and press **Enter**. At the following prompt, type the User Search Filter and press **Enter**.

### **Example**

The following sets the user search filter for MSAD to 'samaccountname':

```
Sentry: set ldap userfilter<Enter>
Enter User Search Filter (Max characters 100):
(samaccountname=%s)<Enter>
```

### Setting the authentication order:

The Set Authorder command sets the authentication order for remote authentication sessions. The PDU 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 PDU 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 PDU device.

---

#### *To set the authentication order:*

At the Sentry: prompt, type **set authorder**, followed by **remotelocal** or **remoteonly** and press **Enter**.

---

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

---

## Displaying LDAP configuration information:

The Show LDAP command displays LDAP configuration information.

- Enabled-disabled status of LDAP support
- Directory Services server IP address and port
- Bind request password type and remote authentication order
- Search bind distinguished name and password
- User search base distinguished name and filter
- Group membership attribute and type

### *To display the LDAP configuration information:*

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

### **Example**

The following command displays the LDAP configuration information:

```
Sentry: show ldap
LDAP Configuration
LDAP:          Enabled
Host 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 68.

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

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

---

**NOTE:** Both IPv4 and IPv6 formats are accepted for DNS IP address.

---

### **Example**

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

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

## Verifying the DNS configuration:

The Ping command can be used to verify the configuration of the DNS IP address.

### *To verify the DNS configuration:*

At the Sentry: prompt, type **ping**, followed by the domain component of the Directory Services server previously configured and press **Enter**.

### **Example**

The following command verifies the DNS configuration:

```
Sentry: ping servertech.com
Pinging servertech.com [98.76.54.32] with 64 bytes of data:
Reply from 98.76.54.32: bytes=64 pseq=0 triptime=0
Reply from 98.76.54.32: bytes=64 pseq=1 triptime=0
Reply from 98.76.54.32: bytes=64 pseq=2 triptime=0
Reply from 98.76.54.32: bytes=64 pseq=3 triptime=0
Reply from 98.76.54.32: bytes=64 pseq=4 triptime=0
```



## Configuring LDAP Groups

### Creating an LDAP group:

The Create LDAPGroup command creates an LDAP group.

#### *To create an LDAP group:*

At the Sentry: prompt, type **create ldapgroup**, optionally followed by a 1-16 character group name (Spaces are not allowed, and LDAP group names are not case sensitive). Press **Enter**.

#### **Example**

The following command creates the LDAP group PowerUser:

```
Sentry: create ldapgroup PowerUser<Enter>
```

### Removing an LDAP group:

The Remove LDAPGroup command removes an LDAP group.

#### *To remove an LDAP group:*

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

### Setting LDAP group access level privileges:

The Set LDAPGroup Access command sets the access level privileges for an LDAP group. The PDU has four defined access privilege levels; Admin, User, On-Only and View-Only.

#### *To set the access level privilege for an LDAP group :*

At the Sentry: prompt, type **set ldapgroup access**, followed by **admin**, **user**, **ononly** or **viewonly**, optionally followed by a LDAP group name and press **Enter**.

#### **Examples**

The following command sets the LDAP group access level for LDAPAdmin to Admin:

```
Sentry: set ldapgroup access admin ldapadmin<Enter>
```

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

```
Sentry: set ldapgroup access user poweruser<Enter>
```

### Granting and removing input status viewing privileges :

The Set LDAPGroup Envmon command grants or removes input status viewing privileges to/from an LDAP group.

#### *To grant or remove input status viewing privileges for an LDAP group:*

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

#### **Example**

The following command grants input status viewing privileges to the LDAP group PowerUser:

```
Sentry: set ldapgroup envmon on poweruser<Enter>
```

### Displaying the LDAP access privilege levels:

The List LDAPGroups command displays all defined LDAP group with their access privilege level.

#### *To display LDAP group access privilege levels:*

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

#### **Example**

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

```
Sentry: list ldapgroups<Enter>
LDAP          Access      Environmental
Group Name   Level       Monitoring
LDAPAdmin    Admin      Allowed
PowerUser    User       Allowed
User         On-Only    Not Allowed
Guest        View-Only  Not Allowed
```

### Adding outlet access to an LDAP group:

The Add OutletToLDAP command grants an LDAP group access to one or all outlets. To grant access for more than one outlet, but not all outlets, you must use multiple Add OutletToLDAP commands.

#### *To grant outlet access to an LDAP group:*

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

Type **add outlettoldap all**, followed by a group name and press **Enter**.

#### **Examples**

The following commands grant the LDAP group PowerUser access to outlets A1 and Webserver\_1:

```
Sentry:add outlettoldap .a1 poweruser<Enter>
Sentry:add outlettoldap WebServer_1 poweruser<Enter>
```

### Deleting outlet access for an LDAP group:

The Delete OutletFromLDAP command removes an LDAP group's access to one or all outlets. You cannot remove access to any outlet for an administrative level group.

#### *To delete outlet access for an LDAP group:*

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

Type **delete outletfromldap all**, followed by a group name and press **Enter**.

### Adding outlet group access to an LDAP group:

The Add GroupToLDAP command grants an LDAP group access to an 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 Sentry: prompt, type **add grouptoldap**, optionally followed by an outlet group name and an LDAP group name. Press **Enter**.

#### **Examples**

The following commands grant to LDAP group PowerUser access to the outlet groups ServerGroup\_1 and ServerGroup\_2:

```
Sentry:add grouptoldap servergroup_1 poweruser<Enter>
Sentry:add grouptoldap servergroup_2 poweruser<Enter>
```

### Deleting outlet group access for an LDAP group:

The Delete GroupFromLDAP command removes an LDAP group's access to an outlet group. You cannot remove access to any group for an administrative level group.

#### *To delete outlet group access for an LDAP group:*

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

### Adding serial port access to an LDAP group:

The Add PortToLDAP command grants an LDAP group access to the serial port.

#### *To grant serial port access to an LDAP group:*

At the Sentry: prompt, type **add porttoldap console** and a group name. Press **Enter**.

### Deleting serial port access for an LDAP group:

The Delete PortFromLDAP command removes an LDAP group's access to the serial port. You cannot remove access to the serial port for an administrative level group.

#### *To delete serial port access for a user:*

At the Sentry: prompt, type **delete portfromldap console** and a group name. Press **Enter**.

## Granting and removing access to environmental monitoring :

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>
```

---

**NOTE:** Granting access to environmental monitoring (temperature/humidity/sensors) to a non-admin user also grants that user access to power monitoring (outlets, infeeds, towers – all the environmental data of the PDU).

---

## Displaying LDAP Group access:

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

### *To display LDAP Group access:*

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

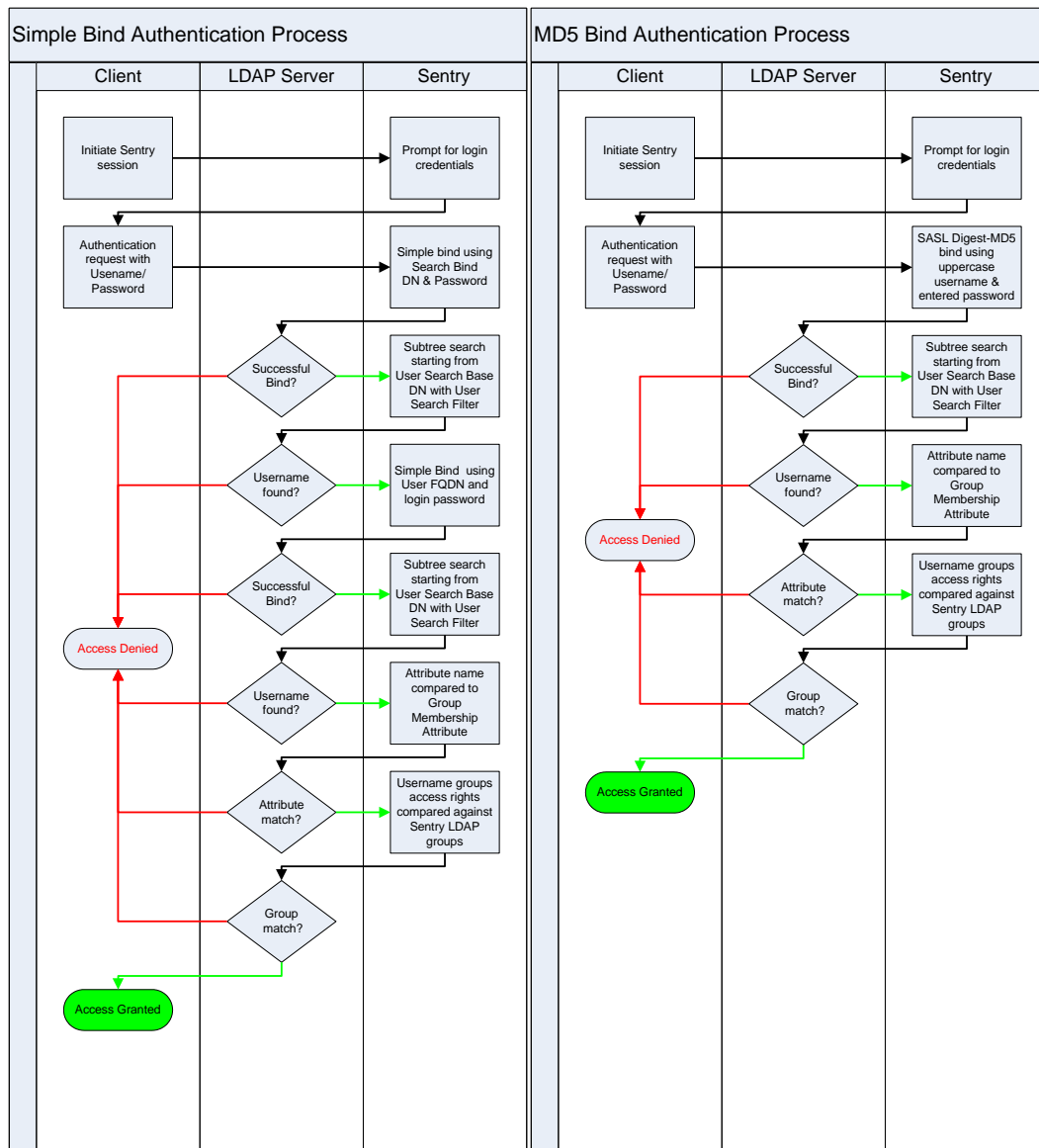
### **Example**

The following command displays information about the LDAP group PowerUser:

```
Sentry: list ldapgroup poweruser<Enter>
Username: PowerUser
  Outlet  Outlet
  ID      Name
  .A1     DataServer_1
  .A2     WebServer_1
Groups:
  ServerGroup_1
  ServerGroup_2
More (Y/es N/o): Y
Ports:
  Port    Port
  ID      Name
  Console Console
```

Members of the PowerUser LDAP group can 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



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

Secure Sockets Layer (SSL)

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\_DES\_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.

## TACACS+

The PDU 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 user's 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 PDU supports 16 different TACACS+ privilege levels; 15 are entirely configurable by the system administrator (1 is reserved for default Admin level access to all Sentry resources).

### TACACS+ Command Summary

Command	Description
Set Authorder	Specifies the authentication order for each new session attempt
Set TACACS	Enables/disables SSL support
Set TACACS Host	Sets the IP address or hostname of the TACACS server
Set TACACS Key	Sets the TACACS encryption key
Set TACACS Port	Sets the TACACS server port number
Show TACACS	Displays TACACS configurations
Add GrouptoTACACS	Grants a TACACS account access to one or more groups
Add OutlettoTACACS	Grants a TACACS account access to one or all outlets
Add PorttoTACACS	Grants a TACACS account access to one or serial ports
Delete GroupfromTACACS	Removes access to one or more groups for a TACACS account
Delete OutlettoTACACS	Removes access to one or more outlets for a TACACS account
Delete PortfromTACACS	Removes access to one or more serial ports for a TACACS account
Set TacPriv Access	Sets the access level for a TACACS account
Set TacPriv Envmon	Grants or removes privileges to view input and environmental monitoring status
List TacPrivs	Displays access levels for all TACACS accounts
List TacPriv	Displays all accessible outlet/groups/ports for a TACACS account

### Enabling and Setting up TACACS+ Support

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

1. Enable TACACS+ support.
2. Define the IP address and domain component of at least one TACACS+server.
3. Set the TACACS+ key configured on the supporting TACACS+server.

#### Enabling and disabling TACACS+ support:

The Set TACACS command is used to enable or disable TACACS+ support.

#### *To enable or disable TACACS+ support:*

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

## Setting the TACACS+ server address:

The Set TACACS Host command sets the IP address or hostname of the TACACS+ server.

---

**NOTE:** Both IPv4 and IPv6 formats are accepted for IP address or hostname.

---

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

At the Sentry: 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:

```
Sentry: set tacacs host1 98.76.54.32<Enter>
```

The following command sets the secondary TACACS+ server address to tacacs.servertech.com:

```
Sentry: 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 PDU and the TACACS+ server. This key must match the key configured on the TACACS+ server.

### *To set the encryption key:*

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

At the TACACS+ Key: prompt, type a key of up to 60 alphanumeric and other keyboard characters (ASCII 32 to 126 decimal). 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**

```
Sentry: set tacacs key<Enter>
TACACS+ Key: <Enter>
Verify TACACS+ Key: <Enter>
```

For security, key characters are not displayed.

---

**NOTE:** A key size of zero results in no encryption being applied which may not be supported by the TACACS+ server and is not recommended for a production environment.

---

## Changing the TACACS port:

With TACACS support enabled, the PDU sends TACACS requests to the default TACACS port number 49. This port number can be changed using the Set TACACS Port command.

### *To change the TACACS port:*

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

### **Example**

The following changes the TACACS port number to 50:

```
Sentry: set tacacs port 50<Enter>
```

## Setting the authentication order:

The Set Authorder command sets the authentication order for remote authentication sessions. The PDU 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 PDU 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 PDU device.

---

### *To set the authentication order:*

At the Sentry: prompt, type **set authorder**, followed by **remotelocal** or **remoteonly** and press **Enter**.

---

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

---

## Displaying TACACS+ configuration information:

The Show TACACS command displays TACACS+ configuration information.

### *To display the TACACS configuration information:*

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

### **Example**

The following command displays the TACACS configuration information:

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

### *To set the access level privilege for a TACACS+ account :*

At the Sentry: prompt, type **set tacpriv access**, followed by **admin**, **user**, **ononly** or **viewonly**, optionally followed by a TACACS+ account number and press **Enter**.

### **Examples**

The following command sets the TACACS+ account access level for account 14 to Admin:

```
Sentry: set tacpriv access admin 14<Enter>
```

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

```
Sentry: set tacpriv access user 5<Enter>
```

### **Granting and removing input status viewing privileges:**

The Set TacPriv Envmon command grants or removes input status viewing privileges to/from a TACACS+ account.

### *To grant or remove input status viewing privileges for a TACACS+ account:*

At the Sentry: prompt, type **set tacpriv envmon**, followed by **on** or **off**, optionally followed by a TACACS+ account number and press **Enter**.

### **Example**

The following command grants input status viewing privileges to the TACACS+ account 5:

```
Sentry: set tacpriv envmon on 5<Enter>
```

### **Displaying the TACACS+ access privilege levels:**

The List TacPrivs command displays all TACACS+ accounts with their access privilege levels.

### *To display TACACS+ account access privilege levels:*

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

### **Example**

The following command displays all TACACS+ account with their access privilege level:

```
Sentry: list tacprivs<Enter>
TACACS      Access      Environmental
Account Name Level      Monitoring
TACAdmin    Admin      Allowed
PowerUser   User       Allowed
User        On-Only    Not Allowed
Guest       View-Only  Not Allowed
```

### **Adding outlet access to a TACACS+ account:**

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

#### *To grant outlet access to a TACACS+ account:*

At the Sentry: prompt, type **add outlettotacacs**, optionally followed by an outlet name and a TACACS+ account number. Press **Enter**, or

Type **add outlettotacacs all**, followed by a TACACS+ account number and press **Enter**.

#### **Examples**

The following commands grant the a TACACS+ account 5 access to outlets A1 and Webserver\_1:

```
Sentry:add outlettotacacs .a1 5<Enter>
Sentry:add outlettotacacs WebServer_1 5<Enter>
```

### **Deleting outlet access for a TACACS+ account:**

The Delete OutletFromTACACS command removes a TACACS+ account's access to one or all outlets. You cannot remove access to any outlet for an administrative level account.

#### *To delete outlet access for a TACACS+ account:*

At the Sentry: prompt, type **delete outletfromtacacs**, optionally followed by an outlet name and a TACACS+ account number. Press **Enter**, or

Type **delete outletfromtacacs all**, followed by a TACACS+ account number and press **Enter**.

### **Adding outlet group access to a TACACS+ account:**

The Add GroupToTACACS command grants a TACACS+ account access to an outlet group. To grant access for more than one outlet group, you must use multiple Add GroupToTACACS commands.

#### *To grant outlet group access to a TACACS+ account:*

At the Sentry: prompt, type **add grouptotacacs**, optionally followed by an outlet group name and a TACACS+ account number. Press **Enter**.

#### **Examples**

The following commands grants to a TACACS+ account number 5 access to the outlet groups ServerGroup\_1 and ServerGroup\_2:

```
Sentry:add grouptotacacs servergroup_1 5<Enter>
Sentry:add grouptotacacs servergroup_2 5<Enter>
```

### **Deleting outlet group access for a TACACS+ account:**

The Delete GroupFromTACACS command removes a TACACS+ account's access to an outlet group. You cannot remove access to any group for an administrative level account.

#### *To delete outlet group access for a TACACS+ account:*

At the Sentry: prompt, type **delete groupfromtacacs**, optionally followed by a outlet group name and a TACACS+ account number. Press **Enter**.

### **Adding serial port access to a TACACS+ account:**

The Add PortToTACACS command grants a TACACS+ account access to the serial port.

#### *To grant serial port access to a TACACS+ account:*

At the Sentry: prompt, type **add porttotacacs console** and a TACACS+ account number. Press **Enter**.

### **Deleting serial port access for a TACACS+ account:**

The Delete PortFromTACACS command removes a TACACS+ account's access to the serial port. You cannot remove access to the serial port for an administrative level account.

#### *To delete serial port access for a TACACS+ account:*

At the Sentry: prompt, type **delete portfromtacacs console** and a TACACS+ account number. Press **Enter**.



## Displaying TACACS account access:

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

### To display TACACS account access:

At the Sentry: prompt, type **list tacpriv**, optionally followed by a TACACS+ account. Press **Enter**.

### Example

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

```
Sentry: list tacpriv 1<Enter>
TACACS+ Privilege Level: 1
  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 can 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 PDU)
rem_addr = 'Sentry3_XXXXXX' (XXXXXX is last six digits of MAC address)
data = "" (null)
```

---

**NOTE:** The password is sent in a CONTINUE packet.

---

Authorization REQUEST Packet includes:

```
authen_method = 6 (TAC_PLUS_AUTHEN_METH_TACACSPLUS)
priv_lvl = 0 (TAC_PLUS_PRIV_LVL_MIN)
authen_type = 1 (TAC_PLUS_AUTHEN_TYPE_ASCII)
authen_service = 1 (TAC_PLUS_AUTHEN_SVC_LOGIN)
user = (entered username)
port = (access path into the PDU)
rem_addr = 'Sentry3_XXXXXX' (XXXXXX is last six digits of Ethernet MAC address)
service = 'shell' (for exec)
cmd = "" (null)
```

---

**NOTE:** The access paths into the PDU 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.

---

## Logging

The PDU 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.

---

The PDU 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.

### **Syslog**

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

#### **Syslog Command Summary**

Command	Description
Set Syslog HostIP	Sets the IP address of the Syslog server
Set Syslog Port	Sets the Syslog server port number
Show Syslog	Displays all Syslog configuration information

#### **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 Sentry: 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:

```
Sentry: 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 can be changed using the Set Syslog Port command.

*To change the Syslog port:*

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

#### **Example**

The following changes the Syslog port number to 411:

```
Sentry: 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 Sentry: prompt, type **show syslog** and press **Enter**.

### **Example**

The following command displays the Syslog configuration information:

```
Sentry: 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**

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

### **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 Sentry: 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.

---

**NOTE:** Both IPv4 and IPv6 formats are accepted for IP address or hostname.

---

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

At the Sentry: 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:

```
Sentry: set email smtp 55.55.55.55<Enter>
```

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

```
Sentry: set email smtp email.servertech.com<Enter>
```

## Changing the SMTP server port:

With SMTP support enabled, the PDU sends SMTP requests to the default SMTP port number 25. This port number can be changed using the Set Email SMTP Port command.

### *To change the TACACS port:*

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

### **Example**

The following changes the SMTP port number to 5555:

```
Sentry: 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 Sentry: 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:

```
Sentry: 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 Sentry: 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:

```
Sentry: set email primaryto DayAdmin@servertech.com<Enter>
```

The following command sets the secondary 'to' email address to NiteAdmin@servertech.com:

```
Sentry: 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 106.

### *To enable or disable event notification types:*

At the Sentry: 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:

```
Sentry: set email event enabled<Enter>
```

The following command sets the disables email notification authentications attempts:

```
Sentry: 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 Sentry: prompt, type **show email** and press **Enter**.

### **Example**

The following command displays the Email configuration information:

```
Sentry: 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 PDU 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

Command	Description
Set FTP Server	Enables or disables the FTP server
Show FTP	Displays FTP configuration information

### Sentry Integrated FTP Server

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

**NOTE:** The integrated FTP Server does NOT support web browser FTP file transfers.

A non-web-browser is required for all Upload/Download requests.

### 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 Sentry: prompt, type **set ftp server**, followed by **enabled** or **disabled** and press **Enter**.

### FTP Configuration Files

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

- CONFIG.BIN This file contains the entire configuration of the PDU excluding TCP/IP settings, serial/factory-only configurations, the x.509 certificate (SSL) and SSH keys. This file is 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 PDU 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 PDU.  
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.  
*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 PDU 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 PDU and force a restart of the device.  
FTP> close

### Appendix A: Resetting to Factory Defaults

You can reset the non-volatile RAM that stores all configurable options. This clears all administrator –editable fields and reset all command line configurable options to their default values, including all user accounts.

You can 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 can be necessary when a forgotten password prevents administrator login. Each of the methods updates the current working configuration to the factory defaults.

#### 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 click **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 you disable the **Reset** button.

---

Insert the tool in the recess, then depress and hold the reset button for at least ten seconds.

---

**NOTE:** If you press and hold the **Reset** button for more than 15 seconds, the reset will terminate.

---

#### 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 click **Apply**.

#### From the command line

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



## Appendix B: Uploading Firmware

You can 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.

---

You can initiate an FTP upload session by issuing a command or from the Web interface. You must have administrator-level privileges to initiate an upload.

### **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**.

Upon issuing this command the unit will restart and upload the firmware file specified with the FTP Filename command from the previously configured FTP Host.

### **Initiate an FTP upload session from the command line**

The Restart FTPLoad command initiates an upload of firmware. Upon issuing this command the unit will restart and upload the firmware file specified with the FTP Filename command from the previously configured FTP Host.

To initiate an FTP firmware upload session:

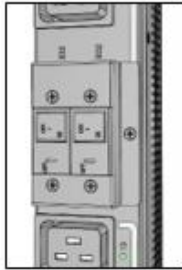
At the Sentry: prompt, type **restart ftpload** and press **Enter**.

## Appendix C: Technical Specifications

### Branch Circuit Protection

Server Technology PDUs are equipped with one of several types of Branch Circuit Protection, including internal fuses, retractable fuse holders, and circuit breakers, as illustrated below.

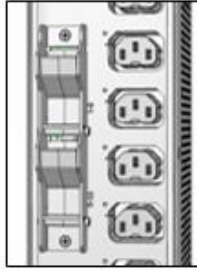
These fuses and circuit breakers meet the strict safety requirements of UL 60950-1 and EN 60950-1 for Branch Circuit Protection.



Circuit Breaker



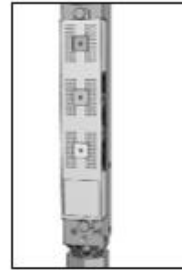
Compact Fuse Holder



Fuse Retractor



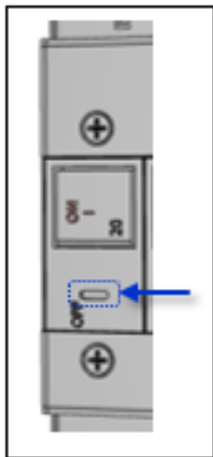
Fuse Access Window



Fuse Access Cover

### Circuit Breaker

If a circuit breaker is tripped, it can be reset by pressing or switching it back ON once the cause of the overload or short circuit has been identified, removed, or resolved. Intelligent PDUs with branch circuit sensing will display a flashing *FE* on the input current LED(s) to indicate *Fuse Error*.



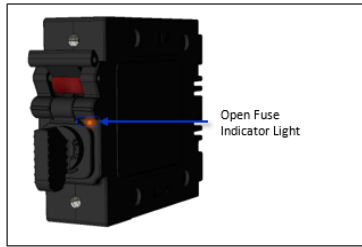
Alternatively, the circuit breaker can be turned OFF manually by inserting a slotted or flat-blade tool into the OFF switch as shown in the illustration on the left.

It is not necessary to disconnect the AC power source to perform this operation.

**NOTE:** This circuit breaker contains no user-serviceable parts. Do not open or disassemble this part.

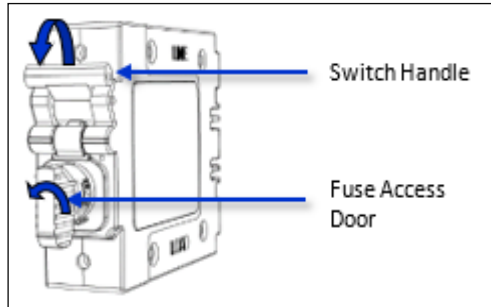
## **Compact Fuse Holder**

The Compact Fuse Holder is a UL 98 listed Fused Disconnect Switch that allows the user to turn OFF the branch circuit and safely service the fuse without having to disconnect the PDU AC power source prior to performing this operation.



To help identify which fuse is open, blown, or missing, the Open Fuse Indicator Light glows **orange** when the PDU is powered and the Switch Handle is in the ON position.

Additionally, intelligent PDUs with branch circuit sensing will display a flashing *FE* on the input current LEDs to indicate *Fuse Error*.



To service the fuse or turn OFF the branch, rotate the Switch Handle toward the Fuse Access Door.

Next, rotate the Fuse Access Door counter clock-wise until it opens.

Only replace the fuse with the same size, type, and ratings as the original fuse.

Reverse these steps after the new fuse(s) is installed.

---

### **CAUTION:**

- Failure to replace the fuse with the same size, type, and ratings will damage the PDU and the connected and nearby equipment, and will cause electrical shock, fire, explosion, or injury/death.
  - Do not attempt to open the Fuse Access Door without first setting the Switch Handle in the OFF position. Forcibly rotating the Fuse Access Door will damage the fused holder.
-

## Fuse Retractor, Fuse Access Window, and Fuse Access Cover

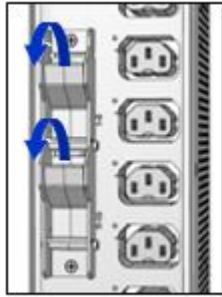


**The PDU AC power source must be disconnected prior to servicing a unit with the Fuse Retractor, Fuse Access Window, and Fuse Access Cover.**

Intelligent PDUs with branch circuit sensing will display a flashing *FE* on the input current LEDs to indicate *Fault Error*.

For the fuse retractor, rotate the fuse holder exposing the fuse.

For the fuse access window or cover, remove the screws that secure the plastic cover.



Fuse Retractor



Fuse Access Window



Fuse Access Cover

Once the fuses are exposed, carefully remove and replace with a new one of the same size, type, and ratings as the original. A fuse puller may be needed for fuse access windows and covers.

Reverse these steps after the new fuse(s) is installed.

---

### **CAUTION:**

- Failure to replace the fuse with the same size, type, and ratings will damage the PDU and the connected and nearby equipment, and will cause electrical shock, fire, explosion, or injury/death.
- 

## Time-Delay Fuses – Class G

**NOTE:** Server Technology PDUs ship with Bussman SC-20 fuses.

Ampere Rating	Voltage	Interrupting Rating	Bussman Part No.*	Server Technology Part No.
20 A	600 Vac	100,000 A RMS Sym. AC	SC-20	FUSE-SC20G

\* Cooper Bussman Technical Data Sheet 1024

For technical support or service with time-delay fuses, contact Server Technology as follows:



### **Experience Server Technology's FREE 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: 1-800-835-1515

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

Reno, Nevada 89521 USA

Fax: 775-284-2065

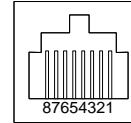
Email: [support@servertech.com](mailto:support@servertech.com)

## Data Connections

### **RS-232 port**

Intelligent IPMs are equipped standard with an RJ45 DTE RS-232c serial port. This connector can be used for direct local access or from other serial devices such as a terminal server. An RJ45 crossover cable is provided for connection to an RJ45 DCE serial port.

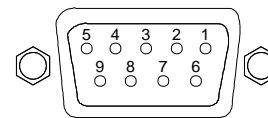
Pin	DTE Signal Name		Input/Output
1	Request to Send	RTS	Output
2	Data Terminal Ready	DTR	Output
3	Transmit Data	TD	Output
4	Signal Ground		
5	Signal Ground		
6	Receive Data	RD	Input
7	Data Set Ready	DSR	Input
8	Clear to Send	CTS	Input



### **RJ45 to DB9F serial port adapter**

Additionally, an RJ45 to DB9F serial port adapter is provided for use in conjunction with the RJ45 crossover cable to connect to a PC DB9M DCE serial port. The adapter pin-outs below reflect use of the adapter with the provided RJ45 crossover cable.

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



## LED Indicators

### **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 60950-1:2007 and CAN/CSA 22.2 No. 60950-1-07
- European Union EN 60950-1:2006 + A11 + A1 + A12

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 the user's 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 exigences du Règlement sur le matériel brouilleur du Canada.

### **European Union Notification**

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms:

- EN55022 Electromagnetic Interference
- EN55024 Electromagnetic Immunity
- EN60950-1 Product Safety



- EN61000-3 Harmonics and Flicker

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。

## **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.

## Appendix D: Product Support Information

### Warranty

For Server Technology warranty information, visit our website: [www.servertech.com](http://www.servertech.com)

### Technical Support



#### **Experience Server Technology's FREE 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: 1-800-835-1515

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

Reno, Nevada 89521 USA

Fax: 775-284-2065

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

### Return Merchandise Authorization

If you have a product that is not functioning properly and needs technical assistance or repair, see the Server Technology **Return Merchandise Authorization** process at: [www.servertech.com](http://www.servertech.com)





## Server Technology®

HEADQUARTERS -  
NORTH AMERICA  
Server Technology, Inc.  
1040 Sandhill Road  
Reno, NV 89521  
United States  
1.775.284.2000 Tel  
1.775.284.2065 Fax  
sales@servertech.com  
www.servertech.com  
www.servertechblog.com

Western Europe, Middle East and  
Africa  
Server Technology  
Fountain Court  
2 Victoria Square  
Victoria Street  
St. Albans  
AL1 3TF  
United Kingdom  
+44 (0) 1727 884676 Tel  
+44 (0) 1727 220815 Fax  
salesint@servertech.com

Central Europe, Eastern Europe and  
Russia  
Niederlassung Deutschland  
Server Technology LLC  
42119 Wuppertal  
Germany  
Tel: + 49 202 693917 x 0  
Fax: + 49 202 693917-10  
salesint@servertech.com

APAC  
Server Technology  
Room 2301, 23/F, Future Plaza  
111-113 How Ming Street,  
Kwun Tong, Hong Kong  
Direct line: +852 3916 2048  
Fax Line: +852 3916 2002  
salesint@servertech.com