



SmartZone[™] Gateway EPA126

User Manual

IM011

Release 1.0 Issue 2

SmartZone Gateway EPA126 User Manual

Copyright © 2014 Panduit Corp. All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from Panduit. No patent liability is assumed with respect to the use of the information contained herein.

Although every precaution has been taken in the preparation of this book, Panduit assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Table of Contents

Introduction	8
Remote Temperature and Humidity Sensing	8
PDU Monitoring	
EPA126 Package	
Front of Gateway EPA126	9
LEDs	9
Network	
Status	9
Power	10
Buttons	10
Back of Gateway EPA126	10
Output Relays	11
Installation Requirements	12
Rack Mounting	12
Equipment Required	12
Before You Begin	12
Installation Warning Statements	12
Rack-Mount the EPA126	13
Initial Setup	14
Default Settings	14
Connecting to the Web Management Interface	14
Changing your PC's IP Address	14
Connecting to the SmartZone Gateway Web Management Interface	19
Initial Network Setup	21
Entering NMS Details	21
Entering Trap Receiver Details	21
Adding Users	
Changing the Unit IP Address	23
HID Reader	24
HID 26 Bit Cards	
HID Corporate 1000 Cards	
Web Management Interface	
Network Setup - Overview	
Setup - IP Configuration	
System Name	
System Location	29
Contact Name	
IP Address	
Subnet Mask	
Gateway	
Config. Protocol	

Setup - HTTP or HTTPS	
Setup – LDAP Servers	
Enabled/Disabled	
Credential Cache	
Primary/Secondary LDAP Server	
Display Name	
IP Address	
Unit Base DN	
Users Base DN 1	
Users Base DN 2	
Setup - SNMP NMS	
NMS IP Address	
Community String	
NMS Access	
Setup - SNMP Receivers	
Receiver IP Address	
Community String	
Receive Traps	
Trap Version	
Setup - Modbus	
Setup - Users	
Username	
Password	
Level	
Setup - Email Alerts	
Setup - Events	40
Setup - Syslog Servers	41
Setup - Time Settings	41
Time Adjustments	42
Setup - Preferences	43
Setup – Restart	44
Restart Unit	44
Restart Now	44
Reset to Factory Defaults	
Input Sensors – Configuration and Status	45
Status	45
Status Indicators	45
Input Sensors – Defaults	46
Calibration Offset	46
Hysteresis Value	46
Limits and Traps	46
Repeat Timer	47
Normal State	47
Trigger Type	47

	47
Normal to Non-Normal (Positive Edge)	
Non-Normal to Normal (Negative Edge)	
Input Sensors - Configure	
Туре	
Outputs – Status	
Control	
Outputs – Configure	
Outputs - Configure - Config	
Input Selection	
Invert	
Logic Operator	54
Logical AND Inputs	54
Logical OR Inputs	54
Delay Timer On	54
Delay Timer Off	
Final Invert	55
Access Control – Configure	
ACU	56
Туре	
Name	56
Timeouts - Door Latch	57
Timeouts – Return to Standby	
ACU In Use Trap	57
Access Code Length	57
Access Control – Codes	57
Name	58
Access Code	
Applied To	58
Access Control – Override	
Power – Configuration and Status	60
Power - Status	60
Status Indicators	60
Power Strips - Configure	61
Control Method	61
HTTP + SNMP	61
HTTP Only	
SNMP Only	62
RS232 Only	
Cycle Up/Down Delay	
Repeat Timer (on Comms Failure)	
Reboot Delay	
Abort Cycle Delay	
, , ,	

Power – Configure Menu	62
Circuit Name	63
RMS Volts	64
Repeat Timer	64
RMS Current	65
Total Power	65
PDU Outlets	65
Power Strips – Control	65
Switching Individual Sockets	
Switching an Entire Strip	66
LDAP	67
SmartZone Gateway LDAP Overview	67
SmartZone Gateway LDAP Structure	67
Group Membership and Access Level	68
Gateway AdminUsers	68
Gateway ControlUsers	69
Gateway ViewUsers	69
SmartZone Gateway Unit Configuration	69
EPAX18 Expansion Unit	
Front of Gateway EPAX18	70
LEDs	70
Network	70
Status	70
Power	71
Installation	71
Gateway Web Management Interface PDU Display	73
Temperature Sensor Adapter Installation	75
New Installations	75
Existing Installations.	75
Fitting the Adapter In-line.	76
Troubleshooting	77
Resetting the SmartZone Gateway to Factory Default Settings	77
Problem: The NMS Cannot Poll the SmartZone Gateway Unit	77
Technical Support	78
Appendix A: Technical Details	
Factory Default Settings	79
Operating Information	79
Appendix B: Hysteresis Demystified	
Appendix C: Networking Reference	82
Reference	82
Communities	82
IP Addresses	82
Subnetting and Subnet Masks	83
Gateways	84

Appendix D: Pressure to Voltage Conversion	85
Appendix E: Encryption and Security	86

Introduction

The SmartZone[™] Gateway EPA126 is a compact device used to monitor and control up to 6 PDUs and 12 multifunction inputs (temperature, humidity, voltage, and digital inputs).

The unit comprises both an SNMP interface and a secure web-based interface for monitoring and management.

Some of the main features of the EPA126 unit are:

- Secure web management and configuration interface.
- SNMP enabled.
- 12 monitoring channels.
- Monitoring of up to 6 PDUs.
- Optional LCD Status module.

Remote Temperature and Humidity Sensing

The Gateway EPA126 has the capability to monitor temperature and humidity and raise alarms or take action if a user-configured threshold is crossed.

PDU Monitoring

The EPA126, via intelligent PDUs, allows around-the-clock monitoring of the electrical power environment of the rack.

EPA126 Package

The standard EPA126 package contains a EPA126 unit with supporting hardware, including a localized mains lead.

Front of Gateway EPA126

The following image shows the front panel of the EPA126 unit:



LEDs

LEDs can be found on the front of the EPA126 unit. Their purpose is described below.

Network

- Link (green): Embedded in RJ45 Ethernet connection. Illuminates when an Ethernet link is established. Flashes with network activity.
- **Speed**(amber): Illuminates when 100mbps connection is used.

Status

- CPU: Indicates system activity.
- Alarm: Indicates any alarm condition.

Power

- **On**: Illuminates when unit is powered.
- Feed B (amber): Illuminates when mains power is present to input Feed B.
- Feed A (amber): Illuminates when mains power is present to input Feed A.

Buttons

There are two buttons on the rear of the EPA126 unit:

- Reset: Allows the user to reboot the unit.
- **Mode**: The mode select switch is used to reset the unit to factory defaults. See the section for details.

Back of Gateway EPA126



- Power Input B: Redundant mains or -48v DC voltage power feed.
- Earth: Grounding stud.
- **Output Relays**: Connect up to four output devices (such as Front and Back Electronic Swing Handles, and more).
- Sensor Ports 1 through 12: Connect up to 12 sensors (such as Temperature, Humidity, Water, Door Contacts, and more).
- **PDU Ports 1 through 6**: Connect up to six power devices (such as Gateway-Enabled Rack PDUs, Inline Meters, and Clamp Meters).
- Access Ports: Connect up to two access and control devices (such as Keypads or HID Card Readers). Must select one type (not mix and match).
- Serial Port: Attach optional devices (such as LCD Status Monitor Unit).
- **Network Port**: An RJ-45 port to connect Gateway to LAN/Network.

- Notifications: Reset/Mode/Power/Status/Alarm notifications duplicated from the Front Panel.
- Power Input A: Mains or -48v DC voltage.

Output Relays

Use the Output Relays to connect up to four output devices (such as Front and Back Electronic Swing Handles, and more). The following diagram shows the output relays of the EPA126 unit:



Installation Requirements

- SmartZone Gateway EPA126 unit.
- IEC mains lead (supplied localized).
- Ethernet or Fast Ethernet network connection.
- Network-connected computer system to setup the EPA126 Unit.

Rack Mounting

This section covers the basic 19-inch rack-mounting of the Gateway EPA126 unit.

Equipment Required

You need to supply a number-1 and a number-2 Phillips screwdriver to rack-mount the Gateway EPA126 unit.

Before You Begin

When determining where to install the Gateway EPA126 unit, please verify that these guidelines are met:

- Airflow around the Gateway EPA126 is unrestricted.
- Clearance to the front and rear panels meet these conditions:
- Front-panel LEDs can be easily read.
- Access to ports is sufficient for unrestricted cabling.
- AC power cord from the power supply can reach the AC power outlet and the Gateway EPA126.
- The 10/100 network cabling does not exceed 100 meters from the Gateway EPA126 to the Network switch.
- Temperature around the EPA126 does not exceed 40° C.
- Humidity around the Gateway EPA126 does not exceed 90%.

Installation Warning Statements

Note: Only trained and qualified personnel should be allowed to install, replace or service this equipment

- To prevent the Gateway unit from overheating, do not operate in an area that exceeds the maximum recommended ambient temperature of 40° C.
- Installation of the Gateway unit must comply with local and national electrical codes.
- To prevent personal injury when mounting or servicing the Gateway unit, ensure that the rack or cabinet is adequately secured so that the system remains stable.
- Circuit Overloading Consult the equipment nameplate ratings when connecting the equipment to the supply circuit to avoid overloading of circuits. Overloading circuits can adversely affect current protection and supply wiring.
- Maintain reliable grounding of rack-mounted equipment. Particular attention should be given to supply connections other than direct connections to the branch circuit (for example, the use of PDUs).

Rack-Mount the EPA126

Hold the Gateway EPA126 and attach the bracket to rack using two 12-24 screws.



Initial Setup

Default Settings

The SmartZone Gateway unit in factory default condition has the following network configuration. Advanced users may wish to make use of these settings to access the Gateway unit's Web Management Interface immediately and proceed with configuration.

Users who do not know how to do this should proceed through this section for information on how to configure the Gateway unit.

IP Address	192.168.0.253
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
Web Management Address	http://192.168.0.253/
Default username	admin
Default password	admin

Note: Password entries are case-sensitive.

Connecting to the Web Management Interface

The SmartZone Gateway monitoring solution can be configured entirely using the builtin Web Management Interface.

You may need to change the IP address of the PC to connect to the Web Management Interface for the first time. The following section details how to change the IP address and connect to the Web Management Interface.

Changing your PC's IP Address

Note: Instructions refer specifically to Windows 7. Please refer to your operating system documentation if you are not using Windows 7.

1. Click the Windows button and select **Control Panel**.



2. In the Control Panel window, select **View network status and tasks** under the Network and Internet heading.



3. Select Change adapter settings from the menu on the left.



- 4. Select Local Area Connection.
- 5. Select **Internet Protocol (TCP/IP) Version 4** (you may need to scroll down). Then click the **Properties** button.

Local Area Connection Properties	×
Networking Sharing	
Connect using:	
Intel(R) 82579LM Gigabit Network Connection	
Configure.	
 Client for Microsoft Networks VMware Bridge Protocol QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Version 9 (TCP/IPv4) 	
Install Uninstall Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
ОК Са	ncel

6. Select the **Use the following IP address** radio button. The **Use the following DNS server addresses** radio button then selects automatically.

Internet Protocol Version 4 (TCP/IPv4)	Propertie	s	Į	?	x
General					
You can get IP settings assigned autom this capability. Otherwise, you need to for the appropriate IP settings.	atically if ask your i	your n netwo	etwork s rk admini	upports strator	
Obtain an IP address automaticall	y				
O Use the following IP address:					- II
IP address:					
Subnet mask:					
Default gateway:		•			
Obtain DNS server address autom	atically				
Ose the following DNS server address	esses:				
Preferred DNS server:	•				
Alternate DNS server:			•		
Validate settings upon exit			Adva	inced	
		ОК		Cance	1

Enter the following details into the appropriate boxes.

- IP address: 192.168.0.10
- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.0.1
- Preferred DNS server: 192.168.0.1
- 7. Click **OK** to accept the entries.

Internet Protocol Version 4 (TCP/IPv4)	Properties
General	
You can get IP settings assigned autor this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator
Obtain an IP address automatical	ly
Ouse the following IP address:	
IP address:	192.168.0.10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192.168.0.1
Obtain DNS server address auton	natically
Ose the following DNS server add	resses:
Preferred DNS server:	192.168.0.1
Alternate DNS server:	•••
Validate settings upon exit	Advanced
	OK Cancel

8. On the Local Area Connection Properties, click **OK** to return to the desktop.

Connecting to the SmartZone Gateway Web Management Interface

1. Connect the SmartZone Gateway unit's network connection directly to a PC's Ethernet network card using a patch cable.

Note: A crossover cable must be used when directly connecting the Gateway unit to a PC's network card.

- 2. Power the Gateway unit.
- 3. Open a web browser.
- 4. Enter the following in the address field: http://192.168.0.253.
- 5. The Web Management Interface loads.

PANDUIT

Username: Password: Login	
Model Number: Serial Number: Firmware:	EPA126 656546-01-32454 2.06.04

- 6. Click login and enter the username and password. The unit defaults are:
- Login:admin
- **Password**:admin

Note: Password entries are case sensitive.

Initial Network Setup

This section provides details on preparing the unit for network access and allowing Simple Network Management Protocol (SNMP) network management.

Connection to the Web Management Interface is required.

Entering NMS Details

1. Click the **Setup** tab on the top menu bar, and then select the **SNMP NMS** link on the left menu bar.

Pand	IUIT								Logged In: admin System Name	(Administrator) SAP SZ Cabinet Logout
						Setup	Input Sensors	Outputs	Access Control	Power
	Setup / SNMP (Netw	ork Management Statio	ons)							
IP Config HTTP Certificates	SNMP access creden	tials are configured her	e. The device sup	ports both SNMPv2c access (I	using Community Strings)	and SNMPv3 a	ccess (using USM Use	ers).		
SNMP NMS	Select the SNMP ve	rsion you wish to config	ure:		SNMPv2c V					
SNMP Rec'rs Users Email Alerts Time Settings Syslog Servers	Community string a Read Only access po Read / Write access Note: To disable SN	nd access permissions armits an NMS using the permits an NMS using MPv2 clear all commu	are specified here specified commu the specified com inity strings.	for the Network Management unity string to use only GET co munity string to use both GET	t Stations. ommands. I and SET commands.					
Events		Community String:	NMS Access:							
Preferences Restart	NMS 1	public	Read Only 🔻							
	NMS 2	private	Read / Write 🔻							
	NMS 3		Read Only 🔻							
	NMS 4		Read Only V							
	NMS 5		Read Only V							
										Stud
										Save

- 2. Enter the chosen community string and required Network Management Station (NMS) access permissions of the NMSs to be used.
- 3. Click **Save** to confirm the changes.
- 4. To disable an NMS, select the **Disabled** option from the **NMS Access** drop-down list.

Entering Trap Receiver Details

- 1. Click the **Setup** tab on the top menu bar.
- 2. Select the SNMP Rec'rs link on the left menu bar.

SmartZone Gateway EPA126 User Manual

NDUIT						Logged In: admin System Name	(Administrator) : SAP SZ Cabinet Logout
			Setup	Input Sensors	Outputs	Access Control	Power
Setup / SNMP (Receivers) Authors in the setup of the set	d here. d to receive SNMP traps sent from this unit m enabled, are generated if an attempt is made format contained within a SNMPv3 message Beceives ID Adduscr:	nust be entered here. e to access the unit with an invalid c e. Authentication or Encryption is no	community stri t supported.	ng.	T	ran Varrian:	
5 Receiver 1	10 64 69 101		Enabled	Tups.		20.	
Receiver 2	10.136.202.90		Enabled	•	l l	2c •	
Receiver 3			Disabled	•	l v	1 •	
Receiver 4			Disabled	•	v	1 •	
Receiver 5			Disabled	•	v	1 •	
Receiver 6			Disabled	•	v	1 •	
Receiver 7			Disabled	T	v	1 •	
Receiver 8			Disabled	•	v	1 •	
Receiver 9			Disabled	٣	v	1 🔻	
Receiver 10			Disabled	۲	v	r1 🔻	
							Test All Save

- 3. Enter the **IP address**.
- 4. Choose whether to enable traps, disable traps, or enable traps including authorization failures (meaning the unit will issue traps if an unauthorized IP address attempts to access the unit's SNMP functions) for each receiver.
- 5. Select Trap Version v1 or v2c.
- 6. Click **Save** to confirm the changes.

Adding Users

- 1. Click the **Setup** tab on the top menu bar.
- 2. Select the Users link on the left menu bar.

PAND	UIT							Logged In: admin (System Name:	Administrator) SAP SZ Cabinet Logout
					Setup	Input Sensors	Outputs	Access Control	Power
Overview IP Config HTTP Certificates SNMP NMS SNMP Rec'rs	Setup / Users Administrator: Confi Controller and Viewe	guration settings can be viewed a er: Configuration settings can only Username:	nd modified. / be viewed. Password:	Level:					
Users	User 1	admin		Administrator V					
Email Alerts	liser 2	szadmin		Administrator T					
Syslog Servers	User 2	support		Viewor					
Events Preferences	User 4	support		Administrator T					
Restart	User 5			Administrator					
	User 6			Administrator					
	User 7			Administrator					
	User 8			Administrator T					
	User 9			Administrator V					
	User 10			Administrator T					
	User 11			Administrator V					
	User 12			Administrator 🔻					
	User 13			Administrator 🔻					
	User 14			Administrator V					
	User 15			Administrator •					
	User 16			Administrator *					
	User 17			Administrator •					
	User 18			Administrator •					
	User 19			Administrator T					
	User 20			Administrator •					
									Save

- 3. You can set usernames, passwords, and access levels here. Unique usernames can be set for individuals who require web management access to the Gateway unit.
- 4. Click **Save** to confirm the changes.

Changing the Unit IP Address

- 1. Click the **Setup** tab on the top menu bar.
- 2. Select the **IP Config** link on the left menu bar.

Pand	UIT										Logged In: admin (System Name:	Administrator) SAP SZ Cabinet Logout
								Setup	Input Sensors	Outputs	Access Control	Power
Overview	Setup / IP Configura	ation										
IP Config HTTP Certificates	Network settings for	r this unit are set h	nere. This will be th	e IP address	that is used to acc	cess the web ma	anagement int	erface and by	a Network Manage	ment Station.		
SNMP Rec'rs Users	System Name:		s	SAP SZ Cabinet							Include in Trap 🕑	
Email Alerts	System Location:		S	Z Cabinet - LOC	CATION-NAME						\$	
Syslog Servers	Contact Name:		5	Z Cabinet Admir	n							
Events Preferences Restart	IP Stack Selection:	Dual •										
	Config. Protocol:	IP DHCP V	'v4	AutoConfig Only	۲		IPv6					
	IP Address:	192.168.0.253										
	Subnet Mask:	255.255.255.0										
	Gateway:	192.168.0.1										
	If Domain Names ar	e to be used, eithe	r here or on other f	orms, then th	he IP address of at	nt least one Dom	iain Name Serv	ver is require	1.			
	DNS Servers Enabled:	Disabled v										
	DNS Server 1 - IP Address:	**]							
	DNS Server 2 - IP Address:	::										
	Upgrade Port [69]:	Enabled •										
												Save

- 3. Enter the **IP Address**, **Subnet Mask**, and the **Gateway** address that the SmartZone Gateway unit will use (required). Contact your network administrator if you do not know the values that you must enter here.
- 4. Select the Config. Protocol (Static, DHCP, or BootP).
- 5. Enter the SNMP **System Name, System Location**, and **Contact Name** if required. These fields will be added to all SNMP traps generated by the unit.
- 6. Click **Save** to confirm the changes.
- 7. Click **Restart** ,and then select **Restart Now** to reboot the unit and implement the changes.

Note: Once the IP configuration has changed, the Gateway unit will no longer be accessible via the default IP address, because the new address will be operational.

The Gateway unit should now be connected to the main network and any further required configuration will be done via the unit's new IP address.

HID Reader

The SmartZone EPA Series Gateways include Smart Card readers that support HID 26 bit cards and HID Corporate 1000 cards.

HID 26 Bit Cards



For 26 Bit cards the Gateway interface must be programmed for nine digits.

Pand	UIT					
	Access Control / Configure					
Configure						
Access Codes						
Override	ACU	Туре	Name			
	1: ACU1	Disabled 👻	ACU 1			
	2: ACU2	Disabled 👻	ACU 2			
	Access Cod	e Length: 9 🔻				

These nine digits consist of the following:

- 3-digit site code
- 1 hyphen
- 5-digit User ID code

Example: 001-21627

Note: The hyphen character must be input (it is included in the length).

HID Corporate 1000 Cards



Corporate Site IDs are not normally printed on HID Corporate 1000 cards. This is confidential to each organization. You will need to ask the security office of the organization or supply company for the Site ID code, which is a four-digit number.

For 34 Bit Corporate 1000 cards, the Gateway interface must be programmed for 12 digits.



These 12 digits consist of the following:

- 4-digit site code
- 1 hyphen
- 7-digit User ID code

Example: 001-21627

Note: The hyphen character must be input (it is included in the length).

If the user ID code does not have seven digits, then the ID number must be padded out with leading zeros. Thus an ID code of "00165" becomes: "0000165".

Example for a card with a 2033 Site ID: 2033-0000165

Web Management Interface

The SmartZone Gateway unit has a built-in Web Management Interface that can be accessed securely. The interface permits complete configuration and monitoring of the Gateway unit.

Windows where changes can be made have a **Save** button in the lower right-hand area. Click **Save** to activate and save any changes made.

Network Setup - Overview

The Overview page is the first page displayed and provides the user with an overview of the Gateway unit's current status.

	UIT							Logged In: admin (System Name:	Administrator) SAP SZ Cabinet Logout
	Network Setup / Ove	erview			Setup	Input Sensors	Outputs	Access Control	Power
view onfig TP icates NMS Rec'rs ers	System Name: System Location: System Contact:	SAP SZ Cabinet SZ Cabinet - LOCATION-NAME SZ Cabinet Admin							
Alerts ettings Servers nts rences tart	MAC Address: Serial Number: Firmware Version: Hardware Revision: System Uptime:	00:07:6e:02:7e:c6 656546-01-32454 2.06.05 ZBHTEIBB-01 v1.02.02 [DRAM:32M 0 days, 4 hours, 8 mins, 28 secs	B Used:16MB]						
	IP Stack: IP Address: Subnet Mask:	Dual IPv4 10.132.80.196 255.255.255.0	IPv6 Auto Conf. FE80::207:6EFF:FE02:7EC6 /64	IPv6					
	Gateway: Config. Protocol: Logged In User:	10.132.80.1 DHCP admin	Auto Configured IPv6						
	Access Level: Model Number:	Administrator EPA126							

System name, MAC address, serial number, firmware version, and other system details can be found here.

Setup - IP Configuration

The IP Config page allows you to set the SmartZone Gateway unit's own management IP address.

JUIT										Logged In: admin (System Name:	Administrator) SAP SZ Cabinet Logout
	••						Setup	Input Sensors	Outputs	Access Control	Power
Network settings for	this unit are se	t here. This will be	the IP address	that is used to a	access the web m	anagement inte	rface and by	a Network Manager	nent Station.		
System Name:			SAP SZ Cabinet				1			Include in Trap	
, System Location:			SZ Cabinet - LOO	CATION-NAME						v	
Contact Name:			SZ Cabinet Admi	in							
IP Stack Selection:	Dual T										
Config. Protocol:	DHCP V	IPv4	AutoConfig Only	•		IPv6					
IP Address:	192.168.0.253										
Subnet Mask:	255.255.255.0										
Gateway:	192.168.0.1										
If Domain Names ar	e to be used, eitl	her here or on othe	r forms, then t	he IP address of	at least one Don	nain Name Serve	er is required	ı.			
DNS Servers Enabled:	Disabled •										
DNS Server 1 - IP Address:	**]							
DNS Server 2 - IP Address:	5 5 6 7]							
Upgrade Port [69]:	Enabled •										
											Save

System Name

You can specify the system name here. This is normally the Fully Qualified Domain Name (FQDN) of the device, but this is not enforced.

You can retrieve the value specified here by querying the sysName node via SNMP. This allows SNMP management platforms to obtain unique names for units where specified. This value has no effect on network communications, and the unit will function correctly with or without a value.

System Location

You can specify the system location here.

You can retrieve the value specified here by querying the 'sysLocation' node via SNMP. This allows SNMP management platforms to obtain location names for units where specified. This value has no effect on network communications, and the unit will function correctly with or without a value.

Contact Name

You can retrieve the unit support contact name by querying the 'sysContact' node via SNMP. This value has no effect on network communications and the unit will function correctly with or without a value.

IP Address

You can enter a standard IP address here. The address is entered in decimal format (for example: 192.168.0.44 or 22.10.45.33). The address entered here will be the address by which the Gateway unit is accessed and managed.

Subnet Mask

The subnet mask is used to determine what part of the IP address is the network portion and what part is the host portion.

It is often 255.255.0.0 or 255.255.255.0. The correct setting is essential for correct operation.

The subnet mask is entered in decimal format (for example: 255.255.255.0 or 255.255.224.0).

Gateway

The Gateway setting specifies the IP address of the machine/router that the Gateway unit uses to communicate with different networks.

The Gateway address is entered in decimal format (for example: 192.168.0.1 or 11.2.24.103).

Most networks will have a Gateway. Correct setting is important for correct network communications.

Config. Protocol

Select the configuration protocol. Choices include:

- Static
- DHCP
- BootP

Note: Once you enter the IP Configuration options and click **Save**, the changes take effect. If incorrect entries are made, this may result in loss of communication. If this happens, reset the Gateway unit's network configuration. Details of how to do this can be found in the Troubleshooting section.

Setup - HTTP or HTTPS

Select the access method for the Web Management Interface here. Both HTTP and HTTPS access modes are available by default. Selecting the HTTPS radio button will allow only HTTPS configuration.

Pandu	IT				Logged In: admin (System Name:	Administrator) SAP SZ Cabinet Logout
		Setup	Input Sensors	Outputs	Access Control	Power
Overview	tup / HTTP					
Overview IP Config HTTP Certificates SNMP Rec'rs Users HT Email Alerts Time Setting Syslog Servers Events Preferences Restart	cess method for the web management interface is selected here. TP and HTTPS - Accessible by either HTTP or HTTPS TPS Only - Accessible by HTTPS only, recommended for security TP Port: 100 TPS Port: 443 HTTP and HTTPS HTTPS Only					
нт	TP Strict Transport Security (HSTS) [Help]					
() () () () () () () () () () () () () (HSTS: Disabled HSTS: Enabled STS Max Age (Seconds): 15724800 HSTS: Do not Include SubDomains					
	HSTS: Include SubDomains					
нт	TP Public Key Pinning (HPKP) [<u>Help</u>]					
® Ma Pri Ba ®	HPKP: Disabled HPKP: Enabled IX Age (Seconds): 5184000 Imary Hash (SHA256 - base64 encoded): ckup Hash (SHA256 - base64 encoded): HPKP: Do not Include SubDomains HPKP: Include SubDomains					
						Save

Use of HTTPS is recommended for security, because the connections will be encrypted.

Additionally, you can specify the TCP port for connection to the Web Management Interface here. If you have specific requirements for default ports, these can be left at their default settings (for example, port 80 for HTTP and port 443 for HTTPS). **Note**: Changing the selection to HTTP or HTTPS requires a reboot for the selection to take effect.

Setup – LDAP Servers

Lightweight Directory Access Protocol (LDAP) configuration options are specified here.

Pand	UIT						Logged In: admin System Name: s	(Administrator) sysName Logout			
				Setup	Input Sensors	Outputs	Access Control	Power			
Overview	Setup / LDAP Server	'5									
IP Config HTTP	Enabled:	Disabled •									
SNMP NMS	Credential Cache:	10 Minutes (Timeout)									
SNMP Rec'rs	Primary LDAP Server										
Modbus Users	Display Name:	LDAP_Server_1									
Email Alerts	IP Address:	0.0.0									
Syslog Servers	Unit Base DN:										
Events	Users Base DN 1:										
Restart	Users Base DN 2:										
	Facandami I DAD Far										
	Dicplay Namo:	DAR Server 2									
	ID Address:										
	Unit Base DN:										
	Users Base DN 1:										
	Users Base DN 2:										
	oscis base bit Li										
								Save			

Configuration options for a Primary and Secondary server are provided with identical configuration choices.

Enabled/Disabled

If you select Disabled, no LDAP servers will be queried to verify user login credentials' access and privileges. Only internal users will be able to log in.

Credential Cache

This configuration option specifies how long (in minutes) users successfully authenticated via LDAP will be allowed to access the unit without re-authenticating against LDAP.

Primary/Secondary LDAP Server

- If you specify only the Primary LDAP Server, only the primary server will be queried to verify user login credentials' access and privileges.
- If you specify only the Secondary LDAP Server, only the secondary server will be queried to verify user login credentials' access and privileges.

 If you specify both the Primary and Secondary LDAP Servers, both servers will be queried (with priority given to the Primary) to verify user login credentials' access and privileges.

Display Name

You can create a display name for the specified LDAP server here. The Display Name is for reference and logging purposes and has no direct effect on LDAP functionality.

IP Address

Specify the IP address of the LDAP server here.

Unit Base DN

You must provide the Distinguished Name (DN) of the directory object containing the SmartZone Gateway LDAP authentication structure here. This field is required for LDAP function.

See LDAP for configuration details.

Users Base DN 1

Provide the Distinguished Name (DN) of the directory object containing directory users for authentication here. This field is required for LDAP function.

See LDAP for configuration details.

Users Base DN 2

You can specify the Distinguished Name (DN) of the directory object containing directory users for authentication here. This field is optional for LDAP function when Users Base DN 1 has been specified.

Setup - SNMP NMS

Specify the IP address, community string, and access permissions for up to five Network Management Stations here.

Any machine that needs to access the unit's SNMP functions must be entered here.

5	UIT								Logged In: admin (System Name:	Administrator) SAP SZ Cabinet Logout			
						Setup	Input Sensors	Outputs	Access Control	Power			
iew	Setup / SNMP (Netw	ork Management Statio	ns)										
nfig P cates	SNMP access creden	tials are configured here	e. The device supp	ports both SNMPv2c access	s (using Community Strings)	and SNMPv3 ac	ccess (using USM Use	rs).					
IMS ec'rs	Select the SNMP ver	sion you wish to config	ure:		SNMPv2c ¥								
rts ngs vers	Community string an Read Only access pe Read / Write access Note: To disable SNI	ommunity string and access permissions are specified here for the Network Management Stations. ead Only access permits an NMS using the specified community string to use only GET commands. ead / Write access permits an NMS using the specified community string to use both GET and SET commands. lote: To disable SNMPV2 clear all community strings.											
		Community String:	NMS Access:										
rt	NMS 1	public	Read Only 🔻										
	NMS 2	private	Read / Write 🔻										
	NMS 3		Read Only 🔻										
	NMS 4		Read Only •										
	NMS 5		Read Only 🔻										
										Save			

NMS IP Address

Enter the IP address of the NMS machine here.

Community String

You must enter the required community string here. The default for many devices is **public**. It is recommended that the community string be changed, because it serves as an access password.

NMS Access

Read-only access permits the NMS to use only GET commands. Read/Write access permits the NMS to use both GET and SET commands.

Setup - SNMP Receivers

Specify the IP address, community string, and access permissions for up to 10 Network Management Stations here.

PANI	лит						Logged In: adm System Nam	n (Administrator) ne: SAP SZ Cabinet Logout	
				Setup	Input Sensors	Outputs	Access Control	Power	
Overview	Setup / SNMP (Receivers)								
IP Config HTTP Certificates SNMP NMS SNMP Rec'rs Users Email Alerts Time Settings	SNMP Trap Receivers are configured her Any machine which will be required to tr Notes: Authentication failure traps, when enabl v3 Traps are sent in a sunpv2-trap form All Traps are generated to port 162.	e. aceive SNMP traps sent from this unit must be er led, are generated if an attempt is made to acces at contained within a SNMPv3 message. Authent	itered here. s the unit with an invalid cor ication or Encryption is not s	mmunity strin supported.	g.				
Syslog Servers	5	Receiver IP Address:		Receive 1	raps:	т	rap Version:		
Events Preferences	Receiver 1	10.64.69.101		Enabled	•	V	2c 🔻		
Restart	Receiver 2	10.136.202.90		Enabled	•	N	2c •		
	Receiver 3			Disabled	•		1 •		
	Receiver 4			Disabled	•		1 •		
	Receiver 5			Disabled	•		1 •		
	Receiver 7			Disabled	•		1 1		
	Receiver 8			Disabled	•		1 •		
	Receiver 9			Disabled	•	N	1 •		
	Receiver 10			Disabled	•	V	1 •		
								Test All Save	

Receiver IP Address

You must enter any machine that is required to receive SNMP traps sent from this unit. Usually any SNMP NMS entries should also be entered.

Community String

The required community string must be entered here. The default for many devices is **public**. The community string should be changed, because it serves as an access password.

Receive Traps

The Receive Traps **Enabled** setting allows the specified NMS to receive the unit's standard range of traps. Receive Traps **Enabled** (incl Auth fails) will cause the unit to issue traps if an unauthorized IP address attempts to access the unit's SNMP functions.
Receive Traps **Disabled** prevents traps from being sent to the specified NMS IP address.

Trap Version

Setup - Modbus

You can enable a Modbus communications protocol, specify the Modbus port number, and enable relays control at this window.

- An t	UIT					Logged In: admin Syste	(Administrator) em Name: Eagle-i Logout
			Setup	Input Sensors	Outputs	Access Control	Power
Overview	Setup / Modbus						
IP Config HTTP I DAP Servers	Enabled:						
SNMP NMS	Modbus port:	502					
SNMP Rec'rs Modbus Users Email Alerts Time Settings Syslog Servers Events Preferences Restart	Enable Relays control:						
							Save

Setup - Users

You can add users with permission to access the Web Management Interface here. Access passwords are also specified along with users' access permissions.

							System Name	SAP SZ Cal
				Setup	Input Sensors	Outputs	Access Control	Power
Setup / Users								
Administrator: Controller and	Configuration settings can be Viewer: Configuration settings	viewed and modified. s can only be viewed.						
	Username:	Password:	Level:					
User 1	admin		Administrator •					
User 2	szadmin		Administrator •					
User 3	support		Viewer •					
User 4			Administrator •					
User 5			Administrator •					
User 6			Administrator *					
User 7			Administrator T					
User 8			Administrator 🔻					
User 9			Administrator *					
User 10			Administrator 🔻					
User 11			Administrator 🔻					
User 12			Administrator T					
User 13			Administrator •					
User 14			Administrator 🔻					
User 15			Administrator •					
User 16			Administrator 🔻					
User 17			Administrator •					
			Administrator •					
User 18			Administrator V					
User 18 User 19			, torning a con					

Username

Enter the required username. This is the username that will be required to login to the Web Management Interface.

Password

Enter access passwords on a per-user basis.

Level

Three user levels are available for assignment.

• **Administrator** : Administrators have full control of SmartZone Gateway configuration settings.

- Controller : Controllers can view configuration settings.
- Viewer : Viewers can view configuration settings.

Warning: User 1 / admin is the master administrator. It is possible to remove administrator rights from the admin user. Doing this is not recommended as it may result in no one having administrator access. In this situation, a reset to factory defaults is the only solution. Details on how to do this can be found in the Troubleshooting section.

Setup - Email Alerts

On this page, you can edit email alert settings for traps. You may set up to 10 email receivers.

PAND		Т								Logged In: admin System Name	(Administrator) : SAP SZ Cabinet Logout
							Setup	Input Sensors	Outputs	Access Control	Power
Overview	Setu	p / Email Alerts									
IP Config	SMT	P Relay Server:									
нттр	From	n Address:									
Certificates	Rep	v-To Address:			_						
SNMP NMS	E-mail										
Users	Emai	Receivers									
Email Alerts	No.	Destination Ad	dress	Enabled	Repeat '	Timer					
Time Settings	1				0	mins.					
Events	2				0	mins.					
Preferences	3			1	0	mins.					
Restart	4				0	mine					
	2				0						
	5				U	mins.					
	6				0	mins.					
	7				0	mins.					
	8				0	mins.					
	9				0	mins.					
	10			i 🛛	0	mins.					
					-						
											Test All Save

Email Alerts							
SMTP Relay Server	The IP Address of the SMTP Server						
From Address	Address from which the alert emails are sent						
Reply-To Address	Address to which the email receivers can reply						

Email Alerts						
Destination Address	Address that will receive the email alerts					
Enabled	Toggle the check box to enable or disable alerts to each address					
Repeat Timer	Number of minutes after which the email alert will repeat					

Setup - Events

The **Events** page shows a history of events that have occurred, along with specific details about each event.

AVD.	UIT							Logged In: admin System Name	a (Administrator a: SAP SZ Cabin Logo) et ut
					Setup	Input Sensors	Outputs	Access Control	Power	
arview	View / Events									
Config ITTP	View Events: 2	017 • November • ® Latest I	First 🔍 Earliest Firs	t [Show]					[<prev] [ne:<="" th=""><th><u>(t>1</u></th></prev]>	<u>(t>1</u>
IP NMS	Date / Time	Туре	User	Event Data						
Alerts Alerts ettings Servers nts rences tart	Nov 20 06:12:4 Nov 20 06:07:3 Nov 20 06:05:2 Nov 20 05:52:4 Nov 20 05:40:2 Nov 20 05:40:2 Nov 20 05:40:2 Nov 20 05:40:2 Nov 20 05:40:2 Nov 20 05:16:2 Nov 20 05:16:2 Nov 17 12:44:4 Nov 17 11:14:4 Nov 17 11:14:4 Nov 17 11:14:4 Nov 17 11:167:5 Nov 17 04:46:2 Nov 17 04:46:4	Auto Logout. Viser Login. Auto Logout. Viser Login. Auto Logout. User Login. Auto Logout. User Login. S Auto Logout. User Login. S Auto Logout. User Login. Viser Login. S User Login. S User Login. S User Login. Suscr Login.	User: admin User: System User: System 2 Ser: System	Watchdog Pin Id: 5, Name: , Pin code: , Expiry Time 0 Relay Id: 6, Current State: Not Active						
	Nov 15 12:12:1	5 Change State or Control of Relay	/. User:System	Relay Id: 5, Current State: Not Active						

To specify a range of events to view, select the desired year and month from the dropdown menus, then click **Show**.

Date/Time, Type, User, and Event Data for each event are displayed.

Events can be ordered **Latest First** or **Earliest First** by clicking the corresponding radio button.

Setup - Syslog Servers

This page allows you to view or edit information about the Syslog Servers currently being used.

MDUI.									Logged In: admin System Name:	(Administrator) SAP SZ Cabinet Logout
						Setup	Input Sensors	Outputs	Access Control	Power
Setup	o / Syslog Serve	ers								
onfig FTP Enab ficates	led:	Disabled •								
P NMS	ary Syslog Serv	er								
ers Disp	lav Name:									
Alerts	dress:	0000								
Servers Port		514								
ents rences start		5.14								
Log	Event Types:	System	Network	Input Config	Logging					
-		Service	Relay Config	Access Control	Power Strip					
Seco	ndary Syslog Se	rver								
Disp	lay Name:									
IP A	ddress:	0.0.0.0								
Port		514								
Log	Event Types:	System	Network	Input Config	Logging					
		Service	Relay Config	Access Control	Power Strip					
										Save

From the Enabled drop-down menu, you can choose which syslog servers are enabled. Fill in the following fields for each Syslog server.

Syslog Server Setup						
Display Name The name of the Syslog server						
IP Address	The IP address of the Syslog server					
Port	The number of the port being used					
Log Event Types	Click the check boxes to choose which events to log					

Setup - Time Settings

The **Time Settings** page allows you to view or edit the current date and time.

PAND	TIUIT						Logged In: admin System Name:	(Administrator) SAP SZ Cabinet Logout
				Setup	Input Sensors	Outputs	Access Control	Power
Overview	Setup / Time Settin	gs						
IP Config	Deter	20 • Nevember • 2017 •						
Certificates	Date:							
SNMP NMS SNMP Rec'rs	Local fille.							
Users Email Alerts	Time Adjustments							
Time Settings	Timezone:	(GMT-06:00) Central Time •						
Events	Daylight Saving:	✓ Enabled						
Preferences Restart		Start the 4th V Sunday in March V						
	D-1-51	Stop the 4th V Sunday in October V						
	Date Format:	dd/mm/yyyy 🔻						
	SNTP Servers							
	Primary Server:		Enabled					
	Secondary Server:		Enabled					
	NTP Update Freq.:	1 Hours						
								Save

Select the correct day, month, and year from the dropdown menus, and verify the local time. If you want to change the time, you must check the Update time checkbox.

Time Adjustments

Select the correct time zone from the drop-down menu.

- **Daylight Saving** can be enabled or disabled by clicking the check box. If Daylight Saving is enabled, select start/stop dates from the subsequent drop-down menus.
- Date Format allows the administrator to choose whether the date is displayed with the day or month first. For example, the date August 20, 2013 can be displayed in one of two ways:

20/08/2013 (DD / MM / YYYY) or 08/20/2013 (MM / DD / YYYY)

Select the desired format from the dropdown menu.

• SNTP Servers - Simple Network Time Protocol synchronizes the clocks of computer systems over a network. Enter the IP address of an SNTP server, and specify (in hours) how often the time should be updated.

Setup - Preferences

The Preferences page allows you to edit system preferences.

AND	UIT						Logged In: admin (A System Name: S	dministrator) AP SZ Cabinet Logout
				Setup	Input Sensors	Outputs	Access Control	Power
verview Config HTTP HTTP tiffcates MP NMS USers all Alerts s Settings s Settings settings estart	Setup / Preferences Default Page: Timestamp Traps: User Session Timeout: Temperature Scale: Page Refresh Period: Browser Autocomplete:	Setup -> Overview None • 5 Minutes Fahrenheit • 10 Seconds (0 for no ref Disabled •	v resh)					
								Save

Preferences							
Default Page	From the dropdown menu, select the first page you want to open when a user logs in. The preset default page is the Overview page.						
Time stamp Traps	Choose from the dropdown menu where the timestamp will be found on traps. There are three options:						
	Prefix – timestamp at the beginning						

	Preferences							
	 Append – timestamp at the end None – no timestamp 							
User Session Timeout	Enter a number of minutes, after which a session will be timed out if the user is inactive.							
Temperature Scale	Select Celsius, Fahrenheit, or Kelvin from the drop-down menu.							
Page Refresh Period	Enter a number of seconds, after which the page will auto mat- ically refresh. If 0 is entered, the page will not refresh auto- matically.							
Browser Auto- complete	Choose Disabled or Enabled from the drop-down menu to auto- mate an autocomplete browser.							

Setup – Restart

A unit may be rebooted or reset to factory defaults here.

Restart Unit

Restart Now

Selecting **Restart Now** commands the unit to reboot. Rebooting the unit will cause any outstanding configuration changes to take effect.

Reset to Factory Defaults

See Troubleshooting for instructions on resetting the factory default settings for the unit.

Input Sensors – Configuration and Status

Status

The Input Sensors status page presents an overview of the input ports. This page displays the input channel number, name, type of input sensor, status, current readings, and thresholds.

	IIT						Logged Ir	n: admin (Adı System Narr	ministrator) ne: EBC Live Logout
				Setup	Input Sensors (Outputs	Access Con	itrol F	ower
Inj	put Sensors / Status								
s Inf	formation from connected input sensors	is presented here.						Pre	v Next
							Lir	mits	
	Channel	Туре	Detected	Status	Value	UC	uw	LW	LC
~	13: F Temp Top	Auto Detect	Temperature	Enabled	72.9 °F	89.6	82.4	64.4	59.0
Image: A start a st	14: F Temp Mid	Auto Detect	Temperature	Enabled	71.9 °F	89.6	82.4	64.4	59.0
✓	15: F Temp Bot	Auto Detect	Temperature	Enabled	72.4 °F	89.6	82.4	64.4	59.0
✓	16: F Humidity	Auto Detect	Humidity	Enabled	22.9 % RH	65.0	60.0	20.0	10.0
✓	17: F Door	Contact	Contact	Enabled	Closed	N/A	N/A	N/A	N/A
Image: A start of the start	18: F Door-Lock	Auto Detect	Contact	Enabled	Closed	N/A	N/A	N/A	N/A
✓	19: F Door-Handle	Auto Detect	Contact	Enabled	Closed	N/A	N/A	N/A	N/A
	20: Not-Used	Disabled	Temperature	Disabled	N/A	N/A	N/A	N/A	N/A
✓	21: R Temp	Auto Detect	Temperature	Enabled	76.8 °F	89.6	82.4	64.4	59.0
	22: Not-Used	Disabled	Temperature	Disabled	N/A	N/A	N/A	N/A	N/A
	23: Not-Used	Disabled	None	Disabled	N/A	N/A	N/A	N/A	N/A
	24: R Door	Auto Detect	Contact	Enabled	Closed	N/A	N/A	N/A	N/A

	UIT						Logged In	n: admin (Ad System Nar	lministrator) ne: EBC Live Logout
				Setup	Input Sensors	Outputs	Access Con	trol I	Power
1	Input Sensors / Status								
status efaults nfigure ogue Trap	Information from connected input sensors is pr	resented here.						Pre	ev Next
CAL							Lin	nits	
	Channel	Туре	Detected	Status	Value	UC	uw	LW	LC
	 25: R Door Lock 	Auto Detect	Contact	Enabled	Closed	N/A	N/A	N/A	N/A
	26: R Door Handle	Auto Detect	Contact	Enabled	Closed	N/A	N/A	N/A	N/A

Status Indicators

Three status indicators are displayed next to input channels to allow quick determination of normal, warning, and critical alarm statuses:

>	Channel reading currently within threshold limits.
<u> </u>	Upper or lower Warning limit reached or exceeded.
8	Upper or lower Critical limit reached or exceeded.

Input Sensors – Defaults

The Input Sensor Defaults menu allows configuration parameters for input sensors of specific types to be defined and applied to all inputs of that type.

The types of input sensors are:

- Temperature
- Humidity
- Analog (Voltage)
- Open/Close Contacts (digital inputs)

The configurable defaults are described below.

Calibration Offset

The value entered here alters the actual reading of a sensor by the amount specified.

For example, if a Calibration offset of 6 was used and a sensor's true reading was 36, the indicated reading used for display and alarm purposes would be 42. This works the same way for both temperature and humidity sensors.

Hysteresis Value

The hysteresis default value to be applied to sensors is specified here. The value specified is an offset from a sensor's threshold values.

For example, a hysteresis value of 5 would mean that, in the case of an Upper Control Limits alarm, the alarm value would have to reduce to 5 below the threshold value before another alarm is issued.

Please see Appendix B: Hysteresis Demystified for detailed information.

Limits and Traps

You can set default values for sensor alarm thresholds here. You also can set the default settings for alarm threshold traps here.

The following thresholds can be set:

- Upper Control Limit
- Upper Warning Limit
- Lower Control Limit
- Lower Warning Limit

You can apply default trap settings for all of these thresholds. With the trap box deselected, no SNMP alarm traps will be generated, even when an alarm condition exists for that threshold.

Repeat Timer

The repeat timer causes alarm traps to be reissued after a specified amount of time if the alarm condition persists.

Setting the repeat timer to zero will disable the repeat traps.

The defaults that can be set for Open/Close contacts differ from the Temperature and Humidity settings.

Normal State

Normal state specifies the condition in which a contact is considered to be in a Normal, Non-alarmed state.

Devices such as smoke alarms and air conditioning units often have normally open contacts. To receive alarm indications from these types of units would cause alarms to be issued when a monitored contact closes.

Setting normally closed in the case of a rack or cabinet door would cause an alarm condition when the door was opened.

Trigger Type

The trigger type defaults for Open/Close sensors are specified here.

The three available options for trigger types are:

Level

Level triggering is the default mode. When an input physically transitions from a Normal to Non-Normal state, an alarm is triggered. However, the alarm persists only while the

input remains in a Non-Normal state. When the input returns to a normal state, the alarm is cleared.

Normal to Non-Normal (Positive Edge)

This type of triggering may be used in situations where a momentary type input (for example, a shock sensor or PIR) is used. Since these types of inputs are momentary, any alarm condition that occurs will persist until manually cleared.

Positive Edge triggering is used when an alarm is required to persist after an input changes from the Normal state to the Non-Normal state.

Non-Normal to Normal (Negative Edge)

This type of triggering may be used in situations where a momentary type input (for example, a shock sensor or PIR) is used. Since these types of inputs are momentary, any alarm condition that occurs will persist until manually cleared.

Negative Edge triggering is used when an alarm is required to persist after an input changes from the Non-Normal to the Normal state.

Input Sensors - Configure

You can configure the individual sensor channels in this window.

					Setup	Outpute	Accoss	Control	Rowor
In	nut Sensors / Status				Setup Input Sensors	outputs	Access	control	Fower
,									
									Prev Ne
Int	formation from connected input se	ensors is presented here.							
								Limits	
	Channel	Туре	Detected	Status	Value	UC	uw	LW	LC
~	13: F Temp Top	Auto Detect	Temperature	Enabled	71.5 °F	89.6	82.4	64.4	59.0
1	14: F Temp Mid	Auto Detect	Temperature	Enabled	69.0 °F	89.6	82.4	64.4	59.0
✓	15: F Temp Bot	Auto Detect	Temperature	Enabled	69.1 °F	89.6	82.4	64.4	59.0
✓	16: F Humidity	Auto Detect	Humidity	Enabled	25.9 % RH	65.0	60.0	20.0	10.0
Δ	17: F Door	Contact	Contact	Enabled	Open	N/A	N/A	N/A	N/A
<	18: F Door-Lock	Auto Detect	Contact	Enabled	Closed	N/A	N/A	N/A	N/A
<	19: F Door-Handle	Auto Detect	Contact	Enabled	Closed	N/A	N/A	N/A	N/A
	20: Not-Used	Disabled	Temperature	Disabled	N/A	N/A	N/A	N/A	N/A
<	21: R Temp	Auto Detect	Temperature	Enabled	70.4 °F	89.6	82.4	64.4	59.0
	22: Not-Used	Disabled	Temperature	Disabled	N/A	N/A	N/A	N/A	N/A
	23: Not-Used	Disabled	None	Disabled	N/A	N/A	N/A	N/A	N/A
\checkmark	24: R Door	Auto Detect	Contact	Enabled	Closed	N/A	N/A	N/A	N/A

Pandu	ШΤ						Logged In Syste	: admin (Adr m Name: SAP	ninistrator) SZ Cabinet Logout
				Setup	Input Sensors	Outputs	Access Cor	itrol I	Power
In	put Sensors / Status								
Status Defaults Configure In Analogue Trap Text	formation from connected input sensors is pr	esented here.						Pre	v Next
							Lir	nits	
	Channel	Туре	Detected	Status	Value	UC	uw	LW	LC
✓	25: R Door Lock	Auto Detect	Contact	Enabled	Closed	N/A	N/A	N/A	N/A
✓	26: R Door Handle	Auto Detect	Contact	Enabled	Closed	N/A	N/A	N/A	N/A

Select the **Config** option to open a detailed configuration page for the selected sensor.

The difference between the menus presented here and the menus presented on the Defaults page is that settings are applied to individual channels.

The submenus contain all the options in the Defaults menu, plus two additional options:

Name

Sensor channels can be assigned names for ease of identification (for example, "Server Room Sensor" or "UPS Battery Fail").

Туре

The type of connected sensor is specified here. The sensor channels can be set to auto detect, temperature, humidity, contact, or disabled.

Note: Occasionally, clear traps will be sent to the NMS trap receivers while a sensor is being connected to a device. This is considered normal behavior, because some voltage surges may be produced when input sensors are physically connected to the gateway. In normal operation, the sensors will always be connected to the device and the sensor voltages will stay within normal expected values

Outputs – Status

The Outputs Status page provides an overview and direct control of the EPA126 unit's four output relays.

ANDUIT						Logged In: admin (Administ System Name: SAP SZ C I	rator) abinet .ogout
			:	Setup Input Senso	rs Outputs	Access Control Powe	r
Outputs / Status							
Information from outputs	is presented here.						
Output	Normal State	Logic Controlled	Current State		CON	ITROL	
1: Output_01	Not Active	-	Not Active	[Activate]	[DeActivate]	[Use Logic]	
2: Output_2	Not Active	-	Not Active	[Activate]	[DeActivate]	[Use Logic]	
3: Output_3	Not Active	-	Not Active	[Activate]	[DeActivate]	[Use Logic]	
4: Output_4	Not Active	-	Not Active	[Activate]	[DeActivate]	[Use Logic]	
5: Front Door	Not Active	YES	Not Active	[Activate]	[DeActivate]	[Use Logic]	
6: Rear Door	Not Active	YES	Not Active	[Activate]	[DeActivate]	[Use Logic]	
7: Output_7 (L)	Not Active	-	Not Active	[Activate]	[DeActivate]	[Use Logic]	
8: Output_8 (L)	Not Active	-	Not Active	Activate	DeActivate	Use Logic	
9: Output_9 (L)	Not Active	-	Not Active	Activate	DeActivate	Use Logici	
10: Output_10 (L)	Not Active	-	Not Active	[Activate]	[DeActivate]	<u>[Use Logic]</u>	
12: Output_12 (L)	Not Active	-	Not Active	[Activate]	[DeActivate]		
12: Output_12 (L)	Not Active	-	Not Active	[Activate]	[DeActivate]		
14: Output_14 (L)	Not Active		Not Active	[Activate]	[DeActivate]	[Use Logic]	
15: Output_15(L)	Not Active	_	Not Active	[Activate]	[DeActivate]	[Use Logic]	
15: Output_15 (L)	Not Active	-	Not Active	[Activate]	[DeActivate]	[Use Logic]	
17: Output_17(L)	Not Active	-	Not Active	[Activate]	[DeActivate]	[Use Logic]	
18: Output 18 (L)	Not Active	-	Not Active	[Activate]	[DeActivate]	[Use Logic]	
L = logical channel only, no p	hysical device present						

Control

- Activate: Commands the selected relay to energize.
- Deactivate: Commands the selected relay to de-energize.
- Use Logic: Commands the selected relay to enter logic-controlled mode. In logiccontrolled mode, the activation and deactivation is governed by any configured and enabled logic.

Outputs – Configure

Outputs / Cor	nfigure					
			SNMP	Traps		Logic
Output	Name	Normal State	Trap Alarm Level	Repeat Timer (Seconds)	Controlled	Configur
1	Output_01	Not Active V	Disabled •	0		Config 1
2	Output_2	Not Active 🔻	Disabled •	0		Config 2
3	Output_3	Not Active •	Disabled 🔻	0		Config 3
4	Output_4	Not Active *	Disabled •	0		Config 4
5	Front Door	Not Active 🔻	Information •	0	4	Config 5
6	Rear Door	Not Active *	Information •	0	•	Config 6
7 (L)	Output_7	Not Active V	Disabled •	0		Config 7
8 (L)	Output_8	Not Active 🔻	Disabled •	0		Config 8
9 (L)	Output_9	Not Active	Disabled •	0		Config 9
10 (L)	Output_10	Not Active V	Disabled •	0		Config 10
11 (L)	Output_11	Not Active V	Disabled •	0		Config 11
12 (L)	Output_12	Not Active •	Disabled •	0		Config 12
13 (L)	Output_13	Not Active V	Disabled •	0		Config 13
14 (L)	Output_14	Not Active •	Disabled •	0		Config 14
15 (L)	Output_15	Not Active V	Disabled •	0		Config 15
16 (L)	Output_16	Not Active •	Disabled •	0		Config 16
17 (L)	Output_17	Not Active V	Disabled •	0		Config 17
18 (L)	Output_18	Not Active	Disabled •	0		Config 18

Relay and logic configuration is performed via two pages.

- Name: The relay output name is specified here. (for example, Fan_Tray or Door_ 1).
- Normal State: Normal State specifies the 'normal' or 'non-alarm' state of a relay.
 - Not Active: Specifies that a output relay in a 'Not Active' ('not-energized) state is normal.
 - Active: Specifies that an output relay in an 'Active' ('Energized) state is normal.
- **Trap Alarm Enabled**: Toggles alarm trap generation. An alarm trap will be generated when the relay is in an alarm state with this enabled.
- **Repeat Timer (Seconds)**: Specifies an interval in which a trap for an *existing* alarm condition will be regenerated. This will be a duplicate of the original trap. A repeat timer is not necessary in NMS systems employing intelligent trap handling. Setting zero (0) disables repeat traps.
- **Controlled**: This toggle acts as a master control to any logic configured for a relay. When selected **Use Logic** may be enabled on the Status page.

It is only possible to select this option if logic has been specified in the **Relay**

Specific Configuration page.

• **Configure**: Click on the **Config** link for the desired output to open the Outputs - Configure - Config window.

Outputs - Configure - Config

Actual Digital Output Relay logic configurations are specified here.

Panduit						Log	ged In: adm	n (Administrator) System Name: a Logout
			Setup	Input Senso	rs Out	puts Access	Control	Power Strips
Outputs	/ Define Logic Control : Ou	itput 1 [Output_1]						
Status Configure	Enskie] Invert Enskie] Invert	Logic Operator:	Delay 0 Delay 0	Timer - ON: Seconds	-Invert	P-		
Normal Normal	Trap Text:		Ĩ	Ion-Normal Tra Non-Normal 1	o Text:		Logged In Syster	Back Save : admin (Administrator) n Name: SAP SZ Cabinet Logout
Outputs / Confi	qure			Setup	Input Se	nsors Outputs	Access Con	trol Power
Status	-				_			
comgure				SNMI	P Traps Repeat		Logic	
Output	Name	Normal State		Trap Alarm Level	Timer (Seconds)	Controlled		Configure
1 2 3 4 5 6 7 (L) 8 (L) 9 (L) 10 (L) 11 (L) 12 (L) 13 (L) 14 (L) 15 (L) 16 (L) 17 (L) 18 (L) L = logical chann	Output_01 Output_2 Output_3 Output_4 Front Door Rear Door Output_7 Output_8 Output_9 Output_10 Output_12 Output_13 Output_15 Output_16 Output_188	Not Active • Not Active •		Disabled • Disabled • Disabled • Information • Disabled •				Config 1.2 Config 3.2 Config 3.2 Config 3.2 Config 5.2 Config 6.2 Config 7.2 Config 9.2 Config 10.2 Config 11.2 Config 12.2 Config 13.2 Config 15.2 Config 15.2 Config 15.2 Config 15.2 Config 16.2 Config 17.2 Config 18.2

Input Selection

Select Inputs into the logic on the left hand side by clicking one of the **Click to Enable** boxes.

Here you can choose a sensor type, sub-type, and name to feed into logic.

Invert

The Invert check box allows the logic inversion of an input into the logic. For example, when an upper warning limit is breached, the following input logic is used.

	No Invert	Invert
Threshold breached	1 (Logic Triggering)	0 (Not Logic Triggering)
Threshold within limit	0 (Not Logic Triggering)	1 (Logic Triggering)

Logic Operator

The Logic Operator provides options that control the evaluation of inputs to logic.

Logical AND Inputs

Logical AND requires **ALL** of the selected inputs to the logic to be in a triggering state to activate the relay logic.

Logical OR Inputs

Logical OR requires only ONE of the selected inputs to be in a triggering state to activate the relay logic.

Delay Timer On

Delay Timer On specifies the time in seconds that must elapse before the logic activates in a situation where it would otherwise activate immediately.

This is useful in a situation where you want a delay to be added before a logic controlled relay is switched on.

If the logic triggering condition clears before the specified time has elapsed then the logic will not activate at all.

Delay Timer Off

Delay Timer Off specifies the time in seconds which must elapse before the logic deactivates in a situation where it would otherwise deactivate immediately.

This is useful in a situation where you want a delay to be added before a logic controlled relay is switched off from a current on state. If the logic triggering condition returns before the specified time has elapsed then the logic will not deactivate at all.

Final Invert

A final invert check box is provided. This allows the final output logical state to the relay to be inverted.

Any conditions that produce a relay on output will produce the reverse.

Access Control – Configure

Configure keypad devices physically attached to the unit at this screen.

PAND	UIT									Logged In: admin System Name:	(Administrator) SAP SZ Cabinet Logout
							Setup	Input Sensors	Outputs	Access Control	Power
Configure	Access Control	/ Configure									
Access Codes							Timeouts (Secs)				
Override	ACU	Туре		Name		Door Latch	Return to Standby	ACL	I in Use Trap Ala	rm Level	
	1: ACU1	2 x 5 🔹		Front Door		20	0	Info	rmation •		
	2: ACU2	Disabled *		Rear Door		20	0	Info	rmation *		
	Assass Code La	nath F T									
	Access Code Le	ingin. 5 T									
	Hide PIN Code:										
	In-Use Trap Te	xt: in use									
	-Remote Auther	ntication Server									
	Enable:										
	IP Address:		0.0.0.0								
	Port No.:		0	A T-+ BAG G	1						
			Sav	e & lest RAS Connecti	ity						
											Cu
											Save

ACU

ACU KP1 and KP2 refer to the two physical keypad connection ports found on the rear of the EPA126 unit.

Туре

Two types of supplied keypads are supported by the EPA126 unit: 2x5 and 3x4.

Name

A keypad name can be specified here for alarm logging and notification reasons. Front_ Door or Rear_Door are common choices.

Timeouts - Door Latch

Since the most common use of the keypad is to activate a solenoid to provide rack access, a door latch timer is provided. The time in seconds specified here controls how long a valid keypad entry will provide a positive input to relay logic. In most situations, this controls how long a door solenoid remains activated after a valid keypad code is entered.

Timeouts – Return to Standby

This parameter specifies the time in seconds that must elapse before the keypad returns to standby after an incomplete code is entered.

ACU In Use Trap

Selecting this option causes a keypad-in-use trap to be produced when any button is pressed on the keypad. This trap will be produced regardless of the entered code's valid-ity.

Access Code Length

An Access Code Length of between 1 and 15 digits can selected here. This Access Code Length applies to all pin codes defined on the Access Control – Pin Codes screen. Any pin codes that do not match the length specified here will be unusable.

Access Control – Codes

Access Codes are specified and applied to one or both keypads here.

Access Control / Codes Applied To: Control Applied To: Control Applied To: Control Contro Control Contro <t< th=""><th></th><th>т</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>Logged In: adn System Na</th><th>nir me</th></t<>		т								Logged In: adn System Na	nir me
Access Code Applied To: Name Access Code ADI ACU2 Explices From. Rer From. Rer 1: Admin 12345 I Never 2: Access User 2 3579 I Never 2: Teating 98765 I Never 3: Teating 98765 I Never 4: Image: Access User 6 Image: Access User 7 Image: Access User 7 Image: Access User 7 4: Access User 10 Image: Access User 10 Image: Access User 10 Image: Access User 10 Image: Access User 10 1: Access User 15 Image: Access User 10 Image: Access User 10 Image: Access User 10 Image: Access User 10 1: Access User 15 Image: Access User 10 Image: Access User 10 Image: Access							Setup	Input Sensors	Outputs	Access Control	
Anme Access Code ACU1 ACU2 Expines From. Retr Retr Retr 1 Admin 12345 Never 2: Access User 2 13579 Never 3: Tealing 98765 Never 4: Image: Comparison of the com	Acce	ss Control / Codes									
Name Access Code ACU1 ACU2 Expires From Rear Rear 1: Admin 1/2245 Ø Never 2: Access User 2 1/3579 Ø Never 2: Access User 2 1/3579 Ø Never 3: Testing Ø/7655 Ø Never 4:				Applied	To:						
From Rear 1: Admin 12345 I Never 2: Access User 1 13579 I Never 3: Tesling 99765 I Never 4: Image: Second		Name	Access Code	ACU1	ACU2	Expires					
11 Admin 12345 Never 2: Access User 2 13579 Never 3: Testing 98765 Never 4:				Fron	Rear						
2: Access User 2 13579 Never 3: Testing 99765 Never 4:	1:	Admin	12345	v		Never					
31 Testing 98765 Never 4: 5: 6: Access User 6 7: Access User 7 8: Access User 7 9: Access User 7 10: Access User 7 11: Access User 10 12: Access User 11 13: Access User 12 14: Access User 13 15: Access User 14 16: Access User 15 17: Access User 17 16: Access User 18 17: Access User 18 18: Access User 19 19: Access User 19 20: Access User 20	2:	Access User 2	13579			Never					
4:	з:	Testing	98765	1		Never					
5: Access User 6 7: Access User 7 8: Access User 7 9: Access User 7 10: Access User 9 11: Access User 9 12: Access User 10 13: Access User 12 14: Access User 13 15: Access User 16 16: Access User 17 18: Access User 17 19: Access User 18 19: Access User 19 20: Access User 20	4:										
6: Access User 6 7: Access User 7 8: Access User 7 9: Access User 8 0: Access User 9 0: Access User 10 11: Access User 10 12: Access User 12 13: Access User 13 14: Access User 14 15: Access User 16 16: Access User 16 18: Access User 17 19: Access User 18 19: Access User 19 20: Access User 20	5:										
7: Access User 7 8: Access User 8 9: Access User 9 10: Access User 10 11: Access User 10 12: Access User 11 13: Access User 12 14: Access User 13 15: Access User 14 16: Access User 15 16: Access User 16 17: Access User 17 18: Access User 18 19: Access User 19 20: Access User 20	6:	Access User 6									
8: Access User 8 9: Access User 9 10: Access User 10 11: Access User 11 12: Access User 12 13: Access User 13 14: Access User 14 15: Access User 15 16: Access User 16 17: Access User 17 18: Access User 18 19: Access User 19 20: Access User 20	7:	Access User 7									
9: Access User 9 10: Access User 10 11: Access User 11 12: Access User 12 13: Access User 13 14: Access User 14 15: Access User 15 16: Access User 16 17: Access User 17 18: Access User 18 19: Access User 19 20: Access User 20	8:	Access User 8									
10: Access User 10 11: Access User 11 12: Access User 12 13: Access User 13 14: Access User 14 15: Access User 15 16: Access User 16 17: Access User 17 18: Access User 17 19: Access User 19 20: Access User 20	9:	Access User 9									
111 Access User 11 122 Access User 12 131 Access User 13 142 Access User 14 153 Access User 15 164 Access User 16 175 Access User 17 181 Access User 18 192 Access User 19 201 Access User 20	10:	Access User 10									
12: Access User 12 13: Access User 13 14: Access User 14 15: Access User 15 16: Access User 16 17: Access User 17 18: Access User 18 19: Access User 19 20: Access User 20	11:	Access User 11									
13: Access User 13 14: Access User 14 15: Access User 15 16: Access User 16 17: Access User 17 18: Access User 18 19: Access User 19 20: Access User 20	12:	Access User 12									
14: Access User 14 15: Access User 15 16: Access User 16 17: Access User 17 18: Access User 18 19: Access User 19 20: Access User 20	13:	Access User 13									
15: Access User 15 16: Access User 16 17: Access User 17 18: Access User 18 19: Access User 19 20: Access User 20	14:	Access User 14									
16: Access User 16 17: Access User 17 18: Access User 18 19: Access User 19 20: Access User 20	15:	Access User 15									
17: Access User 17 18: Access User 18 19: Access User 19 20: Access User 20	16:	Access User 16									
18: Access User 18 19: Access User 19 20: Access User 20	17:	Access User 17									
19: Access User 79 20: Access User 20	18:	Access User 18									
20: Access User 20	19:	Access User 19									
	20:	Access User 20									
											-

Name

A user or group name can be specified here for association with an Access Code.

Access Code

Pin codes can be entered here. Pin code length can range from 1 to 15 digits.

Regardless of PIN length used here, only Pin codes of the length specified by the **Pin Code Length** setting on the Access Control – Configure page will be usable.

Applied To

The check boxes allow PIN codes to be associated with a given keypad or both.

A PIN Code line must have a check box selected for a given keypad if the code is to be considered valid for that pad.

Access Control – Override

This page allows a valid entry to be sent to a keypad remotely. This function is useful in a situation where it may be necessary to grant access to a rack remotely.

Pandu	П									Logged In: admin (System Name:	Administrator) SAP SZ Cabinet Logout
							Setup	Input Sensors	Outputs	Access Control	Power
Configure	cess Control / Override										
Access Codes Override	cking Override has the sam	ne effect as a va	alid code being rec	eived from an ACU	J. Only Enabled A	ACUs are shown.					
Ac	cess Control Unit	Override									
1:	Front Door	Override									

The Override buttons for each enabled keypad direct a 'valid PIN Code' command without the need to enter one physically at the keypad.

Power – Configuration and Status

Power - Status

The Power -Status page presents an overview of connected SmartZone Rack PDUs. The page displays the PDU channel number, name, voltage, and current thresholds.

PANDUIT	System Name: SAP SZ Cabinet
Setup Input Sensors Output	s Access Control Power
Power / Status	
Status 3-Phase Circuit Desclorer	
o i sokul 3 Thresholds Circuit Name Outlets Volts Amps kVA PF	W Hz kWh
Configure 01-L1 PDU Red N/A ✓ 122 ✓ 0.0 ✓ 0.0 √).0 60.0 🖌 3.2
Control 01-L2 A2 ✓ 120 ✓ 0.0 ✓ 0.0 0.61 ✓).0 🖌 3.1
Gangs 01-L3 A3 ✓ 121 ✓ 0.0 ✓ 0.0 0.00 ✓).0 🗸 0.7
PDU Gang 02-L1 PDU Yellow N/A ✓ 122 ✓ 0.1 ✓ 0.0 0.61 ✓).0 60.0 🖌 19.6
CL-Amp $02-L2$ B2 \checkmark 120 \checkmark 0.1 \checkmark 0.0 0.25 \checkmark).0 🗸 7.7
02-L3 B3 ✓ 120 ✓ 0.0 ✓ 0.0 0.64 ✓).0 🖌 1.8
03 C1 N/A N/A N/A N/A N/A	J/A N/A N/A
04 D1 N/A 🗸 204 🖌 0.0 🗸 0.0 0.00 🗸).0 60.8 🗸 0.0
05 E1 N/A 207 V 0.0 V 0.0 V).0 60.8 🗸 0.0
06 F1 View ↓⊗ 208 ↓⊗ 0.0 ✓ 0.0 0.00 ✓).0 60.8 🗸 2.4
Aggregate ✓ 0.1 ✓ 0.0 ✓).0 38.5

NOTE: When the SmartZone[™] Gateway EPAX18 expansion unit is connected to the EPA126, the 24 PDUs are displayed across four screens, each displaying six PDUs. See EPAX18 Expansion Unit for details.

Status Indicators

Three status indicators are displayed next to PDU channels to allow quick determination of normal, warning, and critical alarm statuses:

>	Channel reading currently within threshold limits.
<u> </u>	Upper or lower Warning limit reached or exceeded.
8	Upper or lower Critical limit reached or exceeded.

Power Strips - Configure

The Power Strips - Configure menu provides the ability to configure individual PDU options. You can configure the two PDU channels individually by selecting the **Config** option next to each channel.

A summary of several current configuration parameters is displayed on a per-PDU channel basis.

	Т							Logged In: admi System Nam	n (Administrator) e: SAP SZ Cabinet Logout
					Setup	Input Sensors	Outputs	Access Control	Power
Pow hase s ds re	er / Configure er Circuits are	configured here.						Nie /Mars Daviede	Prev Next
PDU	troi Method:	HILF + SINNF +						Min/Max Period:	10 Seconds
Ig Bon	e op/Down De	Fildy: 1 Seconds (On	Comme					Abort Cycle Delay:	10 Seconds
Сус	le Password:	Seconds (On	comms i	anure)				Abort Cycle Delay:	20 Seconds
Circ	uit	Name	Outlets	Туре					
01-L	1 Cfg	PDU Red	N/A	Monitor Only					
01-L	2 Cfg	A2							
01-L	3 Cfg	A3							
02-L	1 Cfg	PDU Yellow	N/A	Monitor Only					
02-L	2 Cfg	B2							
02-L	3 Cfg	B3							
03	Cfg	C1	N/A	Disabled					
04	Cfg	51	N/A	Monitor Only					
06	Cfg	F1	16	Per Outlet Monitor and Control					
Agg	Cfg	Aggregate	N/A	Calculated					
	Monito	or Trap Text	0	Dutlets Trap Text					
									Save

Control Method

The Control Method parameter specifies which control methods are available to control the outlets on PDUs attached to the unit.

HTTP + SNMP

The Web Management Interface and SNMP can be used to command PDU outlets.

HTTP Only

This option allows only the Web Management Interface to command PDU outlets. This effectively disables SNMP PDU outlet control.

SNMP Only

This option allows only SNMP to command PDU outlets. This effectively disables the Web Management Interface PDU outlet control.

RS232 Only

This option allows PDU control commands to be issued directly to a unit via the onboard RS232 port. This option disables the Web Management Interface and SNMP control.

Cycle Up/Down Delay

This parameter specifies the interval in seconds between switching on and switching off outlets when an entire PDU strip is cycled (all outlets commanded on or off).

Repeat Timer (on Comms Failure)

This parameter specifies the interval in seconds between when an initial PDU comms failure trap is produced and a repeat trap is issued.

Reboot Delay

This parameter specifies how long (in seconds) an outlet remains off after a reboot before switching back on.

Abort Cycle Delay

This parameter specifies how many seconds must elapse before a commanded cycle begins on a PDU. This delay gives the user time to reverse the decision to cycle a PDU before any outlet states are changed.

If you do not want to use this functionality, set the delay to zero.

Power – Configure Menu

This menu allows all the available options for a specific PDU to be specified.

	UT								Logged In: admi System Nam	n (Administrator) ie: SAP SZ Cabinet Logout
						Setup	Input Sensors	Outputs	Access Control	Power
atus 3-Phase rcuit akers sholds figure ntrol jure PDU angs I Gang ntrol	Power / Power C Control Cycle U Repeat	/ Configure Circuits are c I Method: Ip/Down Del Timer:	HTTP + SNMP • 47: 1 Seconds 600 Seconds (On	Comms I	Failure)				Min/Max Period: Reboot Delay: Abort Cycle Delay:	Prev Next Prev Next 15 minutes ▼ 10 Seconds 20 Seconds
Amp	Cycle P	assword:								
	Circuit		Name	Outlets	Туре					
	01-L1	Cfg	PDU Red	N/A	Monitor Only					
	01-L2	Cfg	A2							
	02-11	Cfg	A3 PDU Vellow	N/A	Monitor Only					
	02-L2	Cfg	B2	14/24	Holitor Only					
	02-L3	Cfg	B3							
	03	Cfg	C1	N/A	Disabled					
	04	Cfg	D1	N/A	Monitor Only					
	05	Cfg	E1	N/A	Monitor Only					
	06	Cfg	F1	16	Per Outlet Monitor and Control					
	Agg.	Cfg	Aggregate	N/A	Calculated					
		Monitor	Trap Text	()utiets Trap Text					
										Save

Circuit Name

Individual PDUs can be assigned names for ease of identification (for example, "Rack 5 PDU Sensor" or "Comm Room").

Device Type

Specify the type of PDU connected to channel here.

Disabled

No monitoring or control will be performed on this PDU channel.

Monitor Only

The monitoring of power values will be performed on this PDU channel.

Monitor and Control

Both outlet control and power monitoring will be enabled on this PDU channel.

Per Outlet Monitor

This option enables PDU-level monitoring and monitoring of each individual PDU outlet.

Per Outlet Monitor and Control

This option enables PDU-level monitoring and monitoring of each individual PDU outlet, plus outlet control.

Number of Outlets

This parameter specifies the number of controllable outlets present on a PDU. This is required when the **Control Only** or **Monitor and Control** options have been selected.

For example, if you have a PDU consisting of 24 Outlets, one of which is a permanent live (non-switching) outlet, 23 outlets would be specified.

Warning: Failure to specify the correct number of outlets can lead to the incorrect outlet being switched on or off.

During unit setup and deployment, you should select the **Control Only** or **Monitor and Control** options before critical loads are connected to outlets.

Cycle Password

This field specifies the password required to set a power cycle of outlets on a controllable strip. This password is used when switching outlets using SNMP, not when switching via the web interface.

Power on Mode

In the event that power to the PDU is lost, this parameter specifies how the outlets will be switched back on once power is restored.

RMS Volts

Limits and Traps

You can specify values for voltage, current, and total power thresholds here. You also can enable or disable traps for each threshold.

The following thresholds can be set:

- Upper Control Limit
- Upper Warning Limit
- Lower Warning Limit
- Lower Control Limit

Note: There are no lower limits for total power, because total power consumption can only go up, not down.

Repeat Timer

In the event of a communications failure with a connected PDU, this entry specifies how often (in seconds) Comm Fail traps will be generated.

RMS Current

(See options for RMS Volts above)

Total Power

(See options for RMS Volts above)

PDU Outlets

(See options for RMS Volts above)

Power Strips – Control

Individual outlets or all outlets on a given PDU can be switched on and off using this screen.

	ШТ						Logged In: adm	in (Administrator) System Name: a Logout
				Setup	Input Sensors	Outputs	Access Control	Power Strips
Status Configure Control CL-Amp	Power Strips / Control 1 : A 0 © 2 3 4 2 : 1 - A1 0 Stote: On 3 : Off 0 O Reboot 4 : 0 1 2 3 4 5 : E 0 2 2 3 4 6 : F 0 2 2 3 4	C C	1 12 13 14 15 16 1 12 13 14 15 16 1 12 13 14 15 16 1 12 13 14 15 16 1 12 13 14 15 16 1 12 13 14 15 16 1 12 13 14 15 16 1 12 13 14 15 16 1 12 15 14 15 16 1 12 15 14 15 16 1 12 13 14 15 16 1 12 13 14 15 16	C C C C C C C C C C C T 18 19 20 21 C C C C C C T 18 19 20 21 C C C C C C T 18 19 20 21 C C C C C T 18 19 20 21 C C C C C T 18 19 20 21 C C C C C T 18 19 20 21 C C C C C T 18 19 20 21 T 18 19 20 21 T 18 19 20 21 T 18 19 20 21	C 22 23 4 * C 22 23 7 * * C 23 7 * * *			
Pandu	IT				Setun	Input Sensors	Logged Ir Syste	: admin (Administrator) m Name: SAP SZ Cabinet Logout
Pov	ver Strips / Control							
Status - Shase Out Gircuit Breakers Thresholds Configure Control Configure PDU Gangs PDU Gang Control C Amp	let control for connected Power 01 02 02 03 03 03 05 04 (Monitor Only] 05 [Monitor Only] 06 04 05 [Monitor Only] 06 04 05 05 06 00 05 0 05 00 0	Devices is presented here.						

The display consists of a visual representation of PDUs that have **Control** or **Monitor and Control** enabled on the Configure page.

PDUs that are **Disabled** or in **Monitor Only** status do not display any outlet graphics and are displayed with appropriate text.

PDU inputs are numbered 1 to 2 in ascending order. PDU numbers correspond to the physical input ports on the rear of the SmartZone Gateway unit.

Switching Individual Sockets

When you click on a socket, a control menu above the socket displays further information. Three control options are also presented:

On

Selecting this option commands the selected outlet to switch On. If the outlet is already on this will have no effect.

Off

Selecting this option commands the selected outlet to switch Off. If the outlet is already off this will have no effect.

Reboot

The reboot option commands the selected outlet to switch off. After the time specified by the Reboot Delay timer has elapsed, the outlet will automatically switch itself back On.

Switching an Entire Strip

You can switch all the outlets on any strip Off or On with a single command by clicking the **Lightning Bolt** symbol on the end of a PDU graphic.

A small dialog displays, offering the following options:

On

This option commands all outlets on a selected PDU to switch on. Any outlets already on will remain on; any currently off will be switched on.

Off

This option commands all outlets on a selected PDU to switch off. Any outlets already off will remain off; any currently on will be switched off.

Abort!

Once a command has been issued to turn all outlets on a PDU on or off, you can click the **Abort!** button to abort the command.

The Abort Cycle delay option on the PDUs – Configure – Config menu specifies the time allowed in seconds for an abort to be issued.

LDAP

SmartZone Gateway LDAP Overview

The SmartZone Gateway unit implements a Lightweight Directory Access Protocol (LDAP) client. This allows the Gateway unit to authenticate user logins to the Web Management Interface using an LDAP Directory.

If LDAP is used for authentication, it is first consulted when a user attempts a login. If the user is not found or LDAP denies access, then the credentials are checked against the Gateway unit internal user list.

Note: Configuration of LDAP is an advanced topic and requires existing knowledge of LDAP function and setup.

SmartZone Gateway LDAP Structure

For a Gateway unit to successfully authenticate a user for Web Management Interface login, it needs to be pointed to a specific structure within a directory. You can point a unit to this structure within a directory by specifying the **Unit Base DN** on the Network Setup – LDAP page.

You will need to create the following Organizational Units:

- Gateway (this can be named anything)
- Gateway Administrators
- Gateway Controllers
- Gateway Viewers

Note: Groups are found in the Active Directory schema. However, any implementation which provides a group with a **Members** attribute may function.

The following figure depicts the Gateway LDAP authentication structure:



Once the required LDAP structure has been created, the Distinguished Name (DN) of users should be added to either:

- Gateway AdminUsers
- Gateway ControlUsers
- Gateway ViewUsers

Group Membership and Access Level

Membership in these groups grants the following permissions on Gateway units:

Gateway AdminUsers

Users placed into this group will have Admin privileges on Gateway units.

Gateway ControlUsers

Users placed into this group will have Controller privileges on Gateway units.

Gateway ViewUsers

Users placed into this group will have View privileges on Gateway units.

SmartZone Gateway Unit Configuration

For LDAP authentication to function, you need to provide certain configuration values for each Gateway unit.

PANDUIT								Logged In: admin (Administrator) System Name: sysName Logout		
		Setup	Input Sensors	Outputs	Access Control	Power				
Overview	Setup / LDAP Server	rs								
IP Config HTTP	Enabled:	Disabled •								
SNMP NMS	Credential Cache:	10 Minutes (Timeout)								
SNMP Rec'rs	Primary LDAP Serve									
Users	Display Name:	LDAP_Server_1								
Email Alerts	IP Address:	0.0.0.0								
Syslog Servers	Unit Base DN:]						
Events	Users Base DN 1:]						
Restart	Users Base DN 2:]						
	Focondary LDAD For	107								
	Dicplay Namo:	LDAR Server 2								
	ID Addross:									
	IF Address.	0.0.0		٦						
	Usors Raco DN 1:]						
	Users Base DN 2:]						
	osers base bit 2.									
									Save	

To enter the configuration values, perform the following steps.

- 1. If one LDAP server is to be used, select **Enabled Primary**.
- 2. Enter a descriptive name (for example, AD_Server_1) into the Display Name field.
- 3. Enter the complete DN of the top level OU.
- 4. Enter the DN of where users that are members of Gateway access groups can be found in the Directory. These DNs can be entered into **User Base DN 1** and **User Base DN 2**.
- 5. Click Save.

EPAX18 Expansion Unit

The SmartZone[™] Gateway EPAX18 is an expansion unit that connects directly to an EPA126 to expand its monitoring capabilities from 6 to a total of 24 power devices. When combined with an EPA126, this expansion unit allows up to 12 dual-fed cabinets to be fully monitored from the EPA126's IP address.

The EPAX18 supports up to 18 power distribution units or power monitoring devices, including the following:

- Single-Phase PDUs/Clamp Meters
- 3-Phase PDUs (Monitored)
- Single-Phase Monitored per Outlet PDUs
- Single-Phase Switched per Outlet PDUs

Front of Gateway EPAX18

The following image shows the front panel of the EPAX18 unit:



LEDs

Network

• Link (green): Embedded in the RJ-45 connection. Illuminates when the Ethernet link is established. Flashes with network activity.

Status

• CPU: Indicates system activity.

Power

- On: Illuminates when unit is powered.
- Feed A (amber): Illuminates when main present to input Feed A.
- Feed B (amber): Illuminates when main present to input Feed B.

Installation

To install the EPAX18, perform the following steps.

1. Link the EPAX18 to the EPA126 unit and connect a ground wire (not supplied).



2. Connect the power cords.



3. Connect the network and sensor cables (not supplied).


Gateway Web Management Interface PDU Display

With the EPAX18 expansion connected to the EPA126, the 24 PDUs are displayed across four screens, each displaying six PDUs, as in the examples below.

PAND	UIT												Logged In: ad System	min (Administr Name: Systen Lo	rator) n gout
								Setu	p In	put Sensors	Outputs		Access Control	Power	
Status	Power / S	Status													
Status 3-Phase Thresholds Configure	Informati	on from connected Power De	vices is presented I	iere.										Prev	Next
Control	Circuit	Name	Outlets		Volts		Amps		kVA	PF		kW	Hz		kWh
Configure PDU Gangs	01	Eagle-i1	N/A	 Image: A second s	191	10	0.0	 Image: A second s	0.0	0.00	×	0.0	60.8	 Image: A second s	1.0
PDU Gang	02	Eagle-i2	N/A		?		?.?		?.?	?.?		?.?	?.?		?.?
Control	03	Eagle-i3	N/A	+0	225	10	1.1	 Image: A second s	0.2	1.00	 Image: A second s	0.2	60.0	 Image: A second s	51.0
CL-Amp	04	Eagle-i4	N/A		?		?.?		?.?	?.?		?.?	?.?		?.?
	05	Eagle-i5	N/A	 Image: A second s	192	10	0.0	 Image: A second s	0.0	0.00		0.0	60.8	×	0.6
	06	Eagle-i6	N/A		?		?.?		?.?	?.?		?.?	?.?		?.?
		Aggregate				*	1.1	*	0.2		~	0.2			52.6

NDUIT								Logged In: ad System	min (Administrator) Name: System Logout
					Setup	Input Sensors	Outputs	Access Control	Power
Power / S	Status								
hase Ids Informati	on from connected Power	Devices is presented here	3.					l	Prev Next
Circuit	Name	Outlets	Volts	Amps	kVA	PF	kW	Hz	kWh
07	Eagle-i7	N/A	?	?.?	?.?	?.?	?.?	?.?	?.?
08	H1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
09	Eagle-i9	N/A	?	?.?	?.?	?.?	?.?	?.?	?.?
10	J1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11	K1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12	L1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Aggregate			✓ 1.1	✓ 0.2		✓ 0.2		52.6

SmartZone Gateway EPA126 User Manual

PAND	UIT										Logged In: a Syster	ıdmin (Administrator) m Name: System Logout
								Setup	Input Sensors	Outputs	Access Control	Power
Status Status 3-Phase Thresholds Configure	Power / S	Status ion from connected Power De	vices is presented here.									Prev Next
Control	Circuit	Name	Outlets	Volts		Amps		kVA	PF	kW	Hz	kWh
Gangs	13	M1	N/A	N/A		N/A		N/A	N/A	N/A	N/A	N/A
PDU Gang	14	N1	N/A	N/A		N/A		N/A	N/A	N/A	N/A	N/A
Control	15	01	N/A	N/A		N/A		N/A	N/A	N/A	N/A	N/A
CE Amp	16	P1	N/A	N/A		N/A		N/A	N/A	N/A	N/A	N/A
	17	Q1	N/A	N/A		N/A		N/A	N/A	N/A	N/A	N/A
	18	R1	N/A	N/A		N/A		N/A	N/A	N/A	N/A	N/A
		Aggregate			*	1.1	*	0.2		 ✓ 0.2 		52.6

PAND	UIT									Logged In: a Systen	dmin (Administrator) n Name: System Logout
							Setup	Input Sensors	Outputs	Access Control	Power
Chathur	Power / S	Status									
Status 3-Phase Thresholds Configure	Informati	on from connected Power	Devices is presented l	here.							Prev Next
Control Configure PDU	Circuit	Name	Outlets	Volts	Amps		kVA	PF	kW	Hz	kWh
Gangs	19	S1	N/A	N/A	N/#	ι	N/A	N/A	N/A	N/A	N/A
PDU Gang	20	T1	N/A	N/A	N/4	λ	N/A	N/A	N/A	N/A	N/A
CL-Amp	21	U1	N/A	N/A	N/4	N	N/A	N/A	N/A	N/A	N/A
	22	V1	N/A	N/A	N/4	λ	N/A	N/A	N/A	N/A	N/A
	23	W1	N/A	N/A	N/4	4	N/A	N/A	N/A	N/A	N/A
	24	X1	N/A	N/A	N/4	N	N/A	N/A	N/A	N/A	N/A
		Aggregate			✓ 1.1	. 🗸	0.2		√ 0.2		52.6

Temperature Sensor Adapter Installation

Follow the instructions below to install the ZAHTLADT-02 v1.01.01 temperature sensor adapter module. This adapter allows legacy sensors to provide more accurate temperature readings.

Note: This adapter does not work with the ZETHL-14 temperature sensor.

New Installations

Follow these instructions when you are installing a standard temperature sensor, but the upgraded sensor input is required.

- 1. Plug the adapter directly into the back of the gateway, at the sensor port to be used for temperature.
- 2. Plug the temperature sensor connector into the adapter.
- 3. Update the gateway firmware to the latest release.

Existing Installations.

Follow these instructions when the sensor is already installed along with the gateway.

- 1. Unplug the current temperature sensor from the gateway, noting the location where it resided.
- 2. Insert the adapter into that location.
- 3. Plug the sensor into the end of the adapter.
- 4. Perform these steps for all other temperature sensors to be changed.
- 5. The gateway firmware must be updated to the latest firmware.

Before the adapter is fitted:

After the adapter is fitted:

Fitting the Adapter In-line.

This procedure is not recommended, but it may be the only solution in some cases.

- 1. Using a patch lead from the gateway and an RJ45 Jack to Jack through connector on its non-gateway end, plug the adapter RJ45 Plug into the through connector.
- 2. Plug either the RJ45 plug of a temperature sensor into the jack on the adapter or a patch lead with the temperature sensor on the end.

Troubleshooting

Resetting the SmartZone Gateway to Factory Default Settings

To reset the Gateway unit to factory defaults, perform the following steps:

- 1. Press and release the **Reset** button on the front of the unit. The Alarm LED will flash twice (off/on, off/on).
- 2. Immediately press and hold the Mode button until the alarm LED goes off.
- 3. Immediately press and release the **Reset** button.

NOTE: The unit will now restart. The Status LED will start flashing after around 1 minute. The reset process is complete, and the IP address is set to the default 192.168.0.253.

Problem: The NMS Cannot Poll the SmartZone Gateway Unit

- Solution: Make sure the network is properly connected to the Gateway unit.
- Solution: Make sure the cable is in good condition.
- **Solution**: Try pinging the Gateway unit from another computer on the same network segment as the Gateway unit.
- Solution: Ensure that the NMS IP Address is in the NMS table of the Gateway unit.
- **Solution**:Ensure that the community string has been set for the NMS via the Web Management Interface.

Technical Support

For technical support for the SmartZone Gateway system, please contact Panduit Technical Support using one of the following methods:

- 1-866-721-5302 (toll-free)
 - USA: 6:30 a.m. 8:00 p.m. CST
 - India: 6:30 a.m. 5:00 p.m. IST (8:00 p.m. 6:30 a.m. CST)
 - On Call Support on Weekends
- systemsupport@panduit.com

Appendix A: Technical Details

Factory Default Settings

IP Address:	192.168.0.253
Subnet Mask:	255.255.255.0 (/24)
Default Gateway:	192.168.0.1
Web Management Address:	http://192.168.0.253/
Default username:	admin
Default password	admin

Operating Information

Input Power:	100-240 VAC (45W) 50-60 Hz
Operating Temperature:	0 ^O C to 40 ^O C
Storage Temperature:	-10 ^O C to 70 ^O C
Operating Humidity:	5% to 90% RH
Storage Humidity:	5% to 100% RH

CAUTION: There is a risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Appendix B: Hysteresis Demystified

When a temperature or humidity limit is reached and the relevant limit has its OFF to ON Trap enabled, an alarm trap is issued by the SmartZone Gateway unit.

With a zero hysteresis setting, the traps will continue to be generated each time the limit is reached.

This may be undesirable in a situation where the temperature or humidity level measure has reduced by only a small amount before rising again and triggering further traps.

The hysteresis function is provided to prevent further alarm traps from being generated until the measured value has fallen to a satisfactory level.



As shown in image above, the humidity first rises past its upper warning threshold, which generates an alarm trap.

The humidity then reduces slightly but does not reduce to the hysteresis level, which is 1.5% relative humidity lower than the alarm setting (1.5% relative humidity lower as an absolute measured value, rather than 1.5% of currently measured value).

Humidity then increases and decreases again. However, on the second decrease of humidity the level drops below the hysteresis level. The Humidity falling below the hysteresis level re-enables alarm traps for the next alarm event. An upper limit of 25 and a hysteresis threshold of 1.5 yield a threshold limit of 23.5.

The humidity level again begins to rise and again exceeds the upper limit, however this time an alarm trap is generated again.

The Hysteresis feature acts on the following Temperature and Humidity thresholds:

- Upper Control Limit (UCL)
- Lower Control Limit (LCL)
- Upper Warning Limit (UWL)
- Lower Warning Limit (LWL)

The inverse of the above description is true when applied to Temperature and Humidity lower control and warning limits.

You can configure the hysteresis threshold by using the menu options.

Appendix C: Networking Reference

Reference

This section discusses SNMP communities, IP addressing, subnet masking, routers and Gateways.

Communities

A community is a string of printable ASCII characters that identifies a user group with the same access privileges. For example, a common community name is "public". For security purposes, the SNMP agent validates requests before responding. The agent can be configured so that only managers that are members of a community can send requests and receive responses from a particular community.

This prevents unauthorized managers from viewing or changing the configuration of a device.

IP Addresses

Every device on an internetwork must be assigned a unique IP (Internet Protocol) address. An IP address is a 32-bit value comprised of a network ID and a host ID. The network ID identifies the logical network to which a particular device belongs. The host ID identifies the particular device within the logical network.

IP addresses distinguish devices on an internetwork from one another so that IP packets are properly transmitted.

IP addresses appear in dotted decimal (rather than in binary) notation. Dotted decimal notation divides the 32-bit value into four 8-bit groups, or octets, and separates each octet with a period.

For example, 199.217.132.1 is an IP address in dotted decimal notation. To accommodate networks of different sizes, the IP address has three divisions -

Classes A for large, B for medium, and C for small.

The difference among the network classes is the number of octets reserved for the network ID and the number of octets reserved for the host ID:

Class	Value of First Octet	Network ID	Host ID	Number of Hosts
А	1-126	first octet	last three octets	16,387,064
В	128-191	first two octets	last two octets	64,516
С	192-223	first three octets	last octet	254

Any value between 0 and 255 is valid as a host ID octet except for those values reserved by the IPv4 standard for other purposes:

Value	Purpose
0, 255	Network Number & Broadcast
127	Loopback testing and interprocess communication on local devices
224-254	IGMP multicast and other special protocols

Subnetting and Subnet Masks

Subnetting divides a network address into subnetwork addresses to accommodate more than one physical network on a logical network.

For example: A Class B company has 100 LANs (Local Area Networks) with 100 to 200 nodes on each LAN.

To classify the nodes by its LANs on one main network, this company segments the network address into 100 subnetwork addresses (If the Class B network address is

150.1.x.x, the address can be segmented further from 150.1.1.x through 150.1.100.x.).

A subnet mask is a 32-bit value that distinguishes the network ID from the host ID for different subnetworks on the same logical network.

Like IP addresses, subnet masks consist of four octets in dotted decimal notation.

You can use subnet masks to route and filter the transmission of IP packets among your subnetworks.

The value "255" is assigned to octets that belong to the network ID, and the value "0" is assigned to octets that belong to the host ID.

Network Mask	Routing and Filtering
255.0.0.0	Class A network. First octet defines network number. Final three octets define host address. Valid Class A network numbers are in the range 1 to 126.
255.255.0.0	Class B network. First 2 octets define network number. Final two octets define host address. Valid class B network numbers are in the range 128.0.x.x to 191.255.x.x
255.255.255.0	Class C network. First 3 octets define network number. Final octet defines host address Valid class C network numbers are in the range. 192.0.0.x 223.255.255.x

Gateways

Gateway, also sometimes referred to as a router, is any device with two or more network adapters connecting to different physical networks.

Gateways allow for transmission of IP packets between different networks on an internetwork.

Appendix D: Pressure to Voltage Conversion

This appendix covers pressure-to-voltage conversion based on using the following equipment and settings:

- ZEDIFFPRESS-03
- Pressure Range: -0.625 to 0.625
- Voltage Output: 0 to 5V

Conversion equation:

Voltage = 4 * pressure +2.5

Note: Pressure is measured in units of H2O.

Based on the above information, here are the alarm points.

Measure	Upper Warning Limit	Upper Control Unit
Pressure	0.15	0.3
Voltage	3.1	3.7

Appendix E: Encryption and Security

The Gateways support HTTPS encryption, and they support the following cipher configurations.

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA