Smart PDU

Instruction Manual

barpa

barpa

Instruction Manual
Smart PDU

Summary

Product Overview ---- 3
How to Install in a Telecommunications Rack ---- 3
Ports and Connections ---- 4
Cascading Management ---- 5
LED Indicators ---- 6
Initial Configuration ---- 6
- Overview ---- 7
- Control ---- 8
- Threshold ---- 9
- Network ---- 9
  - TCP/IP ---- 9
  - SNMP ---- 9
  - HTTP ---- 9
  - SMTP ---- 10
  - Update ---- 10
  - Modbus ---- 11
  - Telnet ---- 11
  - SSH ---- 11
- System ---- 11
  - Outlets ---- 11
  - Time ---- 12
  - Users ---- 12
  - USB ---- 12
  - Tool ---- 12
- Logs ---- 13
- About ---- 13
- Procedures ---- 13
  - Firmware Update ---- 13
- Troubleshooting ---- 14
  - The SPDU does not turn on ---- 14
  - Physical display on, but outlets without power ---- 14
  - No access to the web management interface ---- 15
  - SNMP does not respond or does not send data ---- 15
  - Unexpected shutdowns or restarts ---- 16

How to get help ---- 16

barpa

Instruction Manual

Smart PDU

Product Overview

The SmartPDU barpa is an intelligent power distribution unit designed to supply and manage IT equipment safely, efficiently, and in a controlled manner. It allows real-time monitoring of electrical consumption, protection against overloads, and, in some models, remote control of outlets. It is suitable for server racks, data centers, technical cabinets, and professional environments where reliability, energy control, and ease of maintenance are not optional—they are mandatory.

The Smart PDU (SPDU) from barpa is available in two models as Smart Control PDU and Smart Monitor PDU.

How to Install in a Telecommunications Rack

1. The barpa SPDU is of the "rack mount" type, meaning it must be installed in a standard 19" telecommunications rack (such as Norma/Cetus/Orion of barpa). There are versions in horizontal or vertical format, and it can be installed either at the front or rear of the rack, according to project specifications or requirements.

2. When the barpa SPDU is connected to the main power circuit, it can supply power to equipment connected to it (which in this manual will be referred to as "protected equipment").

3. The load current of the protected equipment must not exceed the value specified in the barpa SPDU datasheet. Do not overload the outlets. Protection mechanisms exist, but overloading the SPDU is not recommended.

4. It is strictly forbidden to disassemble this product. Otherwise, all resulting consequences will be entirely your responsibility.

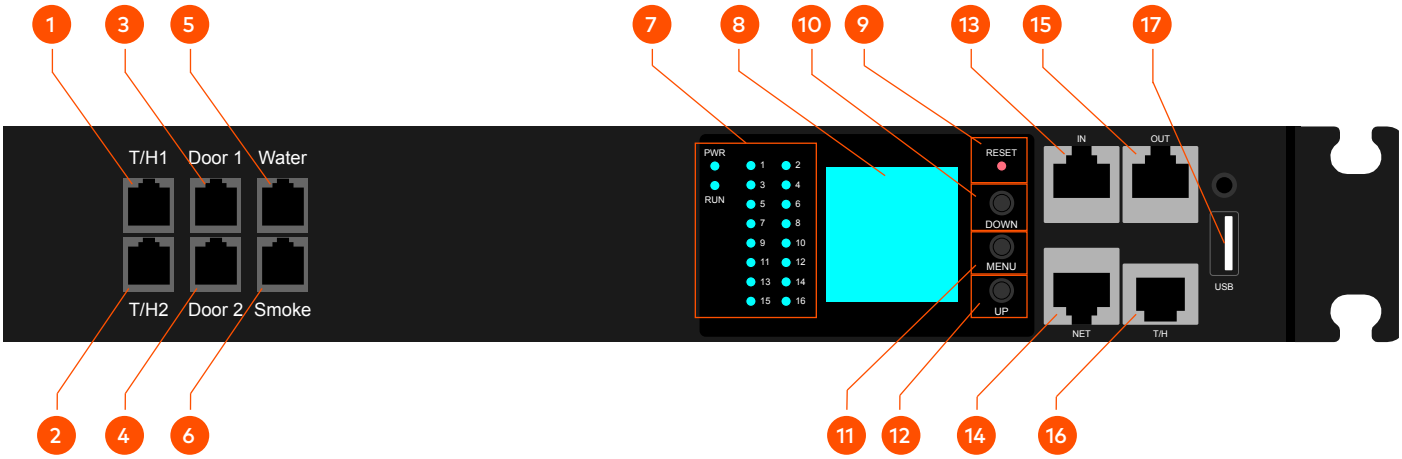
5. Use fixed supports during installation.

6. Connect the cables and outlets correctly and pay attention to electrical safety.

Instruction Manual

Smart PDU

Ports and Connections



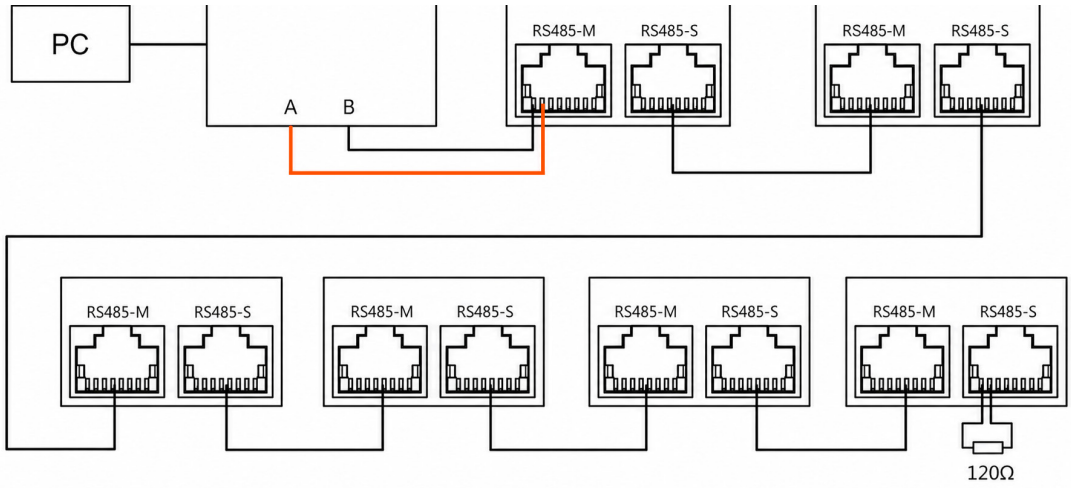
1. RJ11 port, for connecting the temperature & humidity sensor
2. RJ11 port, for connecting the temperature & humidity sensor
3. RJ11 port, for connecting the door opening sensor
4. RJ11 port, for connecting the door opening sensor
5. RJ11 port, for connecting the water leakage sensor
6. RJ11 port, for connecting the smoke detection sensor
7. Set of indicator LEDs. See chapter 5.
8. LCD display
9. Reset button - if pressed for 10 sec, it will restore the equipment settings to factory defaults.
10. Down directional navigation button. If pressed for more than 10 sec, it will restart the SPDU.
11. Menu button, also used as “OK”.
12. Up directional navigation button.
13. RS485/RJ45 port, used for management cascading. See chapter 4.
14. RJ45 port used to provide network connectivity and management to the SPDU.
15. RS485/RJ45 port, used for management cascading. See chapter 4.
16. RJ11 port, for connecting the temperature & humidity sensor
17. USB port, used to update the SPDU firmware. See chapter 6.8.1

Cascading Management

SPDU management is normally carried out via TCP/IP network, using a standard ethernet patch cord connected to its NET port, and the other end connected to a network switch or a computer.

However, it is also possible to use cascading management. This can be useful in situations where we have multiple SPDUs and do not have enough switch ports available. Cascading management uses RS485 communication, and the exchange of information is more sensitive and slower than conventional ethernet.

To use it, the first SPDU must be connected to the network with the RJ45 ethernet patch cord connected to the NET port and an RS485 cable connected to the OUT port, which then must be connected to the next SPDU at its IN port, and so on. Check the diagram below:



Some important considerations:

• Each SPDU added to the cascade adds about 1-2 seconds of communication delay. The maximum allowed is 32 units, which means a total delay of about 1 minute.

• Before using the cascading function, each SPDU must be configured in the appropriate GUEST mode, with the main unit set as HOST.

• It is recommended that RS485 cascade connections have a maximum length of four meters to ensure the validity of the security data.

• When RS485 cables are installed outdoors, make sure the shielding is grounded and that the total cable length does not exceed 1200 meters.

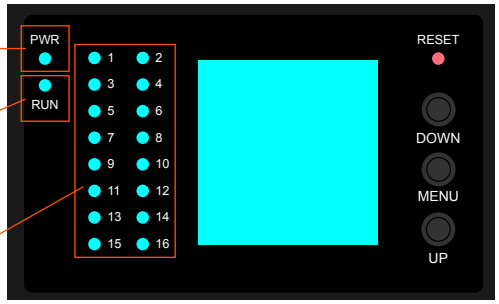
• If the shielded twisted-pair cable is long, an impedance of approximately 120 ohms and a reduction in the transmission rate are recommended to improve communication reliability.

LED Indicators

PWR
Steady light: Indicates that the SPDU is active.
Off: Indicates that the SPDU is inactive.

RUN
Flashing light: Indicates that the SPDU is operating normally.

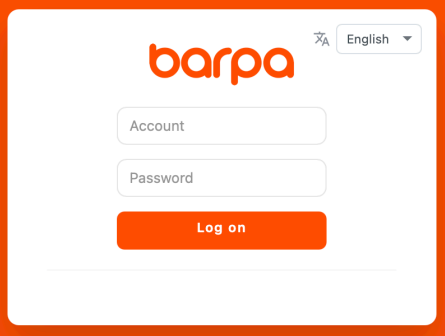
1–16 Indicates the sockets
Steady light: Indicates that the socket is active.
Off: Indicates that the socket is inactive.



Initial Configuration

It is possible to access the barpa SPDU configuration through a web browser, regardless of the operating system. The configuration interface is web-based.

The access details can be checked on the label printed on the product. The default IP address is 192.168.8.8/24, and it can also be checked on the LCD display. Please note that the credentials are case-sensitive.

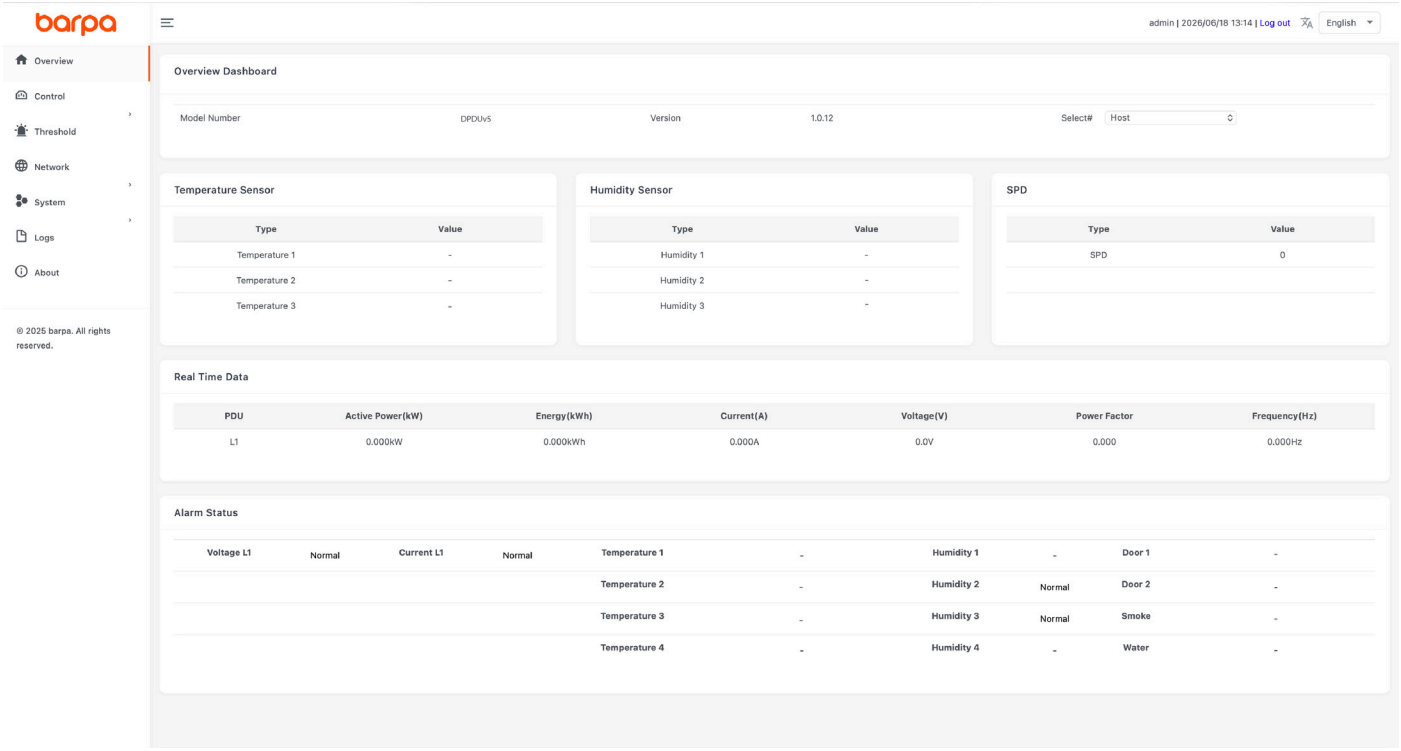


There is a security setting whereby if the password is entered incorrectly 5 times within a 1-minute interval, access is blocked for 5 minutes. This is a security measure implemented to mitigate brute-force attacks against the SPDU.

Instruction Manual
Smart PDU

Overview

This is the screen shown after successfully logging in to the barpa SPDU web address.



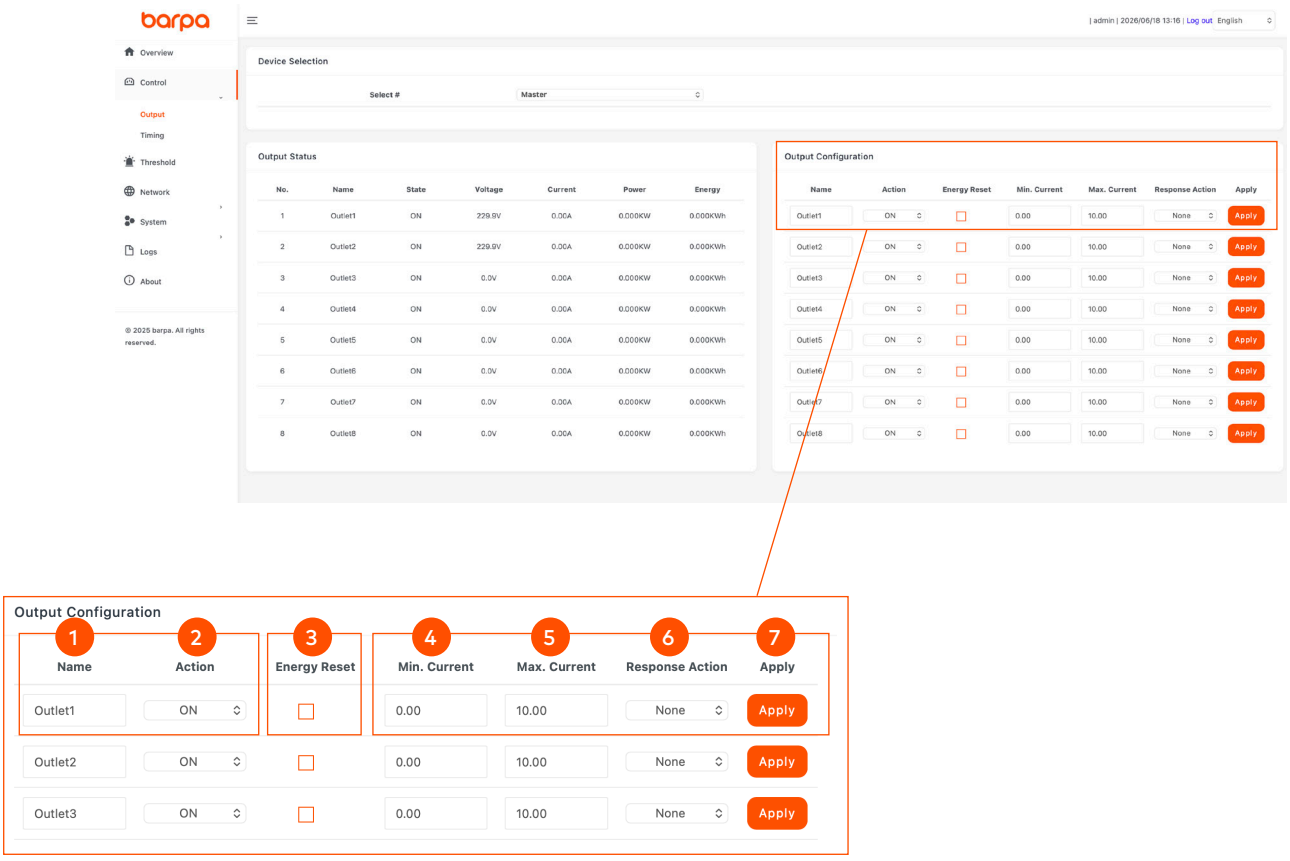
This screen provides an overview of the equipment, including values collected by the sensors, the overall SPDU status, the general electrical status, and whether any alarm is present in the system.

As for the SPDU, it is used to protect the equipment connected to the SPDU against voltage spikes originating from the electrical grid.

Instruction Manual
Smart PDU

Control

The Control feature is only available in Smart Control PDU.



1. Allows us to give a name or description to a socket.
2. Allows us to perform an action on the socket, such as switching it off, on or resetting it.
3. Allows us to reset the socket's energy consumption meters.
4. Allows us to set a minimum current before performing a configured action.
5. Allows us to set a maximum current before performing a configured action.
6. Allows us to define an action that will be automatically performed when the socket's current is outside the configured minimum/maximum values. The action can be to switch the socket off for protection, or to reset it.
7. Button to apply the settings or execute the action.

Threshold

On this screen we can configure the minimum and maximum limits for Voltage, Current, and Temperature and Humidity sensors. This means that when the values reach these configured limits, an alarm notification will be generated.

On this screen we can also enable or disable the SPDU audible alarm. When enabled, if any alarm is detected in the system, the SPDU continuously emits an audible alarm to indicate the event.

Finally, there is the "Electric Energy Setting" function. The SPDU also measures the cumulative energy consumption of each socket. This option allows you to reset these values to zero across the entire SPDU and restart the energy consumption calculation

Network

This menu consists of several submenus, which will be detailed in the following sections.

TCP/IP

Here we can configure the SPDU network settings for both IPv4 and IPv6. By default, the SPDU comes configured with a "Static" IP address, namely 192.168.8.8/24. However, if necessary, it can be configured as a DHCP client.

SNMP

On this screen we can carry out the entire SNMP configuration of the SPDU. By default it comes configured as SNMP v1, but it can be set to v2c or v3 according to the network requirements. It is also on this screen that the SNMP server IPv4 address for sending traps is configured, along with the read and write communities.

Still on this screen, it is possible to configure custom values for:
SysName (oid 1.3.6.1.2.1.1.5.0)
SysDescription (oid 1.3.6.1.2.1.1.1.0)
SysContact (oid 1.3.6.1.2.1.1.4.0)
SysLocation (oid 1.3.6.1.2.1.1.6.0)

HTTP

In this menu, we can define which web protocol will be used to access the SPDU through the browser. By default, it is set to HTTP, but it is possible to select the more secure HTTPS protocol.

If HTTPS is chosen, the SPDU includes an internal mechanism to auto-generate a certificate, but it is possible to upload a custom certificate.

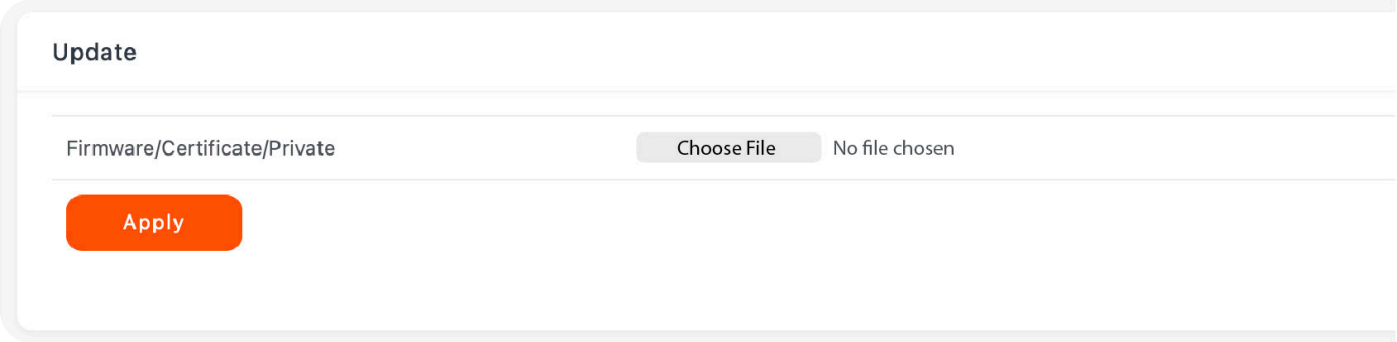
SMTP

On this screen we can configure the credentials of an email account that will be used by the SPDU to send notifications. It is possible to define the number of notification cycles, as well as the interval between notification sends in each cycle.

Update

This is where we can perform SPDU firmware updates. Two update methods are presented here.

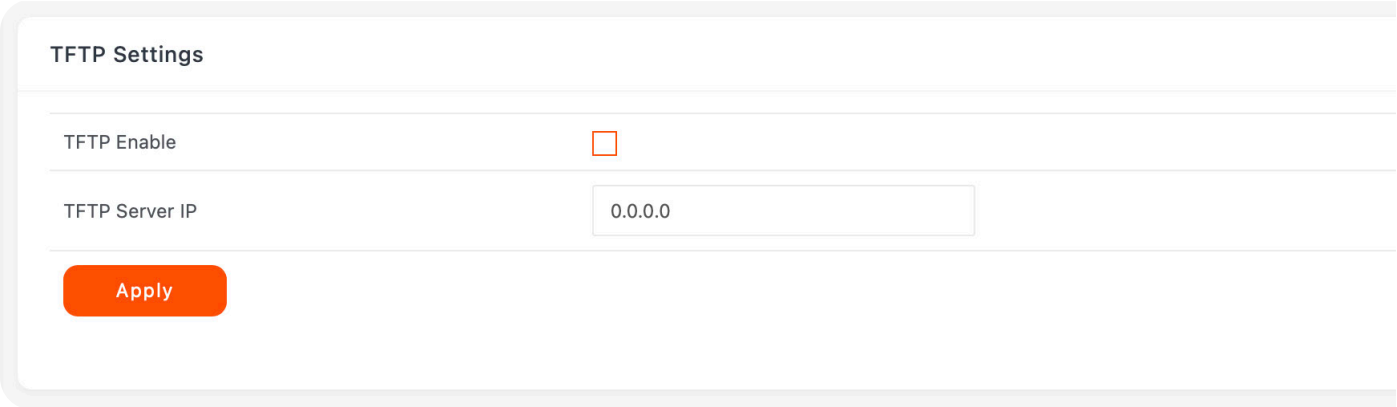
The first option is where we can upload the firmware file to update the SPDU. We must take care to use only the correct file for the respective model. In case of doubt, contact support (see the support section).



On the screen below, we can enable updating by TFTP. Besides enabling the option (which is disabled by default), we must specify the IP address of the TFTP server.

With this method, the SPDU actively fetches the file from the TFTP server at 1-minute intervals.

For more details on how to update, see the section 6.8.1



Modbus

This menu controls SPDU Modbus access over the Ethernet network (Modbus TCP).

Modbus TCP/IP Enable activates or deactivates the Modbus TCP service. When enabled, the PDU starts responding to Modbus requests over the IP network.

Port defines the TCP port used by Modbus. The default value is 502, which is the official port of the Modbus TCP protocol. Only change it if there is a network conflict or a supervisory system requirement.

In Cascade, we can define the SPDU management cascade configuration when several PDUs are interconnected.

Guest selection allows you to select which Modbus addresses (device IDs) will be active in the cascade. Each number represents a unique Modbus address on the network and, consequently, one SPDU. With each SPDU added to the cascade, management latency increases by about 1-2 seconds, and with all 32 active, by about 1 minute in total.

Telnet

In this option, we can enable or disable remote access to the SPDU via TELNET. By default, and for security reasons, this option comes disabled.

SSH

Similarly to TELNET, here we can disable or enable remote access to the SPDU via SSH. SSH is a more robust and secure protocol than TELNET, and therefore it is enabled by default.

System

This menu consists of several submenus, which will be detailed in the following sections.

Outlets

In this submenu we can configure the interval (in seconds) for how long the outlets take to switch on and off. The same can be done for outlet rebooting, where we can configure how long the SPDU waits during the restart.

Time

At this point, we can configure the SPDU system date and time. The configuration can basically be carried out in 3 ways:

Manual: where the SPDU date and time are defined manually.

Obtain the computer time: where the SPDU obtains this data from the client computer.

SNTP: where the SPDU fetches date and time information over the network from the configured SNTP server. It is possible to configure the interval for SNTP queries, as well as time correction.
It is important to ensure that a valid DNS is configured under Network > TCP/IP, otherwise it may compromise SNTP operation if a domain name is used instead of an IP address.

Users

On this screen it is possible to change the default password of the admin user.

It is important to do this as soon as possible, since the default password is printed on the equipment and may compromise system security.

In addition, it is also possible to configure two other users and define individual permissions for each of them.

USB

Here we can enable or disable the SPDU USB port. By default, it is enabled to make on-site firmware updates easier.

Tool

At this point, we can make several general SPDU settings, which are described below:

- Model Number
- LCD Title
- LCD Display Direction
- LCD Backlight
- LCD Backlight Time
- LCD Rest Brightness
- Log Out
- Logout time
- Hostname in Router

We can also disable or enable the use of the button present on the SPDU panel.

We can also disable or enable logging for the outlets, as well as restart the SPDU management module. It is worth noting that restarting SPDU management does not interrupt the power supply to the outlets.

Logs

This is where all events occurring in the SPDU are recorded, whether alarms or events. It is possible to query by date or by type, export the logs in text format, and clear the entire database.

About

On this screen we can view general information about the SPDU, such as its model, firmware version, hardware version, date of the last firmware update, and the uptime of the management module.

Procedures

Firmware Update

The firmware update procedure can basically take place in three ways:

- By the web management interface
- By TFTP
- By USB flash drive

Below, it is described how to carry out the procedure through each of these methods.

Web management interface

This method allows us to update the SPDU firmware by uploading the binary directly through the webGUI, in the Network > Update section.

TFTP

This method allows us to update the SPDU firmware over the network. When this option is enabled, it will begin checking the configured TFTP server for the firmware binary at intervals of approximately every 60 seconds. It is important to keep the file in the root directory of the TFTP server, as the SPDU will look for it directly there. Once it finds the file, it will request permission from the server and start the transfer.
The SPDU will fetch the firmware according to its model.

USB Flash Drive

In this procedure, the update takes place physically where the SPDU is located. It is necessary to have a USB-A flash drive, formatted in NTFS or FAT32, containing only the firmware binary.

When the SPDU detects the connected flash drive, it will look for the appropriate file according to its model and immediately start the transfer. You can follow the transfer progress on the LCD display. Once it is complete, follow the guidance to disconnect the flash drive from the SPDU USB port.

In case of doubt, contact our support team through the indicated channels.

The firmware file name must match the internal model of the SPDU, which can be checked in About > Internal Model. If it is different, it will not update.

Troubleshooting

The SPDU does not turn on

Possible causes

-No power at the input
-Faulty power cable or plug
-Previously detected overload
-Circuit breaker or protection tripped due to overload

Verification

-Confirm that power is present at the input socket.
-Inspect the power cable.
-Check the condition of the SPDU circuit breaker or protection.
-Check whether there are messages or indicators on the physical display.

Corrective action

-Restore the input power supply.
-Reset the circuit breaker protection, if applicable.
-Replace the power cable or plug, if possible.
-Remove the loads and try powering up only the SPDU again.

Physical display on, but outlets without power

Possible causes

-Outputs disabled via the web interface.
-Scheduling or automation rules.
-Failure in the output circuit

Verification

-Access the web interface and check the outlet status.
-Check the event logs for alerts or failures.
-Check the messages shown on the physical display.
-Test an outlet with no load connected.

Corrective action

-Manually activate the affected outlets.
-Adjust or remove scheduling rules.
-Reduce the connected load.
-If the problem persists, contact technical support.

No access to the web management interface

Possible causes

-Incorrect IP configuration.
-Faulty network cable disconnected from the management port.
-Incorrect VLAN.
-Network unavailable.

Verification

-Check the link LEDs on the SPDU management port.
-Check the configured IP on the physical display.
-Test connectivity with ping.
-Confirm the VLAN configured on the switch.

Corrective action

-Correct the network configuration.
-Restart the SmartPDU.
-Restore factory settings if necessary.
-Remove the loads and try powering up only the SPDU again.

SNMP does not respond or does not send data

Possible causes

-SNMP disabled
-Incorrect SNMP community
-Incompatible SNMP version
-Blocked by firewall

Verification

-Confirm that SNMP is enabled in the web interface.
-Check the configured community, version, and permissions.
-Test communication from the SNMP server.
-Check the logs for SNMP-related errors on the server.

Corrective action

-Adjust the SNMP settings.
-Allow communication on the network.
-Restart the service, if applicable.

Unexpected shutdowns or restarts

Possible causes

-Total overload
-Short circuit in connected equipment
-High ambient temperature
-Internal power supply failure

Verification

-Check total consumption on the display or web interface.
-Disconnect loads and reconnect them gradually.
-Check ventilation and the ambient temperature.
-Review event logs.

Corrective action

-Redistribute the load.
-Remove faulty equipment.
-Improve cooling in the room.

How to get help

Get in touch through the company's official channels, namely:

Email: info@barpa.eu
Telephone: +351 224 664 200
Support contact: +351 224 664 200