

LINDY®

CONNECTION PERFECTION

IPower Strip 4

User Manual

English

No. 32661

www.lindy.com

CE

- 1. Device Description 3
 - 1.1. Security Advice 3
 - 1.2. Content of Delivery..... 3
 - 1.3. Description 3
 - 1.4. Installation 4
 - 1.5. Overvoltage Protection..... 5
 - 1.6. Status LED 5
 - 1.7. Bootloader Mode..... 5
 - 1.8. Firmware-Update 7
 - 1.9. Technical Specifications..... 7
 - 1.9.1. Electrical Measurement 8
 - 1.10. Sensor..... 8
- 2. Operating 10
 - 2.1. Operating the device directly 10
 - 2.2. Control Panel 10
 - 2.3. Maintenance Functions 12
- 3. Configuration..... 13
 - 3.1. Configuration by Software 13
 - 3.2. Configuration via Webinterface 14
 - 3.2.1. Power Ports 14
 - 3.2.2. Watchdog 15
 - 3.2.3. IP Address 17
 - 3.2.4. IP ACL 18
 - 3.2.5. HTTP 19
 - 3.2.6. Sensors 20
 - 3.2.7. SNMP 22
 - 3.2.8. Syslog 23
 - 3.2.9. E-Mail 24
- 4. Specifications 25
 - 4.1. IP ACL 25
 - 4.2. IPv6 25
 - 4.3. SNMP 26
 - 4.3.1. Device MIB 28
 - 4.4. SSL 29
 - 4.5. Messages 31
 - 4.5.1. Email 31
 - 4.5.2. SNMP Traps 31
 - 4.5.3. Syslog 32
- 5. Support 32
 - 5.1. Data Security..... 32
 - 5.2. FAQ..... 32

1. Device Description

1.1. Security Advice

- The device must be installed only by qualified personnel according to the following installation and operating instructions.
- The manufacturer does not accept responsibility in case of improper use of the device and particularly any use of equipment that may cause personal injury or material damage.
- The device contains no user-maintenable parts. All maintenance has to be performed by factory trained service personnel.
- This device contains potentially hazardous voltages and should not be opened or disassembled.
- The device can be connected only to 230V AC (50Hz or 60 Hz) power supply sockets.
- The power cords, plugs and sockets have to be in good condition. Always connect the device to properly grounded power sockets.
- The device is intended for indoor use only. Do NOT install them in an area where excessive moisture or heat is present.
- Because of safety and approval issues it is not allowed to modify the device without our permission.
- Please note the safety advises and manuals of connected devices, too.
- The device is NOT a toy. It has to be used or stored out of range of children.
- Care about packaging material. Plastics has to be stored out of range of children. Please recycle the packaging materials.
- In case of further questions, about installation, operation or usage of the device, which are not clear after reading the manual, please do not hesitate to ask our support team.
- Please, never leave connected equipment unattended, that can cause damage.
- Connect only electrical devices that do not have limited on-time. I.e. in case of failure, all connected appliances have to cope with a continuous on-time without causing damage.

1.2. Content of Delivery

The package includes:

- **LINDY IPower Strip 4**
- Quick Start Guide
- CD-ROM with Manual and Softwaretools

1.3. Description

The **LINDY IPower Strip 4** can switch 4 different load outputs (schuko-socket (CEE 7/3), max. 16A). The device has the following features:

- Switching of 4 load outputs.
- Energy Metering of the mains connection and measurement of voltage, current, active power, reactive power, apparent power, frequency, phase angle, power factor.
- Connecting of one optional external sensor to determine the temperature and humidity, or a input switch.

- One three-digit 7-segment LED display (for display of current or temperature / humidity of the external sensors).
- Separated over-voltage protection of the mains connection (Overvoltage Protection).
- Startup delay, individually parametrizable for all load outputs.
- Individually adjustable watchdog function that switches power ports in dependency of the accessibility of a device (network ping) .
- Dual TCP/IP Stack with IPv4 and IPv6 support.
- Control and monitoring of the device via Ethernet with an integrated web server and SNMP (v1, v2c and v3) .
- Generation of messages (e-mail, Syslog and SNMP traps) at relay switching and depending on the energy measurement limits, resp. external sensors.
- Secure E-Mails.

LINDY-Control: LINDY IPower products can be controlled using your smartphone or tablet. Please download the "LINDY-Control" app from Google Play or Apple iTunes.

1.4. Installation



1. Sensor connector
2. Ethernet connector (RJ45)
3. Actual Current (7-segment display)
4. LED indicator for Overvoltage Protection (red - inactive)
5. External Sensor indicator
6. 4 plain text displays (on/off) for the state of the Power Ports
7. Status LED
8. OK Button
9. Select Button




Power Ports 1 to 4


Start-up the device

- Connect the power cord of the unit to the mains supply.
- Plug the network cable into the Ethernet connector (RJ45).
- Attach the external sensor (optional).

1.5. Overvoltage Protection

The device contains an overvoltage protection. The protection is based on input side varistors with thermal fuse between phase (L) and neutral (N) to protect the internal electronics and power ports with failure detection (permanently triggered thermal fuse). The state of the protection is indicated on the front panel by a red flash. A not visible flash means, that the protection is active, a red flash symbolizes that the overvoltage protection fails. In addition, the status of the overvoltage protection can be seen on the Webpage (HTTP) and acquired with SNMP. The surge protection module is designed that it can derive a practical unlimited number of voltage pulses in normal installation environments. In an environment with many energy rich surge pulses it can result in permanent loss of function due to aging of the overvoltage protection element.

 Recovering of the overvoltage protection function can only be performed by the manufacturer of the device. In the normal case, the device will continue to work even after the failure of the protective function.

 A signaling via E-Mail, Syslog or SNMP trap occurs only once during operation, exactly at the moment in which the protection fails. In addition, at the start up of the device a message is generated, when the overvoltage protection is not active.

1.6. Status LED

The Status LED shows different states of the device:

- red: Device is not connected to the Ethernet.
- orange: Device is connected to the Ethernet and waits for answer from the DHCP server.
- green: Device is connected to the Ethernet, TCP/IP settings allocated.
- periodic blinking: Device is in Bootloader mode.

1.7. Bootloader Mode

The configuration with GBL_Conf.exe is only possible if the device is in Bootloader Mode.

Activation of the Bootloader Mode

via push button:

- Hold both buttons for 3 seconds

or

- Remove the power supply
- Hold down the "Select" button. If the push button is recessed, use a pin or paper clip
- Connect the operating voltage

by Software: (only if "Enable FW to BL" was previously activated in GBL_Conf.exe)

- Start GBL_Conf.exe
- Do a network search with the "Search" menu action
- Activate in menu "Program Device" the item "Enter Bootloader"

via web interface:

Press "Enter Bootloader Mode" on the [maintenance](#) web page.

Whether the device is in Bootloader mode, is indicated by the flashing of the status LED, or it is shown in GBL_Conf.exe, after a renewed device search, with the appendix "BOOT-LDR" after the device name. In Bootloader mode the program GBL_Conf.exe can disable the password and the IP ACL, perform a firmware update, and restore the factory settings.



Activation of the Bootloader mode and an abandonment of the Bootloader does not change the state of the power or output ports as long as the supply voltage is maintained.

Abandonment of the Bootloader Mode

via push button:

- Hold both buttons for 3 seconds (only if the device has 2 buttons)

or

- Remove and connect the power supply without operating a button

by Software:

- Start GBL_Conf.exe
- Do a network search with the "Search" menu action
- In menu "Program Device" activate the item "Enter Firmware"

Factory Reset

If the device is in bootloader mode, it can always be put back to its factory default. All TCP / IP settings are reset in this operation.

via push button:

- Activate the Bootloader Mode of the device

- Hold down the button (or the "Select" button for devices with 2 buttons) for 6 seconds. If the push button is recessed, use a pin or paper clip
- The status LED will blink in a fast rhythm, please wait until the LED blinks slowly (about 5 seconds)

by Software:

- Activate the Bootloader Mode of the device
- Start GBL_Conf.exe
- In menu "Program Device" activate the item "Reset to Fab Settings"
- The status LED will blink in a fast rhythm, please wait until the LED blinks slowly (about 5 seconds)

via web interface: Press "Restore Fab Settings and Restart Device" on the maintenance web page.

1.8. Firmware-Update

To perform a firmware update, the program GBL_Conf.exe and the latest firmware is needed.

via web interface:


Use "Browse" on the [maintenance](#) site to locate the desired firmware file and press "Update".

by Software:

- Enable the Bootloader mode (see Chapter Bootloader Mode)
- Start GBL_Conf.exe
- Select the device for which a firmware update is to be performed
- Click "Program Device" and then select there "Firmware Update"
- Specify the firmware file that should be uploaded

Upon completion of the update process, please start the new firmware of the device. You can do this by simply leaving the Bootloader mode.

A firmware update, unlike other functions, is not sent as a network broadcast. Therefore, the device must have a valid IP address and a valid netmask before the firmware update. If necessary, please correct the entries in GBL_Conf.exe in Bootloader mode and save them with "Save Config".

 If after a firmware update, the web page is not displayed correctly anymore, this may be related to the interaction of Javascript with an outdated browser cache. Not always helps a Ctrl-F5, it is recommended that you manually delete the cache in the browser options. Alternatively, you can test start the browser in "private mode".

1.9. Technical Specifications

Interfaces	1 x Ethernet port (RJ45) 1 x Power supply (schuko-plug, max.16 A), length approx 2m 4 x Load outputs (schuko-socket, max. 16 A) 1 x Mini-DIN for external sensor
Network connectivity	10/100 MBit/s 10baseT Ethernet

Protocols	TCP/IP, HTTP, SNMP v1 und v2c, SNMP traps, Syslog, E-Mail (SMTP)
Power Supply	internal power supply (230V AC / -15% / +10%)
Overvoltage Protection <ul style="list-style-type: none"> • maximum operating voltage • single peak current for 20/80us pulse • max. clamping voltage 20/80us pulse, I_{pk} = 100 A 	20 mm/190 J varistor disk 300 VACrms 10000 A 710 V
Environment <ul style="list-style-type: none"> • Operating temperature • Storage temperature • Humidity 	0°C - 50 °C -20°C - 70 °C 0% - 95% (non-condensing)
Case	Synthetic
Measurements	484mm x 46mm x 74mm (L x H x W)
Weight	approx. 1050 kg

1.9.1. Electrical Measurement

Electrical Measurement Specification				
Category	Range	Unit	Resolution	Inaccuracy (typical)
Voltage	110-265	V	0.01	< 1%
Current	0,1 - 16	A	0.001	< 1.5%
Frequency	45-65	Hz	0.01	< 0.03%
Phase	-180 - +180	°	0.1	< 1%
Active power	1 - 4000	W	1	< 1.5%
Reactive power	1 - 4000	Var	1	< 1.5%
Apparent power	1 - 4000	VA	1	< 1.5%
Power factor	0 - 1	-	0.01	< 3%
Energy Counter				
Active Energy (total)	9.999.999,999	kWh	0.001	< 1.5%
Active Energy (temporary)	9.999.999,999	kWh	0.001	< 1.5%

1.10. Sensor

One external sensor can be connected to the **LINDY IPower Strip 4**. The following sensors are currently available



Temperature-Sensor 32648 / 32649	
Cable length	≈ 2m
Connector	Mini-DIN
Measurement range	-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)



Humidity/Temperature-Sensor (on request)	
Cable length	≈ 2m
Connector	Mini-DIN
Measurement range	Temp: -20 to +80°C, ±0,5°C (maximum) and ±0,3°C (typical) Humidity: 0-100%, ±3% (maximum) and ±2% (typical)

The sensors are automatically detected after connect. This is indicated by the green "S1" LED on the front panel. The sensor values are displayed at the "Control Panel" web page:

Port	Name	Temperature	24h min	24h max	
1: 7002	Temperature	26,3 °C	24,4 °C	26,3 °C	Reset min/max

Port	Name	Humidity	24h min	24h max	
1: 7002	Humidity	32,3 %	31,3 %	33,6 %	Reset min/max

2. Operating

2.1. Operating the device directly

Port Switching

The current status of the output is indicated by the color of the LED. Red indicates that the output is off, green shows that the output is on. On the device are the buttons "select" and "ok". If you press "select", the LED will blink for the first output, ie the output is selected. Press "**select**" again to select the next output. Hold down the button "ok" for two seconds, then the status of the selected output is toggled.

Display Information

If no port is selected manually, repeatedly pressing the "ok" key will show the IP-address and the values of the external sensors on the display.

2.2. Control Panel

Access the web interface: <http://IP-address> and log-in.

The screenshot shows a web interface with a navigation bar containing 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. The main content area is divided into two columns: 'Bank A' and 'Bank B'. Each bank contains six power ports, each with a red 'OFF' indicator and a label (e.g., 'A1: Power Port'). Below the ports, both banks show 'OVP operational'. At the bottom, there is a table with energy measurement data and a 'show details' checkbox.

Line Id	Name	Voltage AC rms V	Current AC rms A	Freq Hz	Phase °	Power				total Energy active kWh	resettable Energy		
						active W	reactive VAR	apparent VA	PF		active kWh	time h:m:s	
A	Meter-A	195,5	0,002	49,98	-39,3	0	0	0	0,00	0,196	0,055	2w 4d 00:33:17	Reset
B	Meter-B	196,1	0,002	49,98	-17,9	0	-1	0	0,01	0,197	0,072	2w 5d 21:35:42	Reset
sum			0,004			0				0,393	0,127		

show details

The web page provides an overview of the switching state, energy measurement values, as well as the external sensors, provided that they are connected. When a single port is clicked at the **LINDY IPower Strip 4**, a panel with buttons to control a single port appear:

The screenshot shows a control panel for a single port. It features a red 'OFF' indicator, the label '1: Power Port', and five buttons: 'On', 'Off', 'Reset', 'Batch', and 'Close'.

The Port icon is green when the relay is closed, or red in the open state. An additional small clock icon indicates that a timer is active. Timer can be activated by delay, reset or batch mode.



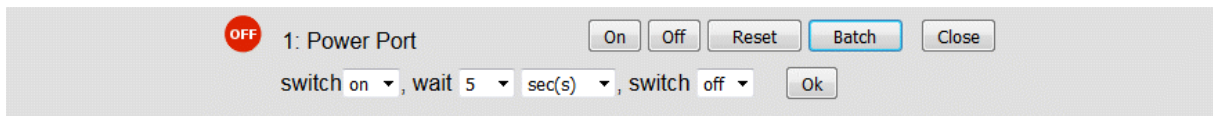
An activated Watchdog is represented by an eye icon. An "X" means, that the address that should be observed, could not be resolved. Two circular arrows show a booting status.



The ports can be switched manually with the "On" and "Off" buttons. If the port is turned on, it can be turned off by pressing the "Reset" button, until after a delay it turns itself on again. The delay time is determined by the parameter Reset Duration, which is described in the chapter "[Configuration - Power Ports](#)". The "Close" button dissolves the panel again.

Batchmode

Each individual port can be set for a selectable period of time to the state "switch on" or "switch off". After the selected time they are automatically switched to the second preselected state.



Optionally the device can be switched via a Perl script or external tools like wget.

2.3. Maintenance Functions

This section provides access to important functions such as Firmware Update or Restart Device. It is advisable to set an HTTP password for this reason.


The screenshot shows a web interface with a navigation bar at the top containing four tabs: "Control Panel", "Configuration", "Maintenance" (which is active), and "Logout". Below the navigation bar, the "Maintenance" section is displayed within a light gray border. It contains three distinct functional areas, each enclosed in a rounded rectangle:

- Firmware Update:** This area features a "Browse..." button followed by the text "No file selected." and an "Upload" button.
- SSL Certificate Upload:** This area features a "Browse..." button followed by the text "No file selected." and an "Upload" button.
- Restart / Fab-Settings:** This area contains four buttons: "Restart Device", "Restore Fab Settings and Restart Device", "Enter Bootloader Mode", and "Flush DNS Cache".

Firmware Update: Start a firmware update.

SSL Certificate Upload: Saves your own SSL certificate. See chapter "[SSL](#)" for the generation of a certificate in the right format.

Restart Device: Restarts the device without changing the status of the relays.

 Some functions such as a firmware update or changing of the IP-address and HTTP settings require a restart of the device.

Restore Fab Settings and Restart Device: Performs a restart and resets the device to factory default.

Enter Bootloader Mode: Jumps into bootloader mode, where additional settings can be made with GBL_Conf.exe.

Flush DNS Cache: All entries in the DNS cache are discarded and address resolutions are requested again.

3. Configuration

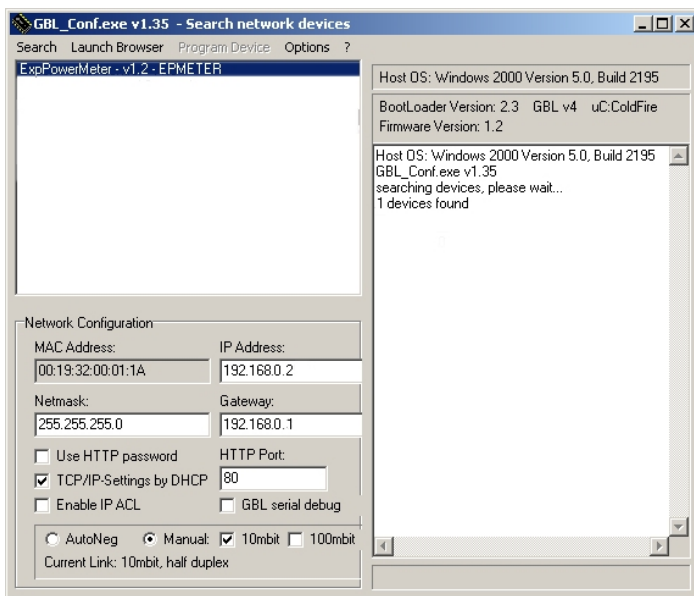
TCP/IP configuration by DHCP

After switching on the device is scanning on the Ethernet for a DHCP server and requests an unused IP address. Check the IP address that has been assigned and adjust if necessary, that the same IP address is used at each restart. To turn off DHCP use the software GBL_Conf.exe or use the configuration via the web interface.

To check the network settings with GBL_Conf.exe, start the program and choose "All Devices" in the "Search" menu. From the list select the appropriate device. The lower part of the left half of the window now shows the current network settings of the device. If the IP address is displayed with the default settings (192.168.0.2), either no DHCP server is present on the network, or there could be no free IP address assigned to it.

3.1. Configuration by Software

To view and change the network settings, you can use the program GBL_Conf.exe. The program is available for free on our website www.Lindy.de. You can also use GBL_Conf.exe to install firmware updates and trigger a [reset to factory](#) defaults.



Interface GBL_Conf

To check the network settings with GBL_Conf.exe, start the program and choose "All Devices" in the "Search" menu. From the list select the appropriate device. The lower part of the left half of the window now shows the current network settings of the device. If the IP address is displayed with the default settings (192.168.0.2), either no DHCP server is present on the network, or there could be no free IP address assigned to it.

- Activate the Bootloader Mode (see Chapter Bootloader Mode) and choose in menu "Search" the item "Bootloader-Mode Devices only"
- Enter the desired settings in the edit window and save them with "Save Config".
- Deactivate the boot loader mode for the changes to take effect. Select again "All Devices" in the "Search" menu of GBL_Conf.exe.
The new network configuration is now displayed.

3.2. Configuration via Webinterface

Access the web interface: `http://IP-address` and log-in.

Use the "Configuration" Tab to enter the configuration menu.

3.2.1. Power Ports

Choose Power Port to configure: This field is used to select the power ports to be configured.

Label: You can assign a name up to 15 characters for each of the power ports. Using the name, an identification of the the device connected to the port can be facilitated.

Start-up Monitoring

It is important, that if necessary the condition of the power ports can be restored after a power failure. Therefore each port can be configured with Initialization status to a specific start-up state. This start-up sequence can be carried out delayed by the parameter Initialization Delay. There is in any case a minimum one-second delay between switching of ports.

Initialization status(coldstart): This is the port state (on, off, remember last state) the port should be set when the device is turned on. The setting "remember last state" saves the last manually set state of the power port in the EEPROM.

Initialization delay: Here can be configured how long the port should wait to switch to its defined state after the device is turned on. The delay may last up to 8191 seconds. This corresponds to a period of approx. two hours and 20 minutes. A value of zero means that the initialization is off.

Repower delay: When this feature is enabled (value greater than 0), the power port will switch itself on again a specified time after it has been disabled. Unlike the "Reset" button this function applies to all switch actions, including SNMP, or an optional serial interface.

Reset Duration: When the "Reset" button is triggered, the device turns the power port off, waits for the time entered here (in seconds) and turns the power port on.

3.2.2. Watchdog

The watchdog feature enables to monitor various remote devices. Therefore either ICMP pings or TCP pings are sent to the device to be monitored. If these pings are not answered within a certain time (both the time and the number of attempts can be set), the port is reset. This allows e.g. to automatically restart not responding server or NAS systems.

When a watchdog is activated it presents various information in the Control Panel. The information is color-coded.

- Green text: The watchdog is active and regularly receives ping replies.
- Orange text: The watchdog is currently enabled, and waits for the first Ping response.
- Red text: The watchdog is active and receives no ping replies anymore from the configured IP address.

After the watchdog has been enabled, the display remains orange until the watchdog receives a ping response for the first time. Only then the watchdog is activated. Even after triggering a watchdog and a subsequent power port reset, the display will remain orange until the device is rebooted and responds again to ping requests. This will prevent a premature watchdog reset of the port, e.g. when a server needs a long time for a file check.

You can monitor devices on your own network, as well as devices on an external network, e.g. the operating status of a router.

The screenshot shows the 'Power Ports' configuration page. At the top, there are navigation tabs: 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. Below these are links for 'Power Ports', 'IP Address', 'IP ACL', 'HTTP', 'Sensors', 'SNMP', 'Syslog', and 'E-Mail'. The main configuration area is titled 'Power Ports' and contains the following settings:

- Choose Power Port to configure: 1: Power Port (dropdown menu)
- Label: Power Port (text input)
- Initialization status (coldstart): on off remember last state
- Initialization delay: 0 s (text input)
- Repower delay: 0 s (text input)
- Reset duration: 10 s (text input)
- Enable watchdog: yes no
 - Watchdog action: reset off
 - Watchdog type: ICMP TCP
 - Hostname: (text input)
 - Ping interval: 10 s (text input)
 - Ping retries: 6 (text input)
 - retry BOOTING after RESET failure: no yes

An 'Apply' button is located at the bottom of the configuration area.

Enable watchdog: Enables the watchdog function for this Power Port.

Watchdog action: When selecting *reset*, the Port will be turned off and switched on again after a Reset Duration. The setting *off* leaves the Port in the off state.

Watchdog type: Here you can choose between the monitoring by ICMP pings or TCP pings.

- ICMP Pings: The classic ping (ICMP echo request). It can be used to check the accessibility of network devices (for example, a server).
- TCP Pings: With TCP pings, you can check if a TCP port on the target device would accept a TCP connect. Therefore a non-blocked TCP port should be selected. A good choice would be port 80 for http or port 25 for SMTP.

Hostname: The name or IP address of the monitored network device.

TCP port: Enter the TCP port to be monitored. When using ICMP pings this is not needed.

Ping interval: Select the frequency (in seconds) at which the ping packet is sent to each network device to check its operating status.

Ping retries: After this number of consecutive unanswered ping requests the device is considered inactive.

retry BOOTING after RESET failure: !!! Be careful, only switch this setting to "yes", if the appliance to be monitored never requires a long boot time !!!

Normally (this option no selected) the watchdog monitors the connected device. When the watchdog is activated, because the device is not answering, the pre-selected watchdog action is executed. Now the watchdog waits until the monitored device is answering to pings again. After this the watchdog is armed again. When you select the option retry BOOTING after RESET failure, the watchdog is armed **directly** after the watchdog action is executed.

This option has the following pitfall: If at the Port to be monitored a server connected, that is in need for a long boot process, because it is doing a file system check, the server would probably exceed the tripping time of the watchdog. The server would be switched off and on again, and the file system check is restarted. This would be repeated endlessly.

retry Boot after N ping timeouts: If retry BOOTING after RESET failure is enabled, the device waits N Ping intervals until the connected device is switched off and on again.

• Enable watchdog:	<input checked="" type="radio"/> yes <input type="radio"/> no
• Watchdog action:	<input checked="" type="radio"/> reset <input type="radio"/> off
• Watchdog type:	<input checked="" type="radio"/> ICMP <input type="radio"/> TCP
• Hostname:	<input type="text"/>
• Ping interval:	<input type="text" value="10"/> s
• Ping retries:	<input type="text" value="6"/>
• retry BOOTING after RESET failure:	<input type="radio"/> no <input checked="" type="radio"/> yes
• retry Boot after N ping timeouts:	<input type="text" value="10"/>

3.2.3. IP Address

Control Panel
Configuration
Maintenance
Logout

Power Ports
[IP Address](#)
[IP ACL](#)
[HTTP](#)
[Sensors](#)
[SNMP](#)
[Syslog](#)
[E-Mail](#)

Configuration - IP

• Hostname:

IPv4

• IPv4 Address:

• IPv4 Netmask:

• IPv4 Gateway address:

• IPv4 DNS address:

• Use IPv4 DHCP: yes no

IPv6

• Use IPv6 Protocol: yes no

• Use IPv6 Neighbor Discovery + SLAAC: yes no

• Use DHCP v6: yes no

• Current IPv6 address(es):

Hostname: Here you can enter a name with up to 15 characters. This name will be used for registration on the DHCP server.



Special characters and umlauts can cause problems in the network.

IP Address: The IP address of the device.

Netmask: The network mask used in the network.

Gateway address: The IP address of the gateway.


Use DHCP: Select "yes" if the TCP/IP settings should be obtained directly from the DHCP server: When the function is selected, each time the device powers up it is checked if a DHCP server is available on the network. If not, the last used TCP/IP setting will be used further.

Use IPv6 Protocol: Activates IPv6 usage.

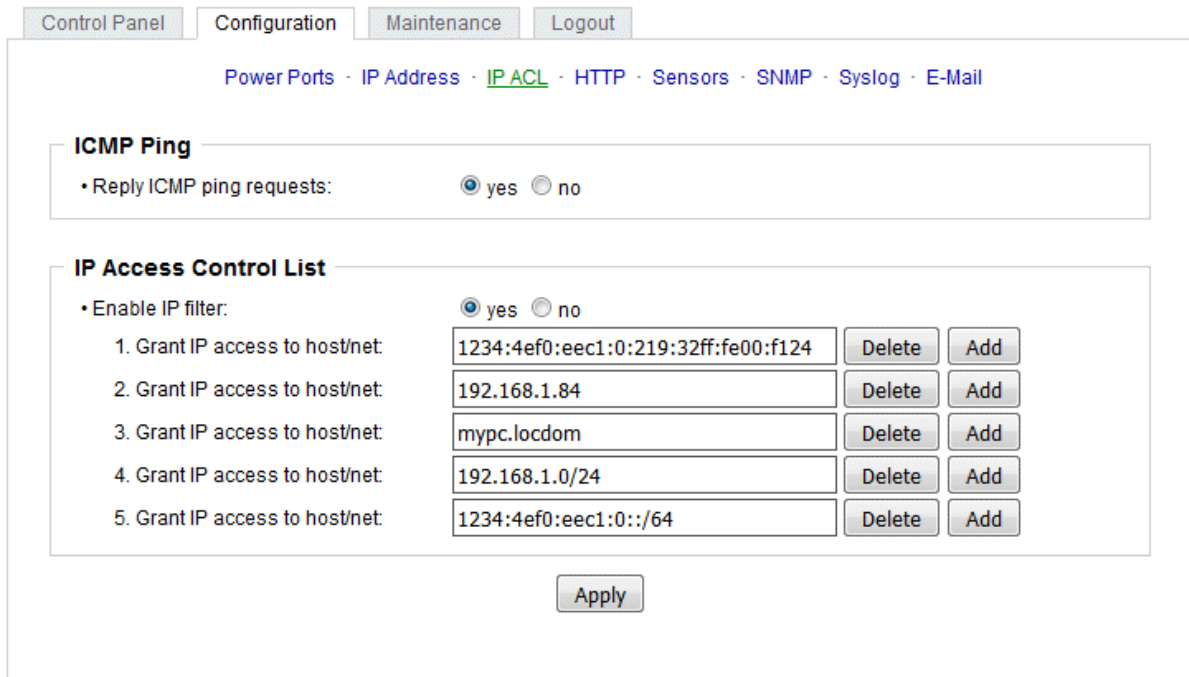
Use IPv6 Neighbor Discovery + SLAAC: The "Stateless Address Auto Vonfiguration" communicates with the router to make the global IPv6 address available.

Use DHCP v6: Requests from an existing DHCPv6 server addresses of the configured DNS server.

Current IPv6 adresse(s): Displays the IPv6 addresses over which the device can be accessed.

 For IP changes a firmware reset is required. This can be done in the Maintenance web page.

3.2.4. IP ACL



The screenshot shows a web interface with a navigation bar at the top containing 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. Below the navigation bar is a breadcrumb trail: 'Power Ports · IP Address · IP ACL · HTTP · Sensors · SNMP · Syslog · E-Mail'. The main content area is divided into two sections:


- ICMP Ping**: A section with a label 'Reply ICMP ping requests:' and two radio buttons, 'yes' (selected) and 'no'.
- IP Access Control List**: A section with a label 'Enable IP filter:' and two radio buttons, 'yes' (selected) and 'no'. Below this is a table with five rows, each representing a grant of IP access. Each row has a text input field for the host/net, a 'Delete' button, and an 'Add' button.


Grant IP access to host/net:	Host/Net	Delete	Add
1. Grant IP access to host/net:	1234:4ef0:eec1:0:219:32ff:fe00:f124	Delete	Add
2. Grant IP access to host/net:	192.168.1.84	Delete	Add
3. Grant IP access to host/net:	mypc.locdom	Delete	Add
4. Grant IP access to host/net:	192.168.1.0/24	Delete	Add
5. Grant IP access to host/net:	1234:4ef0:eec1:0::/64	Delete	Add

At the bottom of the IP Access Control List section is an 'Apply' button.

Reply ICMP ping requests: If you enable this feature, the device responds to ICMP pings from the network.

Enable IP filter: Enable or disable the IP filter here. The IP filter represents an access control for incoming IP packets.

 Please note that when IP access control is enabled HTTP and SNMP only work if the appropriate servers and clients are registered in the IP access control list.

 If you choose a wrong IP ACL setting and locked yourself out, please activate the Bootloader Mode and use GBL_Conf.exe to deactivate the IP ACL. Alternatively, you can reset the device to factory default.

3.2.5. HTTP

Control Panel
Configuration
Maintenance
Logout

Power Ports
IP Address
IP ACL
HTTP
Sensors
SNMP
Syslog
E-Mail

HTTP

- HTTP Server option: HTTP + HTTPS HTTPS only HTTP only
- Server port HTTP:
- Server port HTTPS:
- Enable Ajax autorefresh: yes no

HTTP Password


- Enable password protection: yes no
- Set new **admin** password: (32 characters max)
Repeat **admin** password:
- Set new **user** password: (32 characters max)
Repeat **user** password:

HTTP Server option: Selects whether access is possible only with HTTP, HTTPS, or both.


HTTP port: Here can be set the port number of the internal HTTP. Possible values are from 1 to 65534 (default: 80). If you do not use the default port, you must append the port number to the address with a colon to address the device from a web browser. Such as: "http://192.168.0.2:800"

Server port HTTPS: The port number to connect the web server via the SSL (TLS) protocol.

Enable password protection: If desired, a http password protection can be enabled. In this case, an admin password and a user password have to be assigned. The passwords can have up to 31 characters. User can log in by entering the user's password to query the status information and make changes to ports (if applicable). Admins have the privileges of a User and can change the Configuration settings. In the username field of the password input mask the names "admin" and "user" are supported. In the factory defaults the password for the admin is set to "admin" resp. "user" for the user password.

 If the password mask is redisplayed, only four "bullets" are shown as a symbolic placeholder, since for security reasons the device never stores the password itself, but only the SHA2-256 hash. If you want to change a password, the complete password must always be re-entered.

Enable Ajax autorefresh: If this is activated, the information of the status page is automatically updated via http request (AJAX).

 If you have forgotten your password, please activate the bootloader mode and then turn off the password prompt in GBL_Conf.exe.

3.2.6. Sensors

Control Panel
Configuration
Maintenance
Logout

Power Ports
IP Address
IP ACL
HTTP
Sensors
SNMP
Syslog
E-Mail

Internal Sensors

- Choose power meter:
- Power meter name:
- Generate AC current messages: yes no
 - Maximum value: A
 - Minimum value: A
 - Hysteresis: A

External Sensors

- Choose sensor port:
- Sensor name:
- Generate messages: yes no
 - Maximum value: °C
 - Minimum value: °C
 - Hysteresis: °C
- Min/Max measurement period:

Display

- Default display:

Choose power meter: Selects the measurement channel (only one for the **LINDY IPower Strip 4**).

Power meter name: The configurable name that will be displayed on the overview page under "Line Name".

Generate AC current messages: Enables the generation of AC current messages.

Maximum/Minimum value: Adjustable limits for current levels (high and low), which sends alerts via SNMP traps, syslog or e-mail.

Hysteresis: This describes the margin of when an event is generated after the measured value has crossed the chosen limit.

Choose sensor port: Selects a type of sensor to configure it. The first digit "1" indicates the number of the sensor port (only important for devices with more than one sensor port). This is followed by the sensor name (e.g. 7002 for the hybrid sensor), a letter for the sub-type sensor and the changeable sensor name. The sensor subtypes are defined as: "T" = temperature, "H" = humidity, "I" = sensor input.

Sensor Name: Changeable name for this sensor. Temperature and humidity can have different names, even if they are from the same sensor.

Generate messages: Enables the generation of sensor messages.

Maximum/Minimum value: Here you can choose whether, and at what Maximum/Minimum temperature or humidity measurements limits the alerts are send via SNMP traps, syslog or email.

Hysteresis: This describes the margin of when an event is generated after the measured value has crossed the chosen limit.

Min/Max measurement period: Selects the time range for the sensor min/max values on the overview web page.

Default Display: Selects whether the power (Current) is shown in the LED display, or the value of an external sensor.

Hysteresis Example:

A Hysteresis value prevents that too much messages are generated, when a sensor value is jittering around a sensor limit. The following example shows the behavior for a temperature sensor and a hysteresis value of "1". An upper limit of "50 °C" is set.

Example:

49.9 °C - is below the upper limit

50.0 °C - a message is generated for reaching the upper limit

50.1 °C - is above the upper limit

...

49.1 °C - is below the upper limit, but in the hysteresis range

49.0 °C - is below the upper limit, but in the hysteresis range

48.9 °C - a message is generated for underrunning the upper limit inclusive hysteresis range

...

3.2.7. SNMP

Control Panel
Configuration
Maintenance
Logout

[Power Ports](#) · [IP Address](#) · [IP ACL](#) · [HTTP](#) · [Sensors](#) · [SNMP](#) · [Syslog](#) · [E-Mail](#)

SNMP

• Enable SNMP options: SNMP get SNMP set

SNMP v2

• Enable SNMP v2: yes no

• SNMP v2 public Community: (16 char. max)

• SNMP v2 private Community: (16 char. max)

SNMP v3

• Enable SNMP v3: yes no

• SNMP v3 Username: (32 char. max)

• SNMP v3 Authorization Algorithm:

• Set new **Authorization** password: (8 char. min, 32 char. max)

Repeat **Authorization** password:

• SNMP v3 Privacy Algorithm:

• Set new **Privacy** password: (8 char. min, 32 char. max)

Repeat **Privacy** password:

SNMP Traps

• send SNMP Traps


• SNMP trap receiver 1:

[MIB table](#)

SNMP-get: Enables the acceptance of SNMP-GET commands.

SNMP-set: Allows the reception of SNMP-SET commands.

Enable SNMP v2: Activates SNMP v2.

 Because of security issues, it is advisable to use only SNMP v3, and to disable SNMP v2. Accesses to SNMP v2 are always insecure.

Community public: The community password for SNMP GET requests.


Community private: The community password for SNMP SET requests.


Enable SNMP v3: Activates SNMP v3.

SNMP v3 Username: The SNMP v3 User Name.

SNMP v3 Authorization Algorithm: The selected Authentication Algorithm.

SNMP v3 Privacy Algorithm: SNMP v3 Encryption Algorithm..

 If the password mask is redisplayed, only four "bullets" are shown as a symbolic placeholder, since for security reasons the device never stores the password itself, but only the key formed using the Authorization Algorithm. If you want to change a password, the complete password must always be re-entered.

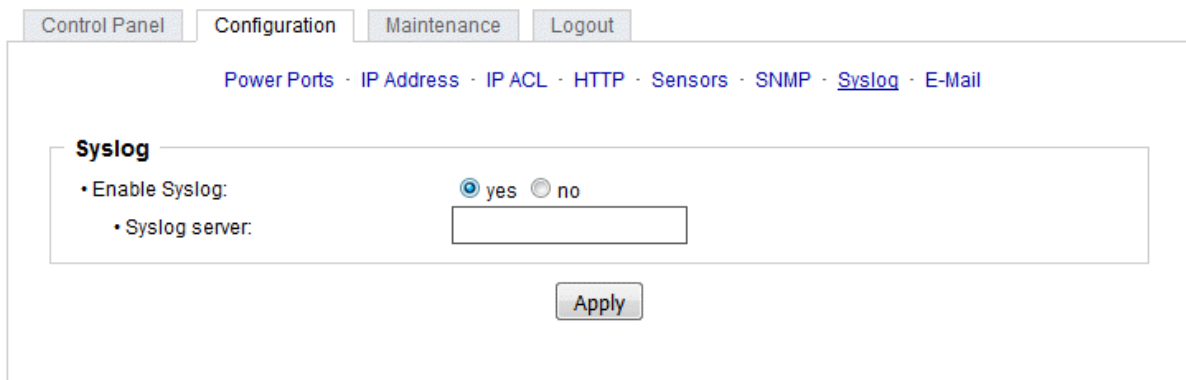
 The calculation of the password hashes varies with the selected algorithms. If the Authentication or Privacy algorithms are changed, the passwords must be re-entered in the configuration dialog.

MIB table: The download link to the text file with the MIB table for the device.

Send SNMP traps: Here you can specify whether, and in what format the device should send SNMP traps.

SNMP trap receiver: You can insert here up to eight SNMP trap receiver.

3.2.8. Syslog



The screenshot shows a web interface for configuring Syslog. At the top, there are navigation tabs: Control Panel, Configuration, Maintenance, and Logout. Below these, a breadcrumb trail reads: Power Ports · IP Address · IP ACL · HTTP · Sensors · SNMP · Syslog · E-Mail. The main content area is titled "Syslog" and contains two configuration items: "Enable Syslog:" with radio buttons for "yes" (selected) and "no", and "Syslog server:" with an empty text input field. An "Apply" button is located at the bottom center of the configuration area.

Enable Syslog: Enables the usage of Syslog Messages.

Syslog Server: If you have enabled Syslog Messages, enter the IP address of the server to which the syslog information should be transmitted.

3.2.9. E-Mail

Control Panel
Configuration
Maintenance
Logout

[Power Ports](#) · [IP Address](#) · [IP ACL](#) · [HTTP](#) · [Sensors](#) · [SNMP](#) · [Syslog](#) · [E-Mail](#)

E-Mail

- Enable E-Mail: yes no
- Sender address:
- Recipient address:
- SMTP server:
- SMTP server port: (Default: 587)
- SMTP Connection Security:

Authentication

- SMTP Authentication (password):
- Username:
- Set new password:
- Repeat password:

Enable E-Mail: Activates the email dispatch of messages.

Sender address: The e-mail address of the sender.

Recipient address: The e-mail address of the recipient.

SMTP Server: The SMTP IP-address of the e-mail server. Either as FQDN, e.g: "mail.gmx.net", or as IP-address, e.g: "213.165.64.20". If required, attach a designated port, e.g: "mail.gmx.net:25".

SMTP server port: The port address of the email server. In the normal case this should be the same as the default, that is determined by the setting SMTP Connection Security.

SMTP Connection Security: Transmission via SSL or no encryption.

SMTP Authentication (password): Authentication of the E-Mail Server.

Username: User name that is registered with the SMTP E-Mail server.

Set new password: Enter the password for the login to the e-mail server.

Repeat password: Enter the password again to confirm it.



If the password mask is redisplayed, only four "bullets" are shown as a symbolic placeholder, since for security reasons the password is never shown itself. If you want to change a password, the complete password must always be re-entered.

E-Mail Logs: Logging of E-Mail system messages.

4. Specifications


4.1. IP ACL

IP Access Control List

The IP Access Control List (ACL IP) is a filter for incoming IP packets. If the filter is active, only the hosts and subnets whose IP addresses are registered in the list, can contact via HTTP or SNMP, and make changes. For incoming connections from unauthorized PCs, the device is not completely transparent. Due to technical restraints, a TCP/IP connection will be accepted at first, but then rejected directly.

Examples:

Entry in the IP ACL	Meaning
192.168.0.123	the PC with IP Address "192.168.0.123" can access the device
192.168.0.1/24	all devices of subnet "192.168.0.1/24" can access the device
1234:4ef0:eec1:0::/64	all devices of subnet "1234:4ef0:eec1:0::/64" can access the device

 If you choose a wrong IP ACL setting and locked yourself out, please activate the Bootloader Mode and use GBL_Conf.exe to deactivate the IP ACL. Alternatively, you can reset the device to factory default.

4.2. IPv6

IPv6 Addresses

IPv6 addresses are 128 bit long and thus four times as long as IPv4 addresses. The first 64 bit form a so-called prefix, the last 64 bit designate a unique interface identifier. The prefix is composed of a routing prefix and a subnet ID. An IPv6 network interface can be reached under several IP addresses. Usually this is the case under a global address and the link local address.

Address Notation

IPv6 addresses are noted in 8 hexadecimal blocks at 16 bit, while IPv4 normally is noted in decimal. The separator is a colon, not a period.

E.g.: 1234:4ef0:0:0:0019:32ff:fe00:0124

Leading zeros may be omitted within a block. The previous example can be rewritten as:

1234:4ef0:0:0:19:32ff:fe00:124

One may omit one or more successive blocks, if they consist of zeros. This may be done only once within an IPv6 address!

1234:4ef0::19:32ff:fe00:124

One may use the usual decimal notation of IPv4 for the last 4 bytes:

1234:4ef0::19:32ff:254.0.1.36

4.3. SNMP

SNMP can be used for status information via UDP (port 161). Supported SNMP commands are:

- GET
- GETNEXT
- GETBULK
- SET

To query via SNMP you need a Network Management System, such as HP OpenView, OpenNMS, Nagios etc., or the simple command line tools of NET-SNMP software. The device supports SNMP protocols v1, v2c and v3. If traps are enabled in the configuration, the device messages are sent as notifications (traps). SNMP Informs are not supported. SNMP Requests are answered with the same version with which they were sent. The version of the sent traps can be set in the configuration.

MIB Tables

The values that can be requested or changed by the device, the so-called "Managed Objects", are described in Management Information Bases (MIBs). These substructures are subordinate to so-called "OID" (Object Identifiers). An OID digit signifies the location of a value inside a MIB structure. Alternatively, each OID can be referred to with its symbol name (subtree name). The device's MIB table can be displayed as a text file by clicking on the link "MIB table" on the SNMP configuration page in the browser.

SNMP v1 and v2c

SNMP v1 and v2c authenticates the network requests by so-called communities. The SNMP request has to send along the so-called community public for queries (read access) and the community private for status changes (write access). The SNMP communities are read and write passwords. In SNMP v1 and v2 the communities are transmitted unencrypted on the network and can be easily intercepted with IP sniffers within this collision domain. To enforce limited access we recommend the use of DMZ or IP-ACL.

SNMP v3

Because the device has no multiuser management, only one user (default name "standard") is detected in SNMP v3. From the User-based Security Model (USM) MIB variables, there is a support of "usmStats ..." counter. The "usmUser ..." variables will be added with the enhancement of additional users in later firmware versions. The system has only one context. The system accepts the context "normal" or an empty context.

Authentication

The algorithms "HMAC-MD5-96" and "HMAC-SHA-96" are available for authentication. In addition, the "HMAC-SHA-2" variants (RFC7630) "SHA-256", "SHA-384" and "SHA-512" are implemented. Since RFC7630 is very new, there are no clients yet with which the "HMAC-SHA-2" implementation could be adequately tested.

The methods "DES", "3DES", "AES-128", "AES-192" and "AES-256" are supported in combination with "HMAC-MD5-96" and "HMAC-SHA-96." For the "HMAC-SHA-2" protocols, there is currently neither RFC nor draft that will allow for cooperation with an encryption.

Passwords

The passwords for authentication and encryption are stored only as computed hashes for security reasons. Thus it is, if at all, very difficult to infer the initial password. However, the hash calculation changes with the set algorithms. If the authentication or privacy algorithms are changed, the passwords must be re-entered in the configuration dialog.

Security

The following aspects should be considered:

- If encryption or authentication is used, then SNMP v1 and v2c should be turned off. Otherwise the device could be accessed with it.
- If only authentication is used, then the new "HMAC-SHA-2" methods are superior to the MD5 or SHA-1 hashing algorithms.
- For SHA-1, there are a little less attack scenarios than MD5. If in doubt, SHA-1 is preferable.
- Encryption "DES" is considered very unsafe, use only in an emergency for reasons of compatibility!
- For cryptologists it's a debatable point whether "HMAC-MD5-96" and "HMAC-SHA-96" can muster enough entropy for key lengths of "AES-192" or "AES-256".
- From the foregoing considerations, we would recommended at present "HMAC-SHA-96" with "AES-128" as authentication and encryption method.

NET-SNMP

[NET-SNMP](#) provides a very widespread collection of SNMP command-line tools (snmpget, snmpset, snmpwalk etc.) NET-SNMP is among others available for Linux and Windows. After installing NET-SNMP you should create the device-specific MIB of the device in NET-SMP share directory, e.g. after

```
c:\usr\share\snmp\mibs
```

or

```
/usr/share/snmp/mibs
```

So later you can use the 'subtree names' instead of OIDs:

```
Name: snmpwalk -v2c -mALL -c public 192.168.1.232 gudeads  
OID: snmpwalk -v2c -mALL -c public 192.168.1.232 1.3.6.1.4.1.28507
```

NET-SNMP Examples

Query Power Port 1 switching state:

```
snmpget -v2c -mALL -c public 192.168.1.232 epc1202PortState.1
```

Switch on Power Port 1:

```
snmpset -v2c -mALL -c private 192.168.1.232 epc1202PortState.1 integer 1
```

4.3.1. Device MIB

Below is a table of all device-specific OID 's which can be accessed via SNMP. In the numerical representation of the OID the prefix " 1.3.6.1.4.1.28507 " (Gude Enterprise OID) was omitted at each entry in the table to preserve space. The example for a complete OID would be "1.3.6.1.4.1.28507.43.1.1.1.1". A distinction is made in SNMP OID 's in between tables and scalars. OID scalar have the extension ".0" and only specify a value. In SNMP tables the "x" is replaced by an index (1 or greater) to address a value from the table.

Name	OID	Type	Acc.
epc1202TrapCtrl	.43.1.1.1.1.0 0 = off 1 = Ver. 1 2 = Ver. 2c 3 = Ver. 3	Integer32	RW
epc1202TrapIIndex	.43.1.1.1.2.1.1.x A unique value, greater than zero, for each receiver slot.	Integer32	RO
epc1202TrapAddr	.43.1.1.1.2.1.2.x DNS name or IP address specifying one Trap receiver slot. A port can optionally be specified: 'name:port' An empty string disables this slot.	OCTETS	RW
epc1202portNumber	.43.1.3.1.1.0 The number of Relay Ports	Integer32	RO
epc1202PortIndex	.43.1.3.1.2.1.1.x A unique value, greater than zero, for each Relay Port.	Integer32	RO
epc1202PortName	.43.1.3.1.2.1.2.x A textual string containing name of a Relay Port.	OCTETS	RO
epc1202PortState	.43.1.3.1.2.1.3.x current state a Relay Port	INTEGER	RW
epc1202PortSwitchCount	.43.1.3.1.2.1.4.x The total number of switch actions occurred on a Relay Port. Does not count switch commands which will not switch the relay state, so just real relay switches are displayed here.	Integer32	RO
epc1202PortStartupMode	.43.1.3.1.2.1.5.x set Mode of startup sequence (off, on , remember last state)	INTEGER	RW
epc1202PortStartupDelay	.43.1.3.1.2.1.6.x Delay in sec for startup action	Integer32	RW
epc1202PortRepowerTime	.43.1.3.1.2.1.7.x Delay in sec for repower port after switching off	Integer32	RW
epc1202ActivePowerChan	.43.1.5.1.1.0 Number of supported Power Channels.	Unsigned32	RO
epc1202PowerIndex	.43.1.5.1.2.1.1.x Index of Power Channel entries	Integer32	RO
epc1202ChanStatus	.43.1.5.1.2.1.2.x 0 = data not active, 1 = data valid	Integer32	RO
epc1202AbsEnergyActive	.43.1.5.1.2.1.3.x Absolute Active Energy counter.	Gauge32	RO
epc1202PowerActive	.43.1.5.1.2.1.4.x Active Power	Integer32	RO
epc1202Current	.43.1.5.1.2.1.5.x Actual Curent on Power Channel.	Gauge32	RO
epc1202Voltage	.43.1.5.1.2.1.6.x Actual Voltage on Power Channel	Gauge32	RO
epc1202Frequency	.43.1.5.1.2.1.7.x Frequency of Power Channel	Gauge32	RO
epc1202PowerFactor	.43.1.5.1.2.1.8.x Power Factor of Channel between -1.0 and 1.00	Integer32	RO
epc1202Pangle	.43.1.5.1.2.1.9.x Phase Angle between Voltage and L Line Current between -180.0 and 180.0	Integer32	RO
epc1202PowerApparent	.43.1.5.1.2.1.10.x L Line Mean Apparent Power	Integer32	RO
epc1202PowerReactive	.43.1.5.1.2.1.11.x L Line Mean Reactive Power	Integer32	RO
epc1202AbsEnergyReactive	.43.1.5.1.2.1.12.x Absolute Reactive Energy counter.	Gauge32	RO
epc1202AbsEnergyActiveResettable	.43.1.5.1.2.1.13.x Resettable Absolute Active Energy counter. Writing '0' resets all resettable counter.	Gauge32	RW
epc1202AbsEnergyReactiveResettable	.43.1.5.1.2.1.14.x Resettable Absolute Reactive Energy counter.	Gauge32	RO
epc1202ResetTime	.43.1.5.1.2.1.15.x Time in seconds since last Energy Counter reset.	Gauge32	RO
epc1202ForwEnergyActive	.43.1.5.1.2.1.16.x Forward Active Energy counter.	Gauge32	RO
epc1202ForwEnergyReactive	.43.1.5.1.2.1.17.x Forward Reactive Energy counter.	Gauge32	RO
epc1202ForwEnergyActiveResettable	.43.1.5.1.2.1.18.x Resettable Forward Active Energy counter.	Gauge32	RO

epc1202ForwEnergyReactiveResettable	Resettable Forward Reactive Energy counter.	.43.1.5.1.2.1.19.x	Gauge32	RO
epc1202RevEnergyActive	Reverse Active Energy counter.	.43.1.5.1.2.1.20.x	Gauge32	RO
epc1202RevEnergyReactive	Reverse Reactive Energy counter.	.43.1.5.1.2.1.21.x	Gauge32	RO
epc1202RevEnergyActiveResettable	Resettable Reverse Active Energy counter.	.43.1.5.1.2.1.22.x	Gauge32	RO
epc1202RevEnergyReactiveResettable	Resettable Reverse Reactive Energy counter.	.43.1.5.1.2.1.23.x	Gauge32	RO
epc1202OVPIIndex	None	.43.1.5.2.1.1.x	Integer32	RO
epc1202OVVPStatus	shows the status of the built-in Overvoltage Protection	.43.1.5.2.1.2.x	INTEGER	RO
epc1202SensorIndex	None	.43.1.6.1.1.1.x	Integer32	RO
epc1202TempSensor	actual temperature, a value of -9999 indicates that data is not available	.43.1.6.1.1.2.x	Integer32	RO
epc1202HygroSensor	actual humidity, a value of -9999 indicates that data is not available	.43.1.6.1.1.3.x	Integer32	RO
epc1202InputSensor	logical state of input sensor	.43.1.6.1.1.4.x	INTEGER	RO

4.4. SSL

TLS Standard

The device is compatible with the standards TLSv1.0 to TLSv1.2. Due to lack of security, SSLv3.0 as well as RC4 and DES encryptions are deactivated.

The following TLS Ciphersuites are supported:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_PSK_WITH_AES_128_GCM_SHA256
- TLS_PSK_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CCM
- TLS_RSA_WITH_AES_256_CCM
- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_AES_256_CCM
- TLS_RSA_WITH_AES_128_CCM_8
- TLS_RSA_WITH_AES_256_CCM_8
- TLS_DHE_RSA_WITH_AES_128_CCM_8
- TLS_DHE_RSA_WITH_AES_256_CCM_8
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Creating your own Certificates

The SSL stack is supplied with a specially newly generated certificate. There is no function to generate the local certificate anew at the touch of a button, since the required random numbers in an embedded device are usually not independent enough. However, you can create new certificates and import them to the device. The server accepts RSA (1024/2048/4096) and ECC (Elliptic Curve Cryptography) certificates.

Usually OpenSSL is used to create an SSL certificate. For Windows for example, there is the light version of Shinning Light Productions. There you open a command prompt, change to the directory "C:\OpenSSL-Win32\bin" and set these environment variables:

```
set openssl_conf=C:\OpenSSL-Win32\bin\openssl.cfg
set RANDFILE=C:\OpenSSL-Win32\bin\.rnd
```


Here are some examples for the generation with OpenSSL:

Creation of a self-signed RSA 2048-bit certificate

```
openssl genrsa -out server.key 2048
openssl req -new -x509 -days 365 -key server.key -out server.crt
```

RSA 2048-bit certificate with Sign Request:

```
openssl genrsa -out server.key 2048
openssl req -new -key server.key -out server.csr
openssl req -x509 -days 365 -key server.key -in server.csr -out server.crt
```

 The server keys should be generated with "openssl genrsa". If in the generated key file it reads only "----- BEGIN PRIVATE KEY -----" and not "----- BEGIN RSA PRIVATE KEY -----", the key is not recognized.

ECC Certificate with Sign Request:

```
openssl ecparam -genkey -name prime256v1 -out server.key
openssl req -new -key server.key -out server.csr
openssl req -x509 -days 365 -key server.key -in server.csr -out server.crt
```

If you have created your key and certificate, both files are concatenated to one file:


Linux:

```
cat server.crt server.key > server.pem
```

Windows:

```
copy server.crt + server.key server.pem
```

The created server.pem can only be uploaded in the maintenance section of the device.

 If several certificates (Intermediate CRT's) should also be uploaded to the device, one should make sure, that firstly the server certificate and secondly the Intermediates are assembled , e.g:

```
cat server.crt IM1.crt IM2.crt server.key > server.pem
```

Performance Considerations

If RSA 4096 certificates are used, the first access to the web server can take 8-10 seconds, because the math unit of the embedded CPU is highly demanded. After that, the parameters are in the SSL session cache, so all other requests are just as fast as with other certificate lengths. For a quick response even on the first access, we recommend RSA 2048-bit certificates that offer adequate security, too.

4.5. Messages

Depending on adjustable events, various messages can be sent from the device. The following message types are supported:

- Sending of e-mails
- SNMP Traps
- Syslog messages

4.5.1. Email

Email messages are triggered by the following events:

- Switching of the Power Ports
- Exceeding of the max / min values of attached sensors
- State change of digital sensor input ports
- Exceeding of max / min values of the measured power consumption
- Condition change of overvoltage protection

4.5.2. SNMP Traps

SNMP Traps are system messages that are sent via the SNMP protocol to different recipients. SNMP traps are triggered by the following events:

- Switching of the Power Ports
- Exceeding of the max / min values of attached sensors
- State change of digital sensor input ports
- Exceeding of max / min values of the measured power consumption
- Condition change of overvoltage protection

4.5.3. Syslog

Syslog messages are simple text messages that are sent via UDP to a syslog server. Under Linux, normally a syslog daemon is already running (eg. syslog-ng), for Microsoft Windows systems some freeware programs are available on the market. The syslog messages are sent for the following events:

- Turning on the device
- Enable/disable of syslog in the configuration
- Switching of the Power Ports
- Exceeding of the max / min values of attached sensors
- State change of digital sensor input ports
- Exceeding of max / min values of the measured power consumption
- Condition change of overvoltage protection

5. Support

You will find the latest product software on our website at www.lindy.de available for download. If you have further questions about installation or operation of the unit, please contact our support team.

5.1. Data Security

To provide the device with a high level of data security, we recommend the following measures:

- Check that the HTTP password is switched on
- Do not use the default HTTP password
- Allow access to HTTP via SSL only
- Authentication and encryption is switched on in SNMPv3
- SNMP v2 access is disabled
- enable STARTTLS or SSL in the email configuration
- In the IP ACL, enter only the devices that require access to HTTP or SNMP

5.2. FAQ

1. What can I do if the device is no longer accessible?

- If the Status LED is red, the device has no connection to the switch. Unplug and plug the Ethernet cable. If the Status LED is still red, try other switches. If one uses no switch, but connects e.g. a laptop directly to the device, make sure you are using a crossover Ethernet cable.
- If the status LED is orange for a longer time after unplugging and plugging the Ethernet cable, then DHCP is configured, but no DHCP server was found in the network. After a timeout, the last IP address is configured manually.
- If there is a physical link (status LED is green) to the device, but you can not access the web server, bring the device into bootloader mode and search for it with [GBL_Conf.exe](#). Then check the TCP-IP parameters and change them if necessary.
- If the device is not found by GBL_Conf.exe in bootloader mode, you can reset the settings to [factory defaults](#) as the last option.

CE Statement

CE Certification

This equipment complies with the requirements relating to Electromagnetic Compatibility Standards EN55022/EN55024 and the further standards cited therein. It must be used with shielded cables only. It has been manufactured under the scope of RoHS compliance.

CE Konformitätserklärung

Dieses Produkt entspricht den einschlägigen EMV Richtlinien der EU für IT-Equipment und darf nur zusammen mit abgeschirmten Kabeln verwendet werden.

Diese Geräte wurden unter Berücksichtigung der RoHS Vorgaben hergestellt.

Die formelle Konformitätserklärung können wir Ihnen auf Anforderung zur Verfügung stellen

LINDY Herstellergarantie – Hinweis für Kunden in Deutschland

LINDY gewährt für dieses Produkt über die gesetzliche Regelung in Deutschland hinaus eine zweijährige Herstellergarantie ab Kaufdatum. Die detaillierten Bedingungen dieser Garantie finden Sie auf der LINDY Website aufgelistet bei den AGBs.

Hersteller / Manufacturer (EU):

LINDY-Elektronik GmbH

Markircher Str. 20

68229 Mannheim

GERMANY

Email: info@lindy.com , T: 0049 (0)621 470050

LINDY Electronics Ltd.

Sadler Forster Way

Teesside Industrial Estate, Thornaby

Stockton-on-Tees, TS17 9JY

United Kingdom

postmaster@lindy.co.uk , T: +44 (0) 1642 754000

Recycling Information



WEEE (Waste of Electrical and Electronic Equipment), Recycling of Electronic Products

Europe, United Kingdom

In 2006 the European Union introduced regulations (WEEE) for the collection and recycling of all waste electrical and electronic equipment. It is no longer allowable to simply throw away electrical and electronic equipment. Instead, these products must enter the recycling process.

Each individual EU member state has implemented the WEEE regulations into national law in slightly different ways. Please follow your national law when you want to dispose of any electrical or electronic products. More details can be obtained from your national WEEE recycling agency.

Germany / Deutschland

Die Europäische Union hat mit der WEEE Richtlinie Regelungen für die Verschrottung und das Recycling von Elektro- und Elektronikprodukten geschaffen. Diese wurden im Elektro- und Elektronikgerätegesetz – ElektroG in deutsches Recht umgesetzt. Dieses Gesetz verbietet das Entsorgen von entsprechenden, auch alten, Elektro- und Elektronikgeräten über die Hausmülltonne! Diese Geräte müssen den lokalen Sammelsystemen bzw. örtlichen Sammelstellen zugeführt werden! Dort werden sie kostenlos entgegen genommen. Die Kosten für den weiteren Recyclingprozess übernimmt die Gesamtheit der Gerätehersteller.

France

En 2006, l'union Européenne a introduit la nouvelle réglementation (DEEE) pour le recyclage de tout équipement électrique et électronique.

Chaque Etat membre de l' Union Européenne a mis en application la nouvelle réglementation DEEE de manières légèrement différentes. Veuillez suivre le décret d'application correspondant à l'élimination des déchets électriques ou électroniques de votre pays.

Italy

Nel 2006 l'unione europea ha introdotto regolamentazioni (WEEE) per la raccolta e il riciclo di apparecchi elettrici ed elettronici. Non è più consentito semplicemente gettare queste apparecchiature, devono essere riciclate. Ogni stato membro dell' EU ha tramutato le direttive WEEE in leggi statali in varie misure. Fare riferimento alle leggi del proprio Stato quando si dispone di un apparecchio elettrico o elettronico.

Per ulteriori dettagli fare riferimento alla direttiva WEEE sul riciclaggio del proprio Stato.



LINDY No 32661

1st Edition, FEB 2016

www.lindy.com