IPower Switch 4 DIN S Pro

User Manual	***English***
Benutzerhandbuch	***Deutsch***
Manuel Utilisateur	***Français***
Manuale	***Italiano***



No. 32662

lindy.com

CE

© LINDY Group - FIRST EDITION (October 2018)

1. Device Description 4

1.1 Security Advice 4

1.2 Content of Delivery 4

1.3 Description 4

1.4 Installation 5

1.4.1 Connection Example 6

1.5 Technical Specifications 7

1.6 Sensor 7

2. Operating 9

2.1 Operating the device directly 9

2.2 Control Panel 10

2.3 Maintenance 11

2.3.1 Maintenance Page 13

2.3.2 Configuration Management 15

2.3.3 Bootloader Activation 16

3. Configuration 18

3.1 Output Ports 18

3.1.1 Watchdog 19

3.2 Input Ports 21

3.3 Ethernet 22

3.3.1 IP Address 22

3.3.2 IP ACL 23

3.3.3 HTTP 24

3.4 Protocols 25

3.4.1 Console 25

3.4.2 Syslog 26

3.4.3 SNMP 27

3.4.4 Radius 28

3.4.5 Modbus TCP 29

3.5 Sensors 30

3.5.1 Port Switching 31

3.6 E-Mail 32

3.7 Front Panel 33

4. Specifications 34

4.1 IP ACL 34

4.2 IPv6 34

4.3 Radius 35

.4 Automated Access..... 35
4.5 SNMP 36
4.5.1 Device MIB 2302 38
4.6 SSL 39
4.7 Console 41
4.7.1 Console Cmd 2302 44
4.8 Modbus TCP 51
4.9 Messages 55

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-maintainable parts. All maintenance has to be performed by factory trained service personnel.
- Connect the device to the mains (230V AC) or to an AC Adaptor (10V to 24V AC, 12V to 28V DC, at 4 watts of power). Under no circumstances should the unit be fed with the mains and the AC Adaptor at the same time!
- 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.
- The device is NOT a toy. It has to be used or stored out or 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.

1.2 Content of Delivery

The package includes:

- **IPower Switch 4 DIN S Pro**
- Lindy QIG

1.3 Description

The **IPower Switch 4 DIN S Pro** can switch 4 different relay outputs and monitor 8 pass- ive signal inputs. The device has the following features:

- 4 switchable, potential-free relay ouputs, switching voltage 230 V AC 16 A / 24 V DC, 10 A
- Relays dispose of high contact reliability also at very small loads
- 8 passive inputs for monitoring NO and NC devices, e.g. door contacts, smoke detectors etc.
- Stop input to switch-off of all relais
- Status and Power-up delay (0...9999 seconds) adjustable individually for each relay port after power blackout
- Programmable turn-on/turn-off sequence
- 4-channel watchdog, an individual watchdog (ICMP/TCP) can be assigned for each relay output
- Operation with 230 V AC or 24 V DC voltage

- Optional sensor for environmental monitoring (temperature, humidity and air pressure)
- Firmware update via Ethernet during operation
- Comfortable configuration by web browser, Windows or Linux tool
- Generation of messages (e-mail, Syslog and SNMP traps) and relay switching depending on input change, resp. external sensors
- IPv6 ready
- HTTP/HTTPS, e-mail (SSL, STARTTLS), DHCP, Syslog
- SNMPv1, v2c, v3 (Get/Traps)
- Modbus TCP Support
- Console Commands with telnet support and serial interface
- TLS 1.0, 1.1, 1.2
- IP Access Control List
- Low internal power consumption
- Developed and manufactured in Germany

1.4 Installation



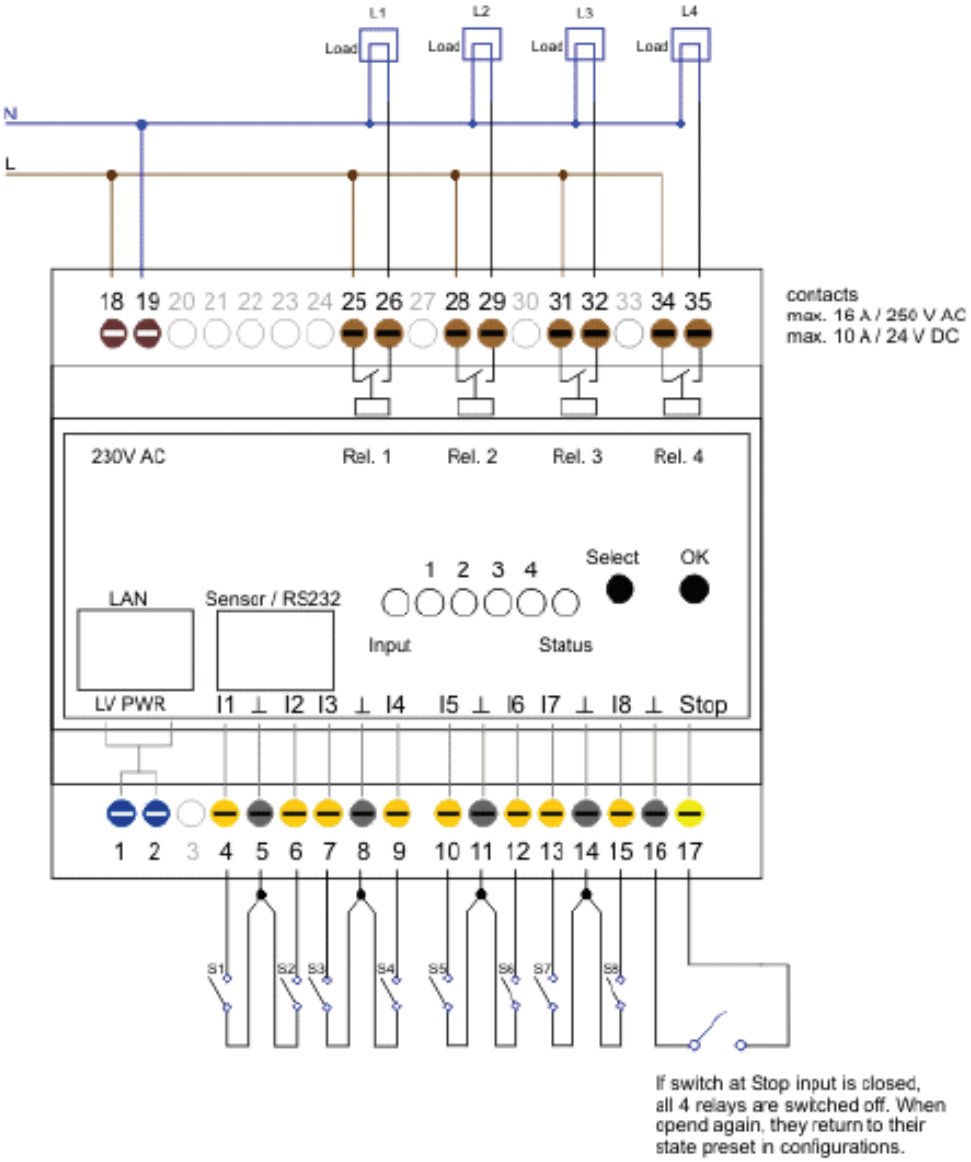
1. 230V AC power supply
2. Four relay outputs (potential-free)
3. Ethernet connector (RJ45)
4. Sensor connector (RJ45)
5. Activity LED (Input) for digital inputs
6. 4 status LED for relay outputs
7. Status LED
8. Button for Select and OK
9. Alternative low power supply LV PWR (Low Voltage PoWeR)
10. Eight passive inputs (with GND (⏚) for 2 inputs each)
11. Stop input (with GND (⏚)) to switch-off of all relais

Start-up the device

- Connect the device to the mains (230V AC) or to an AC Adaptor (10V to 24V AC, 12V to 28V DC, at 4 watts of power). Under no circumstances should the unit be fed with the mains and the AC Adaptor at the same time!
- Plug the network cable into the Ethernet socket (RJ45) .
- Connect the relay to the loads that should be be operated.
- Make contact between the lines to be monitored and the digital inputs. To close an input circuit there has to be a connection between a ground pin (⊥) and the respective input pin has to be made.
- Connect the sensor (if any) to the device.

1.4.1 Connection Example

Here an example of a block diagram in which the device is supplied with 230V AC, and four AC loads (L1 - L4) are connected. In addition, the inputs are joined to eight switches (S1 - S8), and the stop input is connected to the push-button PB1.



1.5 Technical Specifications

Interfaces	1 x Ethernet port (RJ45) 1 x Connector for mains supply (230V AC) 1 x Connector for AC Adaptor (12V DC, 0,5A). 12V DC power supply 12 x screw terminal with 8 inputs and 4 x GND 8 x screw terminal with 4 make contacts (230V AC 16A, 24V DC 10 A) 1 x RJ45 for external sensor
Network connectivity	10/100 MBit/s 10baseT Ethernet
Protocols	TCP/IP, HTTP/HTTPS, SNMP v1/v2c/v3, SNMP traps, Syslog, E-Mail (SMTP)
Power Supply	internal power supply (230V AC) alternative: 10V to 24V AC, 12V to 28V DC (at 4 watts of power)
Environment · Operating temperature · Storage temperature · Humidity	 0°C to 50°C -15°C to 60°C 10% to 85%
Case	plastics black
Measurements	105mm x 70mm x 90mm (L x H x D)
Weight	approx. 300g

1.6 Sensor

One external sensor can be connected to the **IPower Control Plus IEC Pro**. The following sensors are currently available

No.	32638	32633	32634
Cable length	2m	2m	2m
Connector	RJ45	RJ45	RJ45
Temperature range	-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)	-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)	-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)
Air humidity range (non-condensing)	-	0-100%, ±3% (maximum) and ±2% (typical)	0-100%, ±3% (maximum) and ±2% (typical)
Air pressure range (full)	-	-	± 1 hPa (typical) at 300 ... 1100 hPa, 0 ... +40 °C
Air pressure range (ext)	-	-	± 1.7 hPa (typical) at 300 ... 1100 hPa, -20 ... 0 °C
Protection	IP68	-	-

The sensors are detected automatically after connection. The sensor values are displayed directly on the "Control Panel" website:

Id	Name	Temperature °C	Humidity %	Dew Point °C	Dew Diff °C
1: 7102	7102	25.4	46.9	13.2	12.2

A click on the link in the "Name" column opens the display of the Min and Max values. The values in a column can be reset using the "Reset" button. The "Reset" button in the name column deletes all stored Min and Max values.

Id	Name	Temperature °C	Humidity %	Dew Point °C	Dew Diff °C
1: 7102	7102	25.5	46.6	13.2	12.3
	24h min	25.4	46.0	13.1	12.2
	24h max	25.9	47.0	13.5	12.5
	Reset	Reset	Reset	Reset	Reset

2 Operating

2.1 Operating the device directly



Port Switching

The current status of the output is indicated by the color of the LED. A red LED 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.

Status-LED

The Status LED shows the different states of the device:

- Red: The device is not connected to the Ethernet.
- Orange: The device is connected to the Ethernet and waits for data from the DHCP server.
- Green: The device is connected to the Ethernet and the TCP/IP settings are allocated.
- Periodic blinking: The device is in Bootloader mode.

2.2 Control Panel

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



The web page provides an overview of the switching state, as well as the external sensor, provided that it is connected. When a single port is clicked at the **IPower Switch 4 DIN S Pro**, a panel with buttons to control a single port appear:



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.



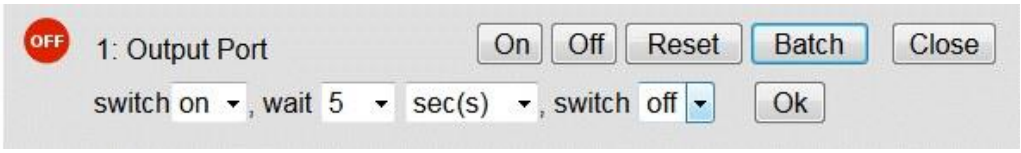
An activated Watchdog is represented by an eye icon. An "X" means, that the address that should be observed, could not be resolved. Two circular arrows show a booting status.



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 - Output Ports solves 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. More information is available on our support at www.lindy.com

Port	Name	logical state	time since transition	toggle count
Input 1	Input	0: off / open	00:05:39	0
Input 2	Input	0: off / open	00:05:39	0
Input 3	Input	0: off / open	00:05:39	0
Input 4	Input	0: off / open	00:05:39	0
Input 5	Input	0: off / open	00:05:39	0
Input 6	Input	0: off / open	00:05:39	0
Input 7	Input	0: off / open	00:05:39	0
Input 8	Input	0: off / open	00:05:39	0
Input 9	Input	0: off / open	00:05:39	0
Input 10	Input	0: off / open	00:05:39	0
Input 11	Input	0: off / open	00:05:39	0
Input 12	Input	0: off / open	00:05:39	0

The website contains a status overview of all passive signal inputs, the time since the last change, and a counter of switching changes. The name and text for a logical stateof each input can be configured in the chapter Configuration-Input Ports.

2.3 Maintenance

The actual device generation with IPv6 and SSL allows all maintenance functions inthe web interface to be carried out on the Maintenance Page

aintenance in the web interface

The following functions are available from the maintenance web page:

- Firmware Update
- Change the SSL certificate
- Load and save the configuration
- Restart the device
- Factory Reset
- Jump into the Bootloader
- Delete the DNS cache

Upload Firmware, Certificate or Configuration

On the Maintenance Page
select the required file with "Browse .." in the sections"Firmware Update", "SSL Certificate Upload" or "Config Import File Upload" and press "Upload". The file is now transferred to the update area of the device and the contents are checked. Only now, pressing the "Apply" button will permanently update the data, or abort with "Cancel".

Only one upload function can be initiated with a reboot, eg. you cannot transmit firmware and configuration at the same time.

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. If a Ctrl-F5 does not help, it is recommended that you manually delete the cache in the browser options. Alternatively, you can test start the browser in "private mode".

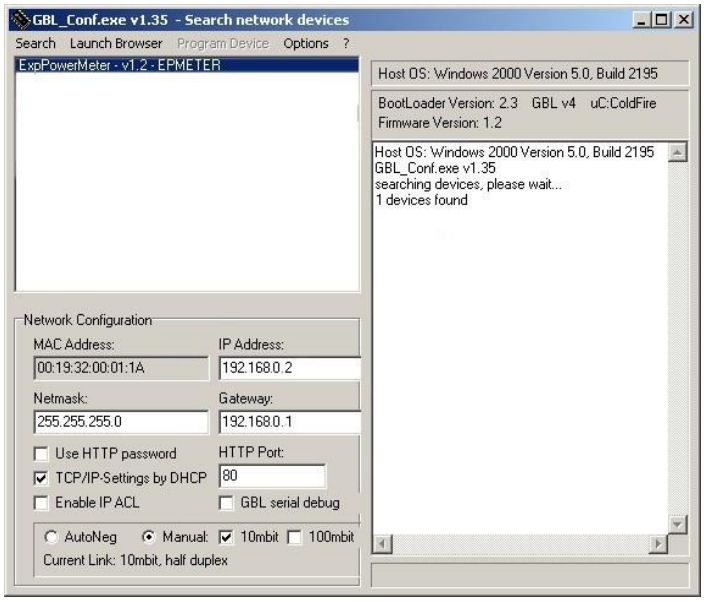
Actions in Bootloader mode

If the web interface of the device is no longer accessible, the device can be put intoBootloader mode (see chapter Bootloader activation) be executed using the GBL_Conf.exe application:
The following functions can

- Set IPv4 address, net-mask and gateway
- Turn HTTP password on and off
- Turn IP-ACL on and off
- Factory Reset
- Jump into the bootloader (can be switched on and off)
- Restart the device

For devices with relays, entering or exiting the bootloader mode does not change the state of the relays as long as the operating voltage is maintained.

The GBL_Conf.exe program is available free of charge on our website lindy.com



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.

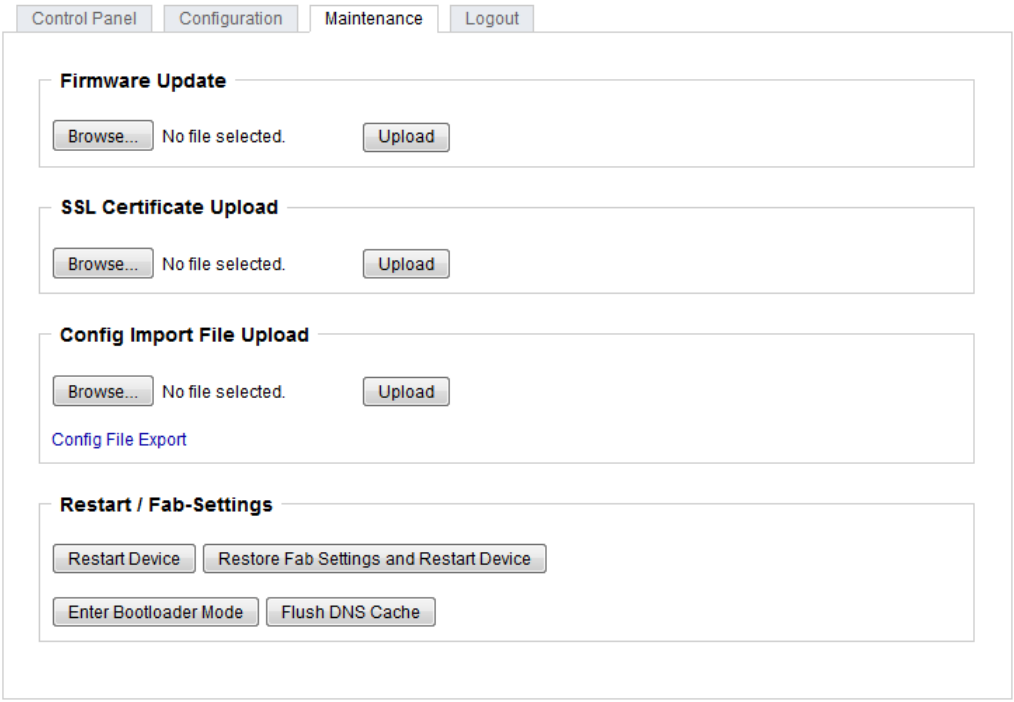
Factory Reset

The device can be reset to the factory default via the web interface from the Maintenance Pages or from the Bootloader mode (see chapter Bootloader activation
TCP/IP settings are reset in this operation.)

If a unit is set to factory defaults, an uploaded certificate or updated firmware will be preserved.

2.3.1 Maintenance Page

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



Firmware Update: Start a firmware update.

SSL Certificate Upload: Saves your own SSL certificate. See chapter "SSL 47" for the generation of a certificate in the right format.

Config Import File Upload: Loads a new configuration from a text file. To apply the new configuration, a "Restart Device" must be executed after the "Upload".

Config File Export: Saves the current configuration in a text file.

Saving the configuration should only be carried out in an SSL connection, since it contains sensitive password information (even if it is encrypted or hashed).

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. A jump to the boot loader or a restart of the device lead by no means to a change of the relay states.

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.

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

2.3.2 Configuration Management

The device configuration can be saved and restored in the maintenance area.



The "Config File Export" function can be used to save the current configuration as a text file. The syntax used in the configuration file corresponds to the commands of the Telnet console. If the configuration of a device is to be restored from a text file, load the file with "Upload" and restart the device with "Restart Device".

Saving the configuration should only be carried out in an SSL connection, since it contains sensitive password information (even if it is encrypted or hashed). For the same reasons, it is advisable to carefully handle the generated configuration files when archiving.

Editing the configuration file

It is possible to customize a saved configuration file with a text editor for your own needs. For example, one scenario would be to use a script language to automate the creation of many customized versions of a configuration, then equip a large number of devices with an individualized configuration. Also Upload and restart with CGI commands can be done in scripting languages. With use of the comment sign "#" you can quickly hide single commands or add personal notes.
If you modify a configuration file manually, it is not always clear which limits are allowed for parameters. After uploading and restarting, commands with invalid parameters are ignored. Therefore, the generated configuration includes comments describing the boundaries of the parameters. Where "range:" refers to a numeric value, and "len:" to a text parameter. E.g:

```
email auth set 0 #range: 0..2
email user set "" #len: 0..100
```

The command "system fabsettings" from the beginning of a generated configuration file brings the device into the factory state, and then executes the individual commands that modify the configuration state. It may be desirable to make the changes relative to the current configuration, and not out of the factory state. Then the "system fabsettings" should be removed.

No output of default values

The configuration file contains (with exceptions) only values which differ from the default. The command "system fabsettings" (go to the factory state) from the beginning of a generated configuration file should not be removed, otherwise the device can get incompletely configured.

Configuration via Telnet

The configuration files can in principle also be transferred in a Telnet session, but then the settings are changed during operation, and not completely when restarting, as it would have been the case with an upload. It can happen that events are triggered at the same time as the device is configured. One should therefore:

a) disable the function
b) completely parametrize
c) reactivate the function

An example:

```
email enabled set 0
email sender set "" #len: 0..100
email recipient set "" #len: 0..100
email server set "" #len: 0..100
email port set 25
email security set 0 #range: 0..2
email auth set 0 #range: 0..2
email user set "" #len: 0..100
email passwd hash set "" #len: 0..100
email enabled set 1 #range: 0..1
```

2.3.3 Bootloader Activation

The configuration of the device from the application "GBL_Conf.exe" is only possible, if the device is in Bootloader Mode.

Activation of the Bootloader Mode

1) via push button:

- Hold both buttons for 3 seconds

2) 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

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

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

4) 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" application after a renewed device search (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.

 For devices with relays, entering or exiting the bootloader mode does not change the state of the relays as long as the operating voltage is maintained.

Abandonment of the Bootloader Mode

1) via push button:

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

2) or

- Remove and connect the power supply without operating a button

3) by Software:

- Start the "GBL_Conf.exe" application
- 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.

If a unit is set to factory defaults, an uploaded certificate or updated firmware will be preserved.

1) 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)

2) by Software:

- Activate the Bootloader Mode of the device
- "Start the GBL_Conf.exe" program
- 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)

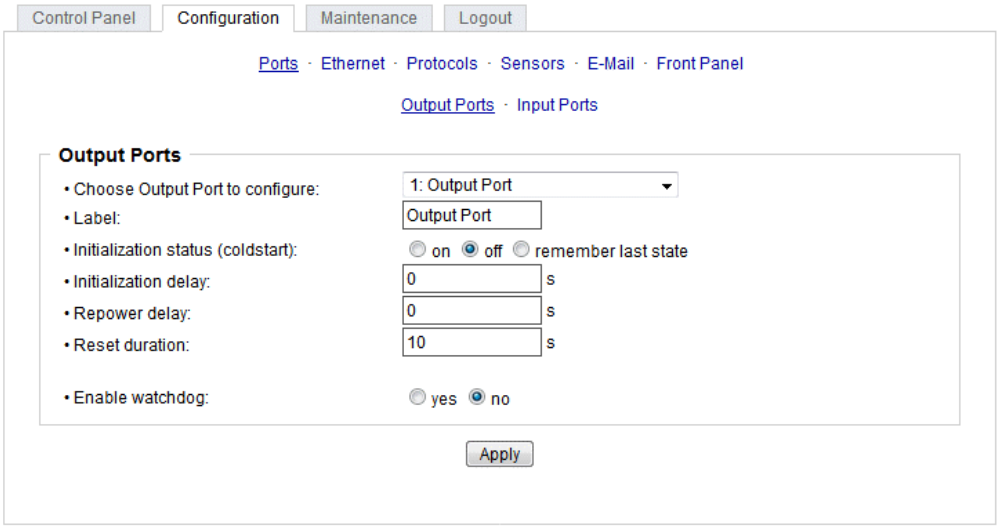
3 Configuration

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 Output Ports



Choose Output Port to configure: This field is used to select the Output Ports to be configured.

Label: You can assign a name up to 15 characters for each of the Output 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 Output 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 Output 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 Output 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 Output Port off, waits for the time entered here (in seconds) and turns the Output Port on.

3.1.1 Watchdog

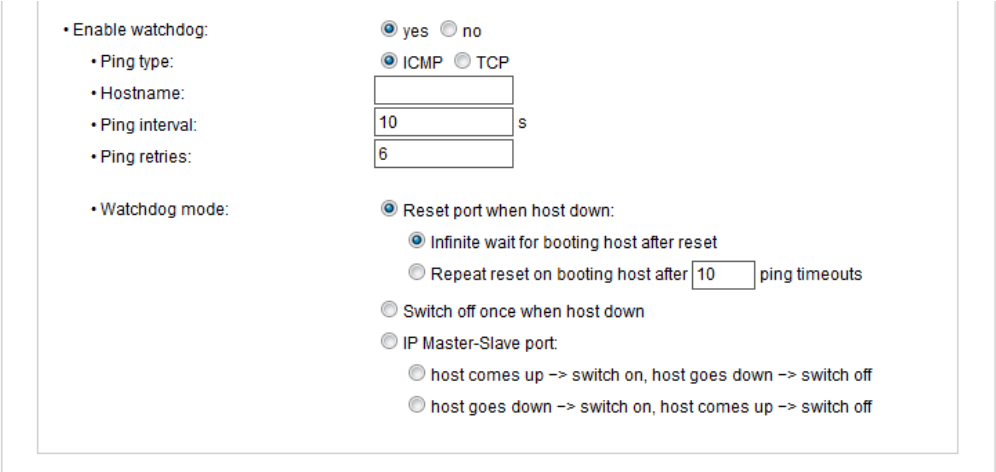
The watchdog feature enables to monitor various remote devices. Therefore either ICMP pings or TCP pings are sent to the device to be monitored. If these pings are not answered within a certain time (both the time and the number of attempts can be set), the port is reset. This allows e.g. to automatically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

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 Output 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.



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

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.

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

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

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.

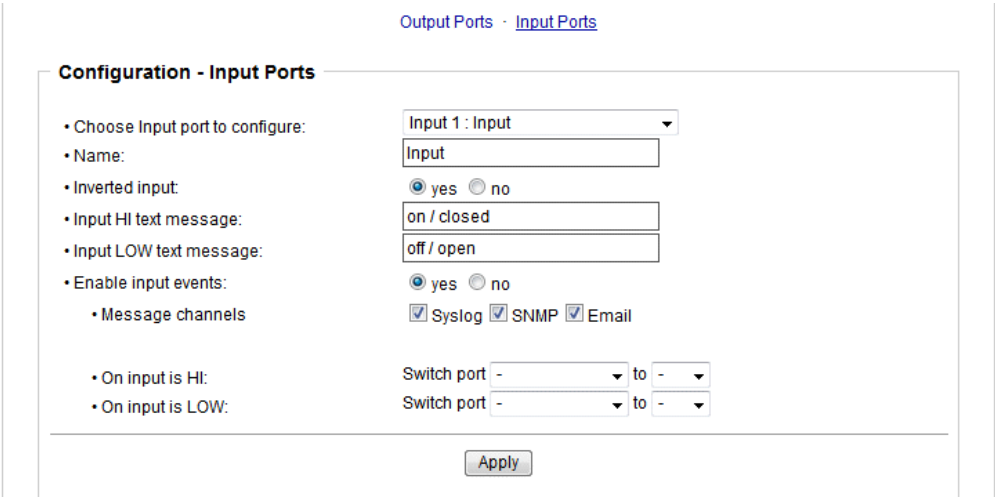
Watchdog mode: When Reset port when host down is enabled, the Output Port is turned off and switched back on after the time set in Reset Duration. In mode Switch off once when host down the Output Port remains disabled.

At the default setting (Infinite wait for booting host after reset) the watchdog monitors the connected device. When there is no longer a reply after a set time, the watchdog performs the specified action, usually a reset of the Output Port. Now the watchdog waits until the monitored device reports again on the network. This may take several minutes depending on the boot duration of the device. Only when the device is accessible from network again, the watchdog is re-armed. If the option Repeat reset on booting host after x ping timeout is enabled, this mechanism is bypassed. Now the watchdog is re-activated after N Ping intervals (input field ping timeouts).

When enabling the IP master-slave mode, the port is switched depending on the availability of a remote device. Depending on the configuration, the port is switched on when the terminal is reachable, or vice versa.

 The option Repeat reset on booting host after x ping timeout has the following pitfall: If a server, that is connected to the monitored Port is in need for a long boot process (e.g. 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.

3.2 Input Ports



Choose Input port to configure: This field is used to select the input port to be configured.

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

Inverted Input: Inverts the assignment of the input signal to a logical HI / LOW state.

Input HI Text Message: Text display in the control panel and messages when a HI signal is present at the input port.

Input LOW Text Message: Text display in the control panel and messages when a LOW signal is present at the input port.

Enable input events: Enables Input Port monitoring.

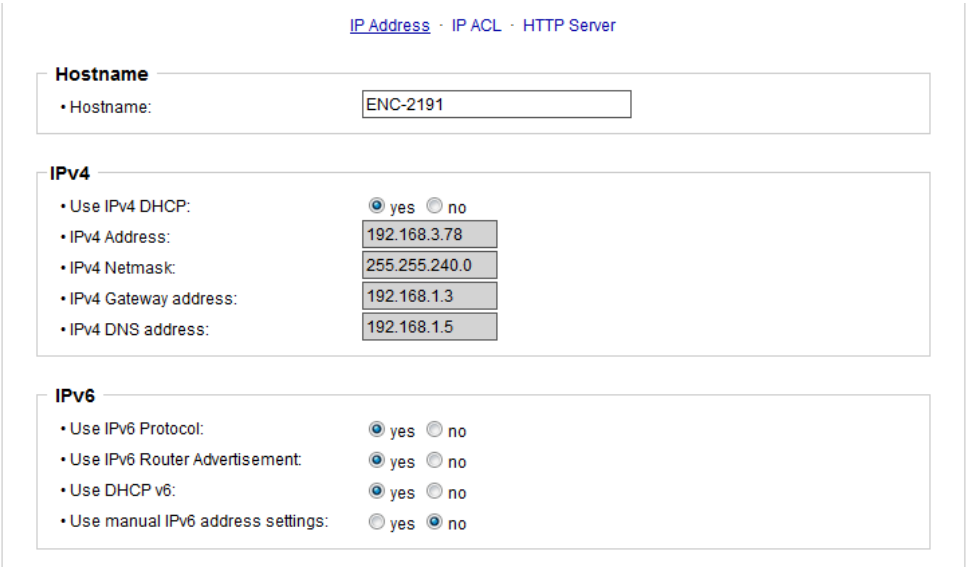
Message Channels: Enables the generation of messages on different channels.

On input is HI: Switching action when Input Port changes from LOW to HI.

On input is LOW: Switching action when Input Port changes from HI to LOW.

3.3 Ethernet

3.3.1 IP Address



Hostname: Here you can enter a name with up to 63 characters. This name will be used for registration on the DHCP server.

Special characters and umlauts can cause problems in the network.

IPv4 Address: The IP address of the device.

IPv4 Netmask: The network mask used in the network.

IPv4 Gateway address: The IP address of the gateway.

IPv4 DNS address: The IP address of the DNS server.

Use IPv4 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.

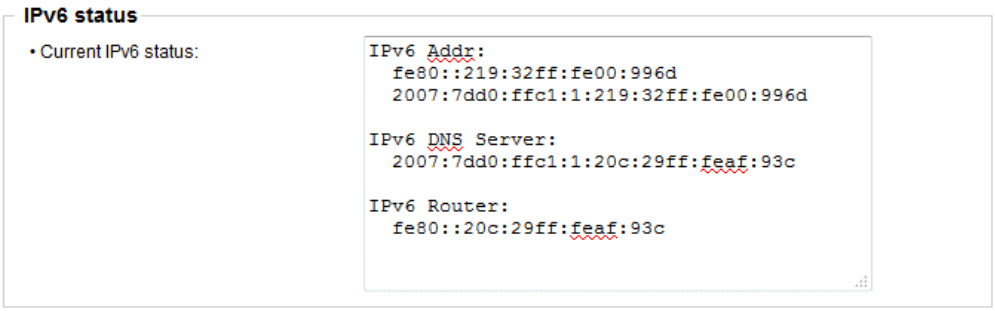
Use IPv6 Protocol: Activates IPv6 usage.

Use IPv6 Router Advertisement: The Router Advertisement communicates with the router to make global IPv6 addresses available.

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

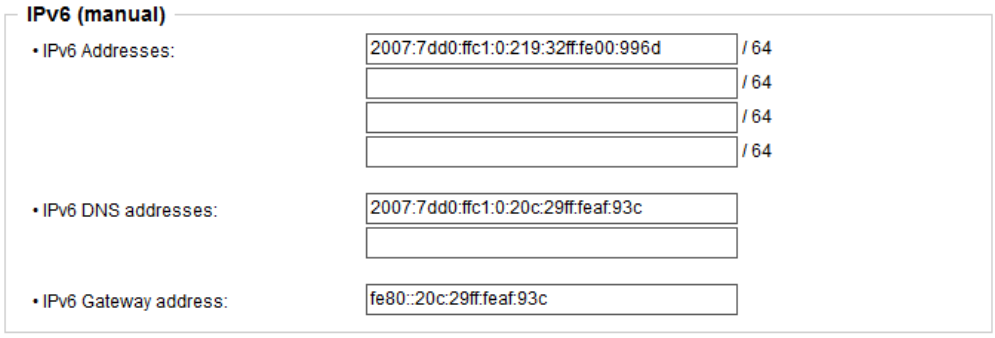
Use manual IPv6 address settings: Activates the entry of manual IPv6 addresses.

IPv6 status: Displays the IPv6 addresses over which the device can be accessed, and additionally DNS and router addresses.



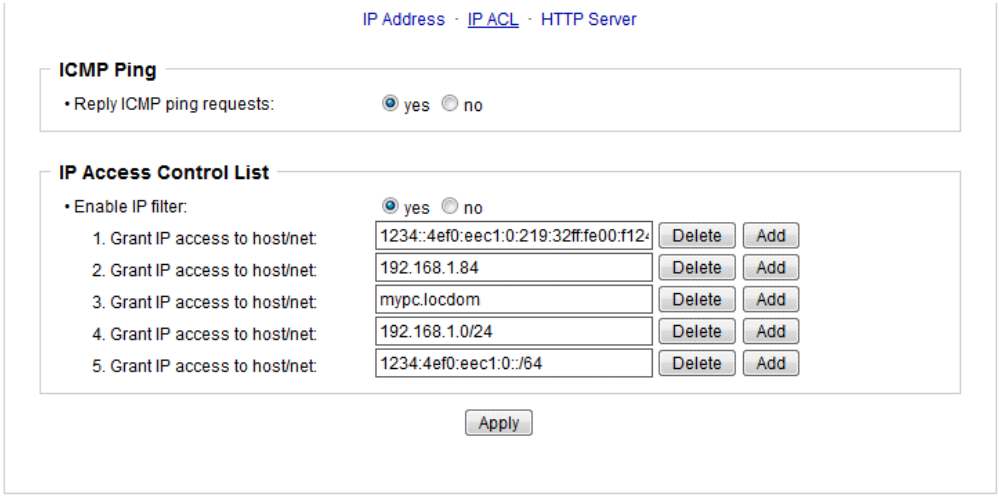
For IP changes a firmware reset is required. This can be done in the Maintenance web page. A restart of the device leads by no means to a change of the relay states.

Manual IPv6 Configuration



The input fields for the manual setting of IPv6 addresses allow you to configure the prefix of four additional IPv6 device addresses, and to set two DNS addresses, and a gateway.

3.3.2 IP ACL



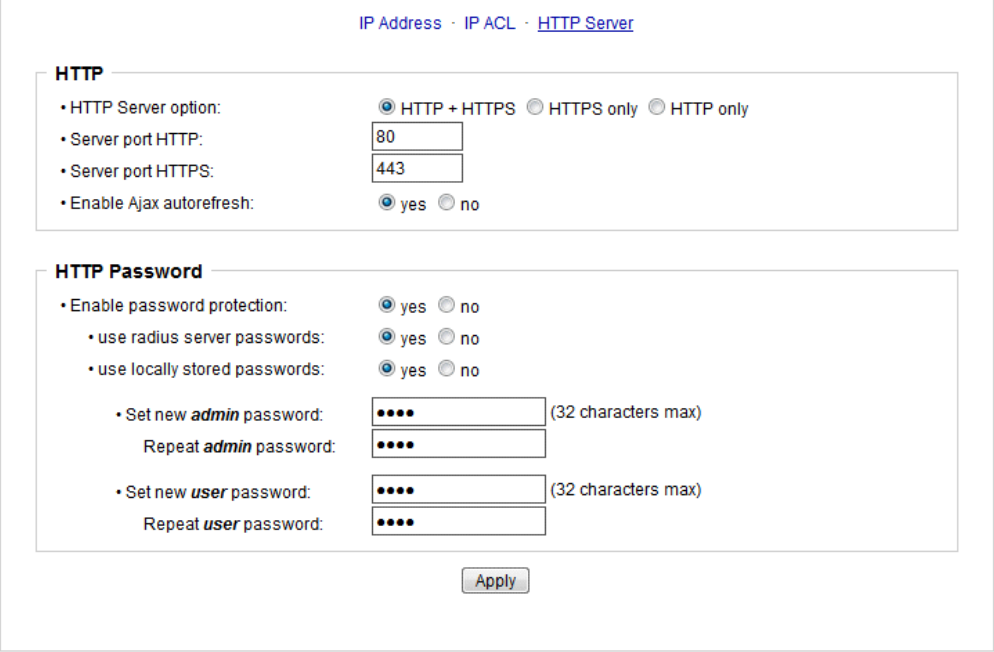
Reply ICMP ping requests: If you enable this feature, the device responds to ICMP pings from the network.

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.

3.3.3 HTTP



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

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

For some HTTP configuration changes a firmware reset is required. This can be done in the Maintenance web page. A restart of the device leads by no means to a change of the relay states.

Enable password protection: Password access protection can be activated. If the admin password is assigned, you can only log in by entering this password to change settings. Users can log in by entering the user password in order to query the status information and initiate switching operations.

Use radius server passwords: Username and password are validated by a Radius Sever.

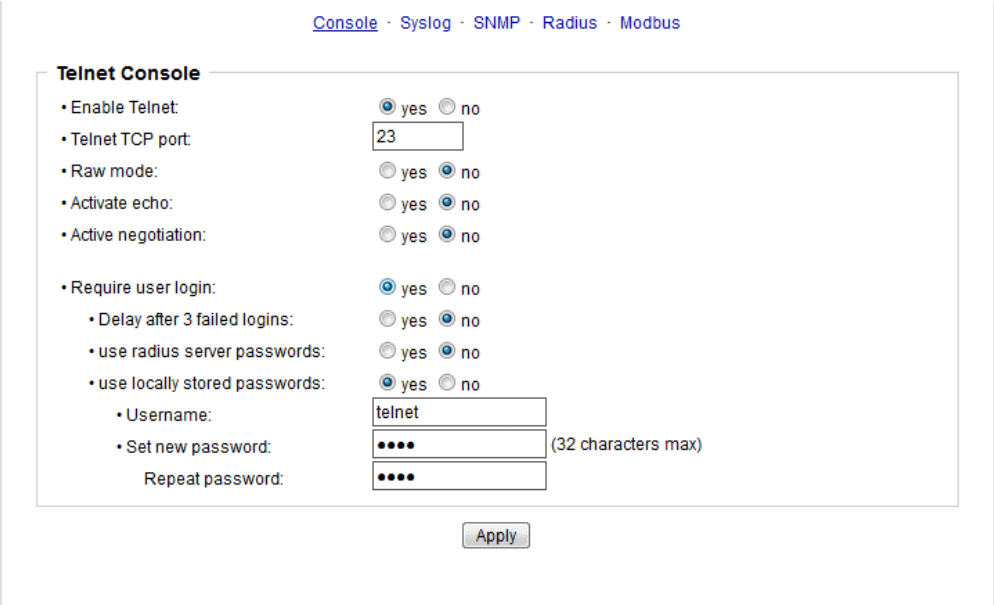
Use locally stored passwords: Username and password are stored locally. In this case, an admin password and a user password must be assigned. The password can have a maximum of 31 characters. The name "admin" and "user" are provided for the user name in the password entry mask of the browser. In factory settings, the password for the admin is set to "admin" or "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.

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

3.4 Protocols

3.4.1 Console



Enable Telnet: Enables Telnet console .

Telnet TCP port: Telnet sessions are accepted on this port.

Raw mode: The VT100 editing and the IAC protocol are disabled.

Activate echo: The echo setting if not changed by IAC.

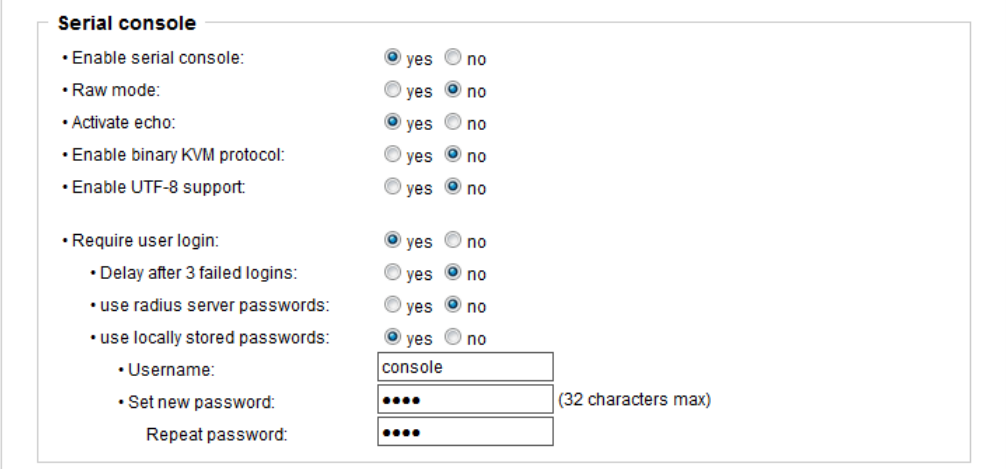
Active negotiation: The IAC negotiation is initiated by the server.

Require user login: Username and password are required.

Delay after 3 failed logins: After 3 wrong entries of username or password, the next login attempt is delayed.

Use radius server passwords: Username and password are validated by a Radius Sever.

Use locally stored passwords: Username and password are stored locally



Enable serial console: Enables the serial console.

Raw mode: The VT100 editing is disabled.

Activate echo: The echo setting.

Enable binary KVM protocol: Additionally activates the KVM protocol.

Enable UTF8 support: Enables character encoding in UTF8.

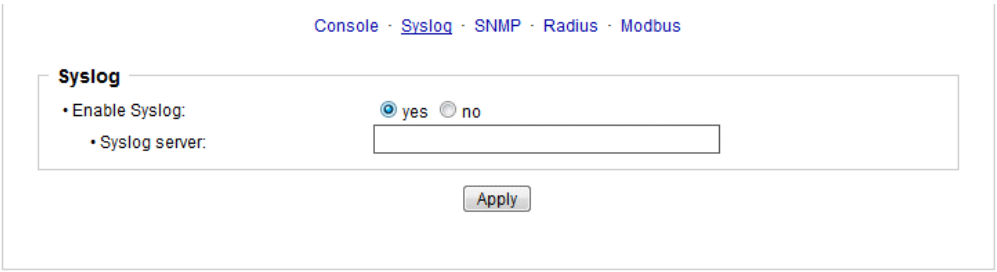
Require user login: Username and password are required.

Delay after 3 failed logins: After 3 wrong entries of username or password, the next login attempt is delayed.

Use radius server passwords: Username and password are validated by a Radius Sever.

Use locally stored passwords: Username and password are stored locally.

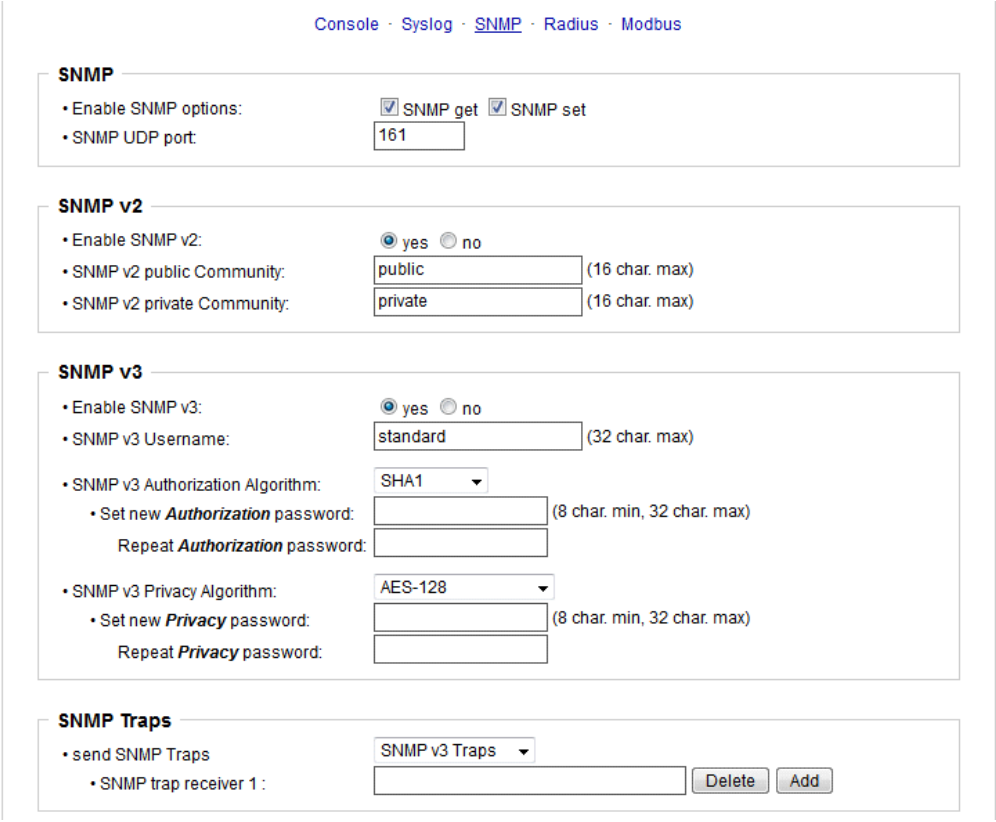
3.4.2 Syslog



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.

3.4.3 SNMP



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

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

SNMP UDP Port: Sets the UDP port where SNMP messages are received.

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. "SHA-384" and "SHA512" are calculated purely in software. If "SHA-512" is set on the configuration page, the time for the key generation may take once up to approx. 45 seconds.

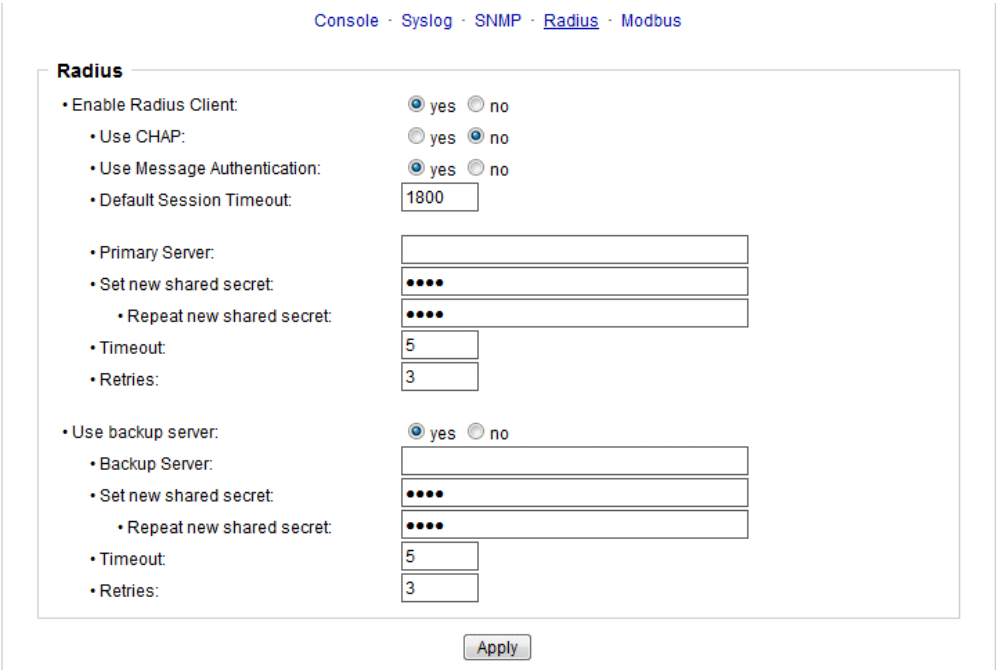
Send SNMP traps: Here you can specify whether, and in what format the device should send SNMP traps.

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

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

More information about SNMP settings are available from our support or can be found on the Internet at lindy.com

3.4.4 Radius



Enable Radius Client: Enables validation over Radius.

Use CHAP: Use CHAP password encoding.

Use Message Authentication: Adds the "Message Authentication" attribute to the Authentication Request.

Primary Server: Name or IP address of the Primary Radius server.

Shared secret: Radius Shared Secret.

Timeout: How long (in seconds) will be waited for a response from an Authentication Request.

Retries: How often an authentication request is repeated after a timeout.

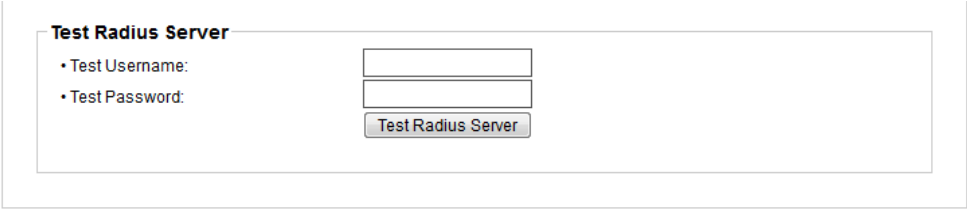
Use Backup Server: Activates a Radius Backup server.

Backup Server: Name or IP address of the Radius Backup server.

Shared secret: Radius Shared Secret.

Timeout: How long (in seconds) will be waited for a response from an Authentication Request.

Retries: How often an authentication request is repeated after a timeout.



Test Username: Username input field for Radius test.

Test Password: Password input field for Radius test.

The "Test Radius Server" function allows you to check whether a combination of User-name and Password is accepted by the configured Radius Servers.

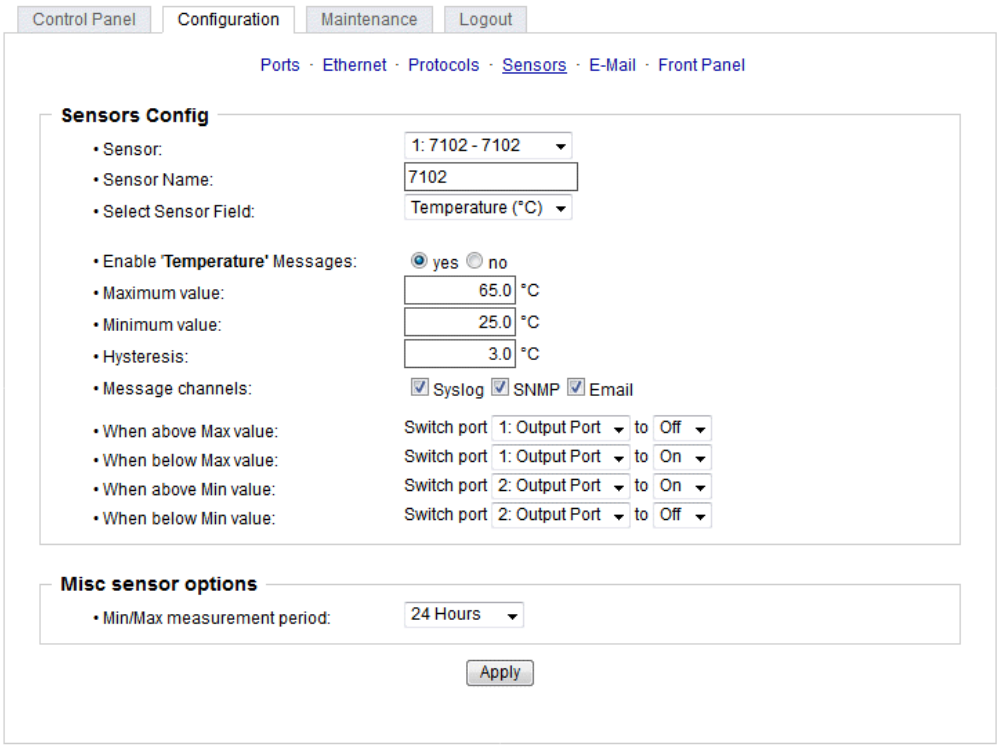
3.4.5 Modbus TCP



Enable Modbus TCP: Enables Modbus TCP support.

Modus TCP port: The TCP/IP port number for Modbus TCP.

3.5 Sensors



Sensor: 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, and the changeable sensor name.

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

Select Sensor Field: Selects a data channel from a sensor.

Enable ... 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 E-Mail.

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

Message channels: Enables the generation of messages on different channels.

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

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:

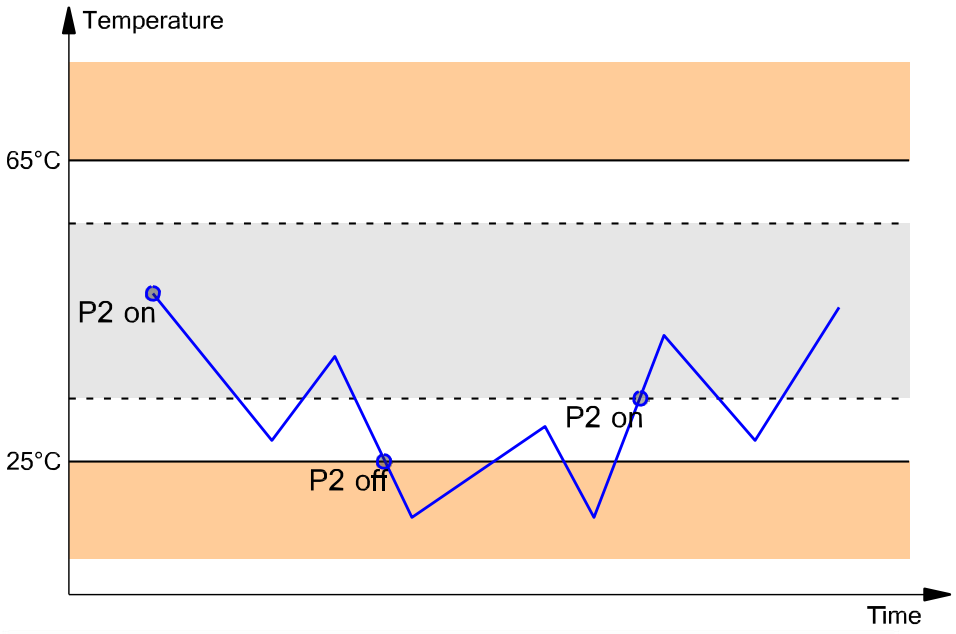
49.9 °C - is below the upper limit
50.0 °C - a message is generated for reaching the upper limit
50.1 °C - is above the upper limit
...

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
...

3.5.1 Port Switching

Depending on the measured Current and the measured sensor values, switching actions can be triggered. During operation, the actions configured for crossing the limits are executed. For example, when a value moves from the range "above max value" inside the range "below max value", the action defined for "below max value" is performed. In the case of device start, configuration or plug-in of the sensor, the actions corresponding to the range in which the current temperature is located are switched.

Example with "Maximum value" of 65 °C, "Minimum value" of 25 °C and hysteresis of 3 °C. The dotted line shows the hysteresis.





Actions during configuration, device start or plugging in the sensor (for given example):

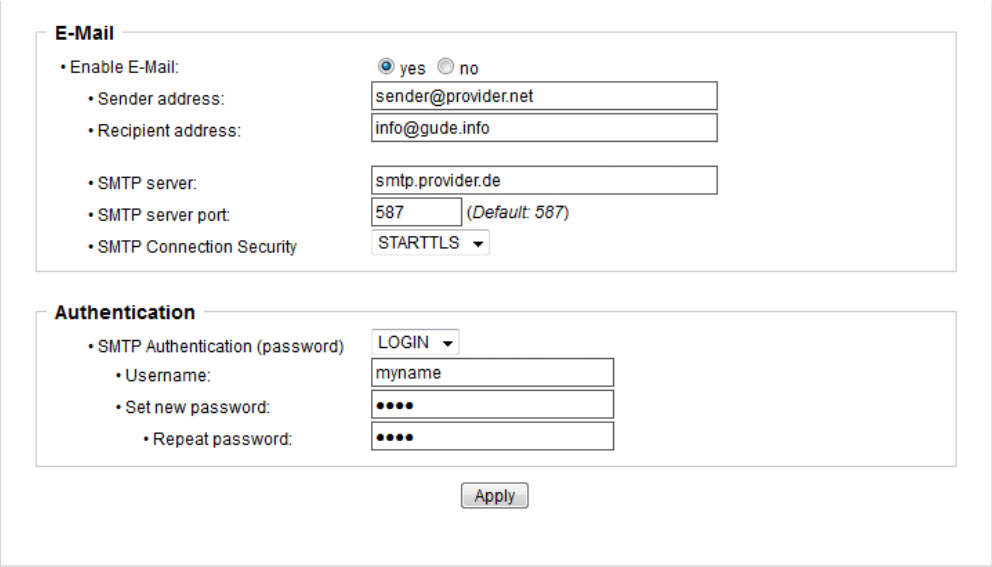
actual temperature during configuration	actions
70 °C	Port 1 Off (above max) + Port 2 On (above min)
45 °C	Port 1 On (below max) + Port 2 On (above min)
20 °C	Port 1 On (below max) + Port 2 Off (below min)

Action matrix during operation when limit values are exceeded (for given example):

	to "above max"	to "below max"	to "above min"	to "below min"
from "above max"	-	P1 On	P1 On	P1 On + P2 Off
from "below max"	P1 Off	-	-	P2 Off
from "above min"	P1 Off	-	-	P2 Off
from "below min"	P1 Off + P2 On	P2 On	P2 On	-

Only the switching operations for which actions have been defined, are triggered. If no "On" or "Off" action is defined for a port, the port can never reach this state by exceeding sensor values. Unless it is the initial state.

3.6 E-Mail



Enable E-Mail: Activates the e-mail dispatch of messages.

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

Recipient address: The e-mail address of the recipient. Additional E-Mail addresses, separated by comma, can be specified. The input limit is 100 characters.

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 e-mail 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 Authentification (password): Authentication method of the E-Mail Server.

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

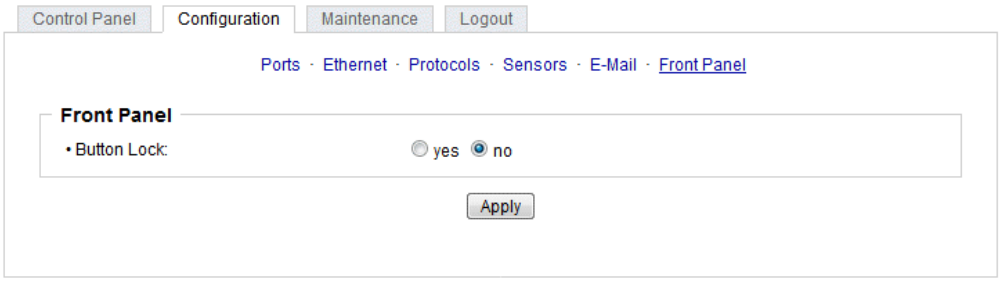
Set new password: Enter the password for the login to the e-mail server.

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.

3.7 Front Panel



Button Lock: Disables the front buttons (activates the key lock) with the exception of the bootloader activation.

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 seperator 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 Radius

The passwords for HTTP, telnet, and serial console (depending on the model) can be stored locally and / or authenticated via RADIUS. The RADIUS configuration supports a primary server and a backup server. If the primary server does respond, the RADIUS request is sent to the backup server. If the local password and RADIUS are enabled at the same time, the system is first checking locally, and then in the event of a failure the RADIUS servers are contacted.

RADIUS attributes

The following RADIUS attributes are evaluated by the client:

Session-Timeout: This attribute specifies (in seconds) how long an accepted RADIUS request is valid. After this time has elapsed, the RADIUS server must be prompted again. If this attribute is not returned, the default timeout entry from the configuration is used instead.
Filter-Id: If the value "admin" is set for this attribute, then an admin rights are assigned for the login, otherwise only user access.
Service-Type: This is an alternative to Filter-Id. A service type of "6" or "7" means admin rights for the HTTP login, otherwise only limited user access.

HTTP Login

The HTTP login takes place via Basic Authentication. This means that it is the responsibility of the web server, how long the login credentials are temporarily stored there. The RADIUS parameter "Session-Timeout" therefore does not determine when the user has to login again, but at what intervals the RADIUS servers are asked again.

4.4 Automated Access

The device can be accessed automatically via four different interfaces, which offer different possibilities to access the configuration data and status information. Only http and the console (telnet and serial) provide full access to the device.

List of different access options (if supported by the model):

Interface	Scope of Access
HTTP	read / write all configuration data read / write all status information
Console 48	read / write all configuration data read / write all status information
SNMP 43	read / write status of Power Ports (relays) read / write names of Power Ports (relays) read / write status of Port start configuration read / write status Buzzer

	read measurement values of external sensors read measurement values of all energy sensors resetting the energy meters read the status of Overvoltage Protection
Modbus TCP 56	read / write status of Power Ports (relays) read status of Inputs read measurement values of external sensors read measurement values of all energy sensors

The device can be controlled via HTTP interface with CGI commands and returns the internal configuration and status in JSON format.

4.5 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.

 "SHA-384" and "SHA512" are calculated purely in software. If "SHA-384" or "SHA-512" is set on the configuration page, the time for the key generation may take once up to approx. 45 seconds.

Encryption

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.

 While in the settings "AES-192" and "AES256" the key calculation is based on "draft-blumenthalphoto-aes-usm-04", the methods "AES 192-3DESKey" and "AES 256-3DESKey" utilize a key generation, which is also used in the "3DES" configuration ("draft-reeder-snmpv3-usm-3desede-00"). If one is not an SNMP expert, it is recommended to try in each case the settings with and without "...- 3DESKey".

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. Since only SHA-256 is accelerated in hardware, and SHA-384 and SHA-512 are calculated purely in software, one should normally select SHA-256. From a cryptographic point of view, the security of SHA-256 is sufficient for today's usage.
- 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.

Change in Trap Design

In older MIB tables, a separate trap was defined for each combination of an event and a port number. This results in longer lists of trap definitions for the devices. For example, from **epc8221SwitchEvtPort1** to **epc8221SwitchEvtPort12.** Since new firmware versions can generate many more different events, this behavior quickly produces several hundred trap definitions. To limit this overabundance of trap definitions, the trap design has been changed to create only one specific trap for each event type. The port or sensor number is now available in the trap as an index OID within the variable bindings.

In order to recognize this change directly, the "Notification" area in the MIB table has been moved from sysObjectID.0 to sysObjectID.3. This way, unidentified events are generated until the new MIB table is imported. For compatibility reasons, SNMP v1 traps are created in the same way as before.

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 epc822XPortState.1

Switch on Power Port 1:

snmpset -v2c -mALL -c private 192.168.1.232 epc822XPortState.1 integer 1

4.5.1 Device MIB 2302

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 "1.3.6.1.4.1.28507.70.1.1.1". 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.
Description			
enc2302TrapCtrl	.70.1.1.1.1.0	Integer32	RW
0 = off 1 = Ver. 1 2 = Ver. 2c 3 = Ver. 3			
enc2302TrapIPIndex	.70.1.1.1.2.1.1.x	Integer32	RO

	A unique value, greater than zero, for each receiver slot.		
enc2302TrapAddr	.70.1.1.1.2.1.2.x	OCTETS	RW
	DNS name or IP address specifying one Trap receiver slot. A port can optionally be specified: 'name:port' An empty string disables this slot.		
enc2302portNumber	.70.1.3.1.1.0	Integer32	RO
	The number of Relay Ports		
enc2302PortIndex	.70.1.3.1.2.1.1.x	Integer32	RO
	A unique value, greater than zero, for each Relay Port.		
enc2302PortName	.70.1.3.1.2.1.2.x	OCTETS	RW
	A textual string containing name of a Relay Port.		
enc2302PortState	.70.1.3.1.2.1.3.x	INTEGER	RW
	current state a Relay Port		
enc2302PortSwitchCount	.70.1.3.1.2.1.4.x	Integer32	RO
	The total number of switch actions ocurred on a Relay Port. Does not count switch commands which will not switch the ralay state, so just real relay switches are displayed here.		
enc2302PortStartupMode	.70.1.3.1.2.1.5.x	INTEGER	RW
	set Mode of startup sequence (off, on , remember last state)		
enc2302PortStartupDelay	.70.1.3.1.2.1.6.x	Integer32	RW
	Delay in sec for startup action		
enc2302PortRepowerTime	.70.1.3.1.2.1.7.x	Integer32	RW
	Delay in sec for repower port after switching off		
enc2302ActiveInputs	.70.1.5.6.1.0	Unsigned32	RO
	Number of suppported Input Channels.		
enc2302InputIndex	.70.1.5.6.2.1.1.x	Integer32	RO
	None		
enc2302Input	.70.1.5.6.2.1.2.x	INTEGER	RO
	Input state of device		
enc2302SensorIndex	.70.1.6.1.1.1.x	Integer32	RO
	None		
enc2302TempSensor	.70.1.6.1.1.2.x	Integer32	RO
	actual temperature		
enc2302HygroSensor	.70.1.6.1.1.3.x	Integer32	RO
	actual humidity		
enc2302InputSensor	.70.1.6.1.1.4.x	INTEGER	RO
	logical state of input sensor		
enc2302AirPressure	.70.1.6.1.1.5.x	Integer32	RO
	actual air pressure		
enc2302DewPoint	.70.1.6.1.1.6.x	Integer32	RO
	dew point for actual temperature and humidity		
enc2302DewPointDiff	.70.1.6.1.1.7.x	Integer32	RO
	difference between dew point and actual temperature (Temp - DewPoint)		

4.6 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_ECDH_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 Shining 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
```

An uploaded certificate will be preserved, when a device is put back to factory defaults 21.

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.

4.7 Console

For the configuration and control of the device, there is a set of commands with parameters that can be entered through a console. The console is available via Telnet, or for devices with RS232 port through using a serial terminal. The communication can also be performed automated (e.g. via scripting languages). The console features are configured through the web interface 31.

Command Set

There are several command levels. The following commands are usable from each level:

back	go back one level
help	all commands of the actual level
help all	show all commands
logout	logout (only when login required)
quit	quit console

The "help" command returns all the commands of the current level. If "help" is called from the top level, e.g. the line "http [subtopics]" appears. This means that there is another level for "http". With the command "http help" all commands below "http" are shown. Alternatively, with entering "http" you can select the http level, and "help" shows all the commands on the selected level. The command "back" again selects the top level. It is possible to use "help" at any position: "http passwd help" provides all commands that have the prefix "http passwd".

You will find a complete list of all possible device commands in the chapter "Cmd Overview".

Parameter

If parameters are expected for the command, the parameter may be passed as numeric or constant. If e.g. you get the following line as help:

```
http server set {http_both=0|https_only=1|http_only=2}
```

the following instruction pairs are equivalent:

```
http server set https_only
http server set 1
```

or

```
http server set https_both
http server set 0
```

Numerical parameters can be entered with different bases. Here is an example of the decimal value 11:

Base	**Input**
decimal (10)	11
hexadecimal (16)	0xb
octal (8)	013
binary (2)	0b1011

Return Values

If a command is unknown or a parameter is incorrect, the output "ERR." is given at the beginning of the line, followed by a description of the fault. Successful instructions without special return value will be acknowledged by "OK.". All other return values are output within a single line. There are of two exceptions:

1. Some configuration changes, that affect TCP / IP and UDP, need a restart to be applied. These parameters are output on two lines. In the first line the current value is shown, on the second row the value after a restart. In the "Cmd Overview" table this is marked with "Note 2".
2. Other configurations (such as the assigned IPv6 addresses) have several values that can change dynamically. This is marked with "Note 3" in the "Cmd Overview" table.

Numerical Returns

For parameters that support constants, these constants are output as return values. To better deal with scripting languages, it may be easier to work only with numerical returns. The command "`vt100 numeric set ON`" enables that only numerical values appear.

Comments

If you use a tool to send an entire file of commands via Telnet, it is helpful, if you can place comments in there. Beginning with the comment character "#", the remaining contents of a line is ignored.

Telnet

If the configuration "Raw Mode" is turned off, it is tried to negotiate the Telnet configuration between client and server using IAC commands. If this fails, the editing functions are not active, and the "Activate echo" option determines whether the characters sent to the Telnet server will be returned. Normally the client begins with the IAC negotiation. If this is not the case with the client, the device configuration "Active negotiation" should be turned on.

Raw Mode

If you want to use the console only automated, it may be advantageous to set the configuration "Raw mode" to "yes" and "Activate echo" to "no" to. Then there is no interfering interaction with the editor functions and the is no need to filter the sent characters to process the return values.

 If in the console "Raw mode" is activated but not in the used Telnet client, the IAC commands sent at the beginning can appear as interfering characters in the command line (partially invisible).

Editing

The following edit functions are available when the terminal supports VT100, and Raw Mode is deactivated. Entered characters are inserted at the cursor position.

Keys	Function
Left, Right	moves cursor left or right
Pos1, End	moves cursor to the beginning or end of line
Del	deletes character under the cursor
Backspace	deletes character left of cursor
Up, Down	shows input lines history
Tab, Ctrl-Tab	completes the word at cursor
Ctrl-C	clears the line

 When a shrink of the terminal window leads to the result, that the input line extends over multiple lines on the terminal, the editing does not work reliably.

4.7.1 Console Cmd 2302

Command	Description	Note
logout	go to login prompt when enabled	2
quit	quits telnet session - nothing in serial console	2
back	back one cmd level	2
help	show all cmds from this level	2
help all	show all cmds	2
console	enters cmd group "console"	
console version	shows unique console version number	
console telnet enabled set {OFF=0|ON=1}	enables telnet on/off	
console telnet enabled show	shows if telnet enabled	
console telnet port set {ip_port}	sets telnet port	
console telnet port show	shows telnet port	
console telnet raw set {OFF=0|ON=1}	sets raw mode (disables editing) on/off	
console telnet raw show	shows if raw mode enabled	
console telnet echo set {OFF=0|ON=1}	enables echo on/off	
console telnet echo show	shows if echo enabled	
console telnet activeneg set {OFF=0|ON=1}	enables telnet active negotiation (IAC) on/off	
console telnet activeneg show	shows if active negotiation enabled	
console telnet login set {OFF=0|ON=1}	enables login on/off	
console telnet login show	shows if login enabled	
console telnet login local set {OFF=0|ON=1}	enables local login on/off	
console telnet login local show	shows if local login enabled	
console telnet login radius set {OFF=0|ON=1}	enables login for RADIUS on/off	
console telnet login radius show	shows if RADIUS login enabled	
console telnet login delay set {OFF=0|ON=1}	enables delay (after 3 login fails) on/off	
console telnet login delay show	shows if login delay enabled	
console telnet user set "{username}"	sets login user name	
console telnet user show	shows login user name	
console telnet passwd set "{passwd}"	sets login password	
console telnet passwd hash set "{passwd}"	sets login hashed password	
console serial enabled set {OFF=0|ON=1}	enables serial console on/off	
console serial enabled show	shows if serial console enabled	
console serial raw set {OFF=0|ON=1}	sets raw mode (disables editing) on/off	
console serial raw show	shows if raw mode enabled	
console serial echo set {OFF=0|ON=1}	enables echo on/off	
console serial echo show	shows if echo enabled	
console serial kvm set {OFF=0|ON=1}	enables binary KVM cmds on serial port on/off	
console serial kvm show	shows if binary KVM cmds enabled	
console serial utf8 set {OFF=0|ON=1}	enables UTF8 support	
console serial utf8 show	shows if UTF8 enabled	
console serial login set {OFF=0|ON=1}	enables login on/off	
console serial login show	shows if login enabled	
console serial login local set {OFF=0|ON=1}	enables local login on/off	
console serial login local show	shows if local login enabled	
console serial login radius set {OFF=0|ON=1}	enables login for RADIUS on/off	
console serial login radius show	shows if RADIUS login enabled	
console serial login delay set {OFF=0|ON=1}	enables delay (after 3 login fails) on/off	
console serial login delay show	shows if login delay enabled	
console serial user set "{username}"	sets login user name	
console serial user show	shows login user name	
console serial passwd set "{passwd}"	sets login password	
console serial passwd hash set "{passwd}"	sets login hashed password	
email	enters cmd group "email"	
email enabled set {OFF=0|ON=1}	enables email on/off	
email enabled show	shows if email is enabled	
email sender set "{email_addr}"	sets email sender address	
email sender show	shows email sender address	
email recipient set "{email_addr}"	sets email recipient address	
email recipient show	shows email recipient address	
email server set "{dns_name}"	sets email SMTP server address	
email server show	shows email SMTP server address	
email port set {ip_port}	sets email SMTP port	
email port show	shows email SMTP port	
email security set {NONE=0|STARTTLS=1| SSL=2}	sets SMTP connection security	
email security show	shows SMTP connection security	
email auth set {NONE=0|PLAIN=1|LOGIN=2}	sets email authentication	
email auth show	show email authentication	
email user set "{username}"	sets SMTP username	
email user show	shows SMTP username	
email passwd set "{passwd}"	sets SMTP password	

email passwd hash set "{passwd}"	sets crypted SMTP password	
email testmail	send test email	
ethernet	enters cmd group "ethernet"	
ethernet mac show	shows MAC address	
ethernet link show	shows ethernet link state	
ethernet phyprefer set {10MBIT_HD=0|10MBIT_FD=1|100MBIT_HD=2|100MBIT_FD=3}	sets preferred speed for PHY Auto Negotiation	
ethernet phyprefer show	shows preferred speed for PHY Auto Negotiation	
extsensor	enters cmd group "extsensor"	
extsensor {port_num} {sen_field} value show	shows sensor value	6
extsensor {port_num} {sen_type} label set "{name}"	sets sensor name to label	6
extsensor {port_num} {sen_type} label show	shows label of sensor	6
extsensor {port_num} type show	shows type of sensor	
extsensor {port_num} {sen_type} {sen_field} events set {off=0|on=1}	enables sensor events on/off	6
extsensor {port_num} {sen_type} {sen_field} events show	shows if sensor events are enabled	6
extsensor {port_num} {sen_type} {sen_field} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	enables different event types	6
extsensor {port_num} {sen_type} {sen_field} events type show	shows what event types are enabled	6
extsensor {port_num} {sen_type} {sen_field} maxval set {num}	sets maximum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} maxval show	shows maximum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} min-val set {num}	sets minimum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} min-val show	shows minimum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} hyst set {num}	sets hysterese value for sensor	6
extsensor {port_num} {sen_type} {sen_field} hyst show	shows hysterese value for sensor	6
extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0|ABOVEMIN=1|ABOVEMAX=2|BELOWMAX=3} port set {port_num}	sets Port for Power Port Switching actions	6
extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0|ABOVEMIN=1|ABOVEMAX=2|BELOWMAX=3} port show	shows Port for Power Port Switching actions	6
extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0|ABOVEMIN=1|ABOVEMAX=2|BELOWMAX=3} state set {OFF=0|ON=1|DISABLED=2}	sets Port state for Power Port Switching actions	6
extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0|ABOVEMIN=1|ABOVEMAX=2|BELOWMAX=3} state show	shows Port state for Power Port Switching actions	6
extsensor period set {24H=0|12H=1|2H=2|1H=3|30MIN=4}	sets sensor Min/Max measurement period	
extsensor period show	shows sensor Min/Max measurement period	
http	enters cmd group "http"	
http server set {HTTP_BOTH=0|HTTPS_ONLY=1|HTTP_ONLY=2}	sets connection types the webserver accepts	
http server show	shows webserver accepting connection types	
http port set {ip_port}	sets http port	
http port show	shows http port	
http portssl set {ip_port}	sets https port	
http portssl show	shows https port	
http ajax enabled set {OFF=0|ON=1}	enables ajax autorefresh on/off	
http ajax enabled show	shows if ajax autorefresh enabled	
http passwd enabled set {OFF=0|ON=1}	enables http password on/off	
http passwd enabled show	shows if http password enabled	
http passwd user set "{passwd}"	sets http user password	
http passwd admin set "{passwd}"	sets http admin password	
http passwd hash user set "{passwd}"	sets hashed http user password	
http passwd hash admin set "{passwd}"	sets hashed http admin password	
input	enters cmd group "input"	
input {port_num} state show	shows input state	

input all state {MODE0=0|MODE1=1|MODE2=2}
show shows input state of all ports in 3 different view modes 4

nput {port_num} name set "{name}"	sets sensor name to label
input {port_num} name show	shows label of sensor
input {port_num} invert enabled set {off=0|on=1}	inverts input on/off
input {port_num} invert enabled show	shows if input inverted
input {port_num} label {LOW=0|HIGH=1} set "{name}"	sets input low/high text
input {port_num} label {LOW=0|HIGH=1} show	shows inputs low/high text
input {port_num} events set {off=0|on=1}	enables input events on/off
input {port_num} events show	shows if input events are enabled
input {port_num} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	enables different event types
input {port_num} events type show	shows what event types are enabled
input {port_num} {LOW=0|HIGH=1} port set {port_num}	sets Port for Power Port Switching actions
input {port_num} {LOW=0|HIGH=1} port show	shows Port for Power Port Switching actions
input {port_num} {LOW=0|HIGH=1} state set {OFF=0|ON=1|DISABLED=2}	sets Port state for Power Port Switching actions

input {port_num} {LOW=0|HIGH=1} state show	shows Port state for Power Port Switching actions	
input volt3 state show	shows state of 3V input voltage {ON=1|VERR=3}	
input volt12 state set {OFF=0|VLO=1|VHI=2}	sets state of 12V input voltage	
input volt12 state show	shows state of 12V input voltage {OFF=0|VLO=1|VHI=2|VERR=3} incl possible error condition	
ip4	enters cmd group "ip4"	
ip4 hostname set "{name}"	sets device hostname	
ip4 hostname show	shows device hostname	3
ip4 address set "{ip_address}"	sets IPv4 address	
ip4 address show	shows IPv4 address	3
ip4 netmask set "{ip_address}"	sets IPv4 netmask	
ip4 netmask show	shows IPv4 netmask	3
ip4 gateway set "{ip_address}"	sets IPv4 gateway address	
ip4 gateway show	shows IPv4 gateway address	3
ip4 dns set "{ip_address}"	sets IPv4 DNS server address	
ip4 dns show	shows IPv4 DNS server address	3
ip4 dhcp enabled set {OFF=0|ON=1}	enables IPv4 DHCP on/off	
ip4 dhcp enabled show	shows IPv4 DHCP state	3
ip6	enters cmd group "ip6"	
ip6 enabled set {OFF=0|ON=1}	enables IPv6 on/off	
ip6 enabled show	shows if IPv6 is enabled	3
ip6 routadv enabled set {OFF=0|ON=1}	enables IPv6 router advertisement	
ip6 routadv enabled show	shows IPv6 router advertisement state	3
ip6 dhcp enabled set {OFF=0|ON=1}	enables IPv6 DHCP on/off	
ip6 dhcp enabled show	shows if IPv6 DHCP is enabled	3
ip6 address show	show all IPv6 addresses	4
ip6 gateway show	show all IPv6 gateways	4
ip6 dns show	show all IPv6 DNS server	4
ip6 manual enabled set {OFF=0|ON=1}	enables manual IPv6 addresses	
ip6 manual enabled show	shows if manual IPv6 addresses are enabled	3
ip6 manual address {1..4} set "{ip_address}"	sets manual IPv6 address	
ip6 manual address {1..4} show	shows manual IPv6 address	3
ip6 manual gateway set "{ip_address}"	sets manual IPv6 gateway address	
ip6 manual gateway show	shows manual IPv6 gateway address	3
ip6 manual dns {1..2} set "{ip_address}"	sets manual IPv6 DNS server address	
ip6 manual dns {1..2} show	shows manual IPv6 DNS server address	3
ipacl	enters cmd group "ipacl"	
ipacl ping enabled set {OFF=0|ON=1}	enables ICMP ping on/off	
ipacl ping enabled show	shows if ICMP ping enabled	
ipacl enabled set {OFF=0|ON=1}	enable IP filter on/off	
ipacl enabled show	shows if IP filter enabled	
ipacl filter {ipacl_num} set "{dns_name}"	sets IP filter {ipacl_num}	
ipacl filter {ipacl_num} show	shows IP filter {ipacl_num}	
modbus	enters cmd group "modbus"	
modbus enabled set <off=0/on=1>	enables Modbus TCP support	
modbus enabled show	shows if Modbus is enabled	
modbus port set <ip_port>	sets Modbus TCP port	
modbus port show	shows Modbus TCP port	
port	enters cmd group "port"	
port {port_num} state set {OFF=0|ON=1}	sets port to new state	
port {port_num} state show	shows port state	
port all state set "{port_list}" {OFF=0|ON=1}	sets several ports in one cmd - e.g. port all state set "1,3,5" 1	
port all state {MODE0=0|MODE1=1|MODE2=2} show	shows all port states in 3 different view modes	4
port {port_num} reset	start reset sequence for port	
port {port_num} toggle	toggles port	
port {port_num} batch set {OFF=0|ON=1} wait {num_secs} {OFF=0|ON=1}	starts batch mode for port	
port {port_num} batch cancel	cancels batch mode	
port {port_num} label set "{name}"	sets port label name	
port {port_num} label show	shows port label name	
port {port_num} initstate coldstart set {OFF=0|ON=1|REMEMBER=2}	sets port coldstart initialization	
port {port_num} initstate coldstart show	shows port coldstart initialization	
port {port_num} initstate delay set {num}	sets port init delay	
port {port_num} initstate delay show	shows port init delay	
port {port_num} repowerdelay set {num}	sets port repower delay	
port {port_num} repowerdelay show	shows port repower delay	
port {port_num} resettime set {num}	sets port reset duration	
port {port_num} resettime show	shows port reset duration	
port {port_num} watchdog enabled set {OFF=0|ON=1}	sets port watchdog to on/off	
port {port_num} watchdog enabled show	shows port watchdog state	

port {port_num} watchdog mode set {OFF=0|PORT_RESET=1|IP_MS=2|IP_MS_INV=3}	sets port watchdog mode
port {port_num} watchdog mode show	shows port watchdog mode
port {port_num} watchdog type set {WD_ICMP=0|WD_TCP=1}	sets port watchdog type
port {port_num} watchdog type show	shows port watchdog type
port {port_num} watchdog host set "{dns_name}"	sets port watchdog host target
port {port_num} watchdog host show	shows port watchdog host target
port {port_num} watchdog port set {ip_port}	sets port watchdog TCP port
port {port_num} watchdog port show	shows port watchdog TCP port
port {port_num} watchdog pinginterval set {num}	sets port watchdog ping interval
port {port_num} watchdog pinginterval show	shows port watchdog ping interval
port {port_num} watchdog pingretries set {num}	sets port watchdog ping retries
port {port_num} watchdog pingretries show	shows port watchdog ping retries
port {port_num} watchdog retrybooting set {OFF=0|ON=1}	sets port watchdog retry booting to on/off
port {port_num} watchdog retrybooting show	shows port watchdog retry booting state
port {port_num} watchdog bootretries set {num}	sets port watchdog retry boot timeout
port {port_num} watchdog bootretries show	hows port watchdog retry boot timeout
radius	enters cmd group "radius"
radius {PRIMARY=0|SECONDARY=1} enabled set <off=0/on=1>	enables radius client
radius {PRIMARY=0|SECONDARY=1} enabled show	show if radius client enabled
radius {PRIMARY=0|SECONDARY=1} server set "<dns_name>"	sets radius server address
radius {PRIMARY=0|SECONDARY=1} server show	shows radius server address
radius {PRIMARY=0|SECONDARY=1} password set "{passwd}"	sets radius server shared secret
radius {PRIMARY=0|SECONDARY=1} password hash set "{passwd}"	sets radius server crypted shared secret
radius {PRIMARY=0|SECONDARY=1} auth timeout set {num_secs}	sets server request timeout
radius {PRIMARY=0|SECONDARY=1} auth timeout show	shows server request timeout
radius {PRIMARY=0|SECONDARY=1} retries set {num}	sets server number of retries
radius {PRIMARY=0|SECONDARY=1} retries	

show	shows server number of retries
radius chap enabled set <off=0/on=1>	enables CHAP
radius chap enabled show	shows if CHAP is enabled
radius message auth set <off=0/on=1>	enables request message authentication
radius message auth show	shows if request message authentication is enabled
radius default timeout set {num_secs}	sets default session timeout (when not returned as Session-Timout Attribute)
radius default timeout show	shows default session timeout
snmp	enters cmd group "snmp"
snmp port set {ip_port}	sets SNMP UDP port
snmp port show	shows SNMP UDP port
snmp snmpget enabled set {OFF=0|ON=1}	enables SNMP GET cmds on/off
snmp snmpget enabled show	show if SNMP GET cmds are enabled
nmp snmpset enabled set {OFF=0|ON=1}	enables SNMP SET cmds on/off
snmp snmpset enabled show	show if SNMP SET cmds are enabled
snmp snmpv2 enabled set {OFF=0|ON=1}	enables SNMP v2 on/off
snmp snmpv2 enabled show	show if SNMP v2 is enabled
snmp snmpv2 public set "{text}"	enables SNMP v3 on/off
snmp snmpv2 public show	show if SNMP v3 isenabled
snmp snmpv2 private set "{text}"	sets SNMP v2 public cummnity
snmp snmpv2 private show	shows SNMP v2 public community
snmp snmpv3 enabled set {OFF=0|ON=1}	sets SNMP v2 private community
snmp snmpv3 enabled show	shows SNMP v2 private community
snmp snmpv3 username set "{text}"	sets SNMP v3 username
snmp snmpv3 username show	shows SNMP v3 username
snmp snmpv3 authalg set {NONE=0|MD5=1|SHA1=2|SHA256=3|SHA384=4|SHA512=5}	sets SNMP v3 authentication
snmp snmpv3 authalg show	show SNMP v3 authentication algorithm
snmp snmpv3 privalg set {NONE=0|DES=1|3DES=2|AES128=3|AES192=4|AES256=5|AES192*=6|AES256*=7}	sets SNMP v3 privacy algorithm

snmp snmpv3 privalg show	show SNMP v3 privacy algorithm
snmp snmpv3 authpasswd set "{passwd}"	sets SNMP v3 authentication password
snmp snmpv3 privpasswd set "{passwd}"	sets SNMP v3 privacy password
snmp snmpv3 authpasswd hash set "{passwd}"	sets SNMP v3 authentication hashed password
snmp snmpv3 privpasswd hash set "{passwd}"	sets SNMP v3 privacy hashed password
snmp trap type set {NONE=0|V1=1|V2=2|V3=3}	sets type of SNMP traps
snmp trap type show	show SNMP trap type
snmp trap receiver {trap_num} set "{dns_name}"	sets address and port of SNMP trap receiver {trap_num}
snmp trap receiver {trap_num} show	show address and port of SNMP trap receiver {trap_num}
syslog	enters cmd group "syslog"
syslog enabled set {OFF=0|ON=1}	enables syslog msgs on/off
syslog enabled show	show if syslog enabled
syslog server set "{dns_name}"	sets address of syslog server
syslog server show	shows address of syslog server
system	enters cmd group "system"
system restart	restarts device
system fabsettings	restore fab settings and restart device
system bootloader	enters bootloader mode
system flushdns	flush DNS cache
system uptime	number of seconds the device is running
system panel enabled set {OFF=0|ON=1}	blocks panel buttons when not enabled
system panel enabled show	shows if panel buttons are enabled
vt100	enters cmd group "vt100"
vt100 echo set {OFF=0|ON=1}	sets console echo state
vt100 echo show	shows console echo state
vt100 numeric set {OFF=0|ON=1}	sets numeric mode
vt100 numeric show	shows numeric mode state
vt100 reset	resets terminal

Notes

1. Legacy - The command has been replaced by a newer version
2. Command can be entered on any level
3. The output may show 2 lines - the 1st line shows the actual state, the 2nd line the status after reboot
4. The output may show several lines
5. N/A
6. Please see the **External Type and External Sensor Field Tables** for the correct sensor index

External Sensor Type Table "{sen_type}"

Constants "{7x01=0|7x04=0|7x02=1|7x05=1|7x06=2}"

Index	Description	Products
0	Temperature	7001, 7101, 7201
0	Temperature	7004, 7104, 7204
1	Temperature, Humidity	7002, 7102, 7202
1	Temperature, Humidity	7005, 7105, 7205
2	Temperature, Humidity, Air Pressure	7006, 7106, 7206

External Sensor Field Table "{sen_field}"

Index	Description	Unit
0	Temperature	°C
1	Humidity	%
2	Digital Input	bool
3	Air Pressure	hPa
4	Dew Point	°C
5	Dew Point Temperature Difference	°C

4.8 Modbus TCP

If Modbus TCP is activated in the configuration, the ports (relays) can be switched and the following data is callable:

- State of Port (relay)
- State of DC input
- Number of ports (relays)
- Number of energy sensors
- Measured values of energy sensors
- Measured values of the external sensors

This chapter is general for all Lindy devices. Depending on the device type, some ports or certain sensors are not available.

Address Range:

Device Resource	**Start**	**End**	**Modbus Data Type**
Power/Output Ports	0x000	0x3ff	Coils
DC Inputs	0x400	0x7ff	Discrete Inputs
Info Area	0x000	0x005	Input Registers
External Sensors	0x100	0x1ff	Input Registers
Line Energy Sensors	0x400	0x39ff	Input Registers
Port Energy Sensors	0x3a00	0x6fff	Input Registers

These functions are supported:

- Read Coils (0x01)

Reads the state of the ports (relay):

Request Code	1 Byte	0x01
Starting Address	2 Bytes	0x000 to 0x3ff
Quantity of coils	2 Bytes	1 to 0x400

Response Code	1 Byte	0x01
Byte count	1 Byte	n

Coil Status	n Byte	each Bit represents a state

· Read Discrete Inputs (0x02)

Reads state informations:

Request Code	1 Byte	0x02
Starting Address	2 Bytes	0x400 to 0x7ff
Quantity of Inputs	2 Bytes	1 to 0x400

Response Code	1 Byte	0x02
Byte count	1 Byte	n
Input Status	n Byte	each Bit represents a state

Address	**Information**
0x400 to 0x7ff	State of passive device Inputs
0x800	Stop Condition active (ENC 2302)
0x801	POE active
0x1000 to 0x100f	State of Power Sources

· Write Single Coil (0x05)

Sets the state of a port (relay):

Request Code	1 Byte	0x05
Output Address	2 Bytes	0x00 to 0x3ff
Output Value	2 Bytes	0x0000 or 0xff00

Response Code	1 Byte	0x05
Output Address	2 Bytes	n

· Write Multiple Coils (0x0F)

Sets the state of several ports (relays):

Request Code	1 Byte	0x0f
Starting Address	2 Bytes	0x00 to 0x3ff
Quantity of Outputs	2 Bytes	1 to 0x400
Byte count	1 Byte	n
Outputs Value	n x 1 Byte	each Bit represents a state

Response Code	1 Byte	0x0f
Starting Address	2 Bytes	0x00 to 0x3ff
Quantity of Outputs	2 Bytes	1 to 0x400

· Read Input Registers (0x04)

Read 16-bit values that contain different device information depending on the address:

Request Code	1 Byte	0x04
Starting Address	2 Bytes	0x0000 to 0xffff
Quantity of Inputs	2 Bytes	1 to 0x7d

Response Code	1 Byte	0x04
Byte count	1 Byte	2 x n
Input Status	n x 2 Byte	16-bit or 32-bit data

Various state information and measured values of the device are arranged in the input registers:

Address	**Width**	**Information**
0	16-bit	Number of Ports (Relay)
1	16-bit	Number of Ports with Energy Measurement
2	16-bit	Number of Banks
3	16-bit	Lines per Bank
4	16-bit	Phases per line
5	16-bit	Number of Inputs
0x100 to 0x1ff	16-bit (signed)	external Sensors
0x400 to 0x39ff	32-bit (signed)	Line Energy Sensors
0x3a00 to 0x6fff	32-bit (signed)	Port Energy Sensors

External Sensors:

The measured value of the external sensors are coded as fixed point arithmetic. For a factor of e.g. 0.1 in the unit the value must be divided by 10 in order to reach the real measured value. A value of 0x8000 means that no sensor is plugged into the corresponding port, or the corresponding field in the sensor is not available. The formula for the address is (the port numbers start at zero):

0x100 + Port * 8 + Offset

Offset	**Sensor Field**	**Unit**
0	Temperature	0.1 °C
1	Humidity	0.1 %
2	Digital Input	bool
3	Air Pressure	1 hPa (millibar)
4	Dew Point	0.1 °C
5	Dew Point Difference	0.1 °C

For example, the humidity of the second port has the address: 0x100 + 1 * 8 + 1 = 0x109

Energy Sensors:

We distinguish the line sensors (which correspond to the input circuits) and the port sensors, which measure the energy that is passed over the switched port. The measured values of the energy sensors are returned as signed 32-bit integers. The high-order 16-bits are starting on the even address, followed by the low-order 16-bits on the odd address. To calculate the address, there are the following formulas (the values for line, port and phase start at zero):

Line: 0x0400 + Line * 0x120 + Phase * 0x60 + Offset * 2

Port: 0x3a00 + Port * 0x120 + Phase * 0x60 + Offset * 2

For devices with only one phase, the phase is set to zero in the formula.

Examples:

"Power Active" for 1st line sensor and 3rd phase: 0x400 + 0 * 0x120 + 2 * 0x60 + 1 * 2 = 0x4C2

"Voltage" for 2nd line sensor and single phase device: 0x400 + 1 * 0x120 + 2 * 2 = 0x524

"Power Angle" for 4th port sensor and single phase device: 0x3a00 + 3 * 0x120 + 6 * 2 = 0x3d6c

Offset	Sensor Field	Unit
0	Absolute Active Energy	Wh
1	Power Active	W
2	Voltage	V
3	Current	mA
4	Frequency	0.01 hz
5	Power Factor	0.001
6	Power Angle	0.1 degree
7	Power Apparent	VA
8	Power Reactive	VAR
9	Absolute Active Energy Resettable	Wh
10	Absolute Reactive Energy	VARh
11	Absolute Reactive Energy Resettable	VARh
12	Reset Time - sec. since last Energy Counter Reset	s
13	Forward Active Energy	Wh
14	Forward Reactive Energy	VARh
15	Forward Active Energy Resettable	Wh
16	Forward Reactive Energy Resettable	VARh
17	Reverse Active Energy	Wh
18	Reverse Reactive Energy	VARh
19	Reverse Active Energy Resettable	Wh
20	Reverse Reactive Energy Resettable	VARh
21	Residual Current Type A	mA
22	Neutral Current	mA
23	Residual Current Type B RMS	0.1 mA
24	Residual Current Type B DC	0.1 mA

Whether the measured values "Residual Current" and "Neutral Current" are supported depends on the respective device model. For measured values such as "Neutral Current", which are independent of the phase, the same value is returned for all phases.

· Read Device Identification (0x2B / 0x0E)

Returns manufacturer name and device identification:

Request Code	1 Byte	0x2b
MEI Type	1 Byte	0x0e
Read Dev ID code	1 Byte	0x01
Object Id	1 Byte	0x00

Response Code	1 Byte	0x2b
MEI Type	1 Byte	0x0e
Read Dev ID code	1 Byte	0x01
Conformity Level	1 Byte	0x01

More Follows	1 Byte	0x00
NextObjectID	1 Byte	0x00
Number of Objects	1 Byte	0x03
Object ID	1 Byte	0x00
Object Length	1 Byte	n1
Object Value	n1 Bytes	"Company Id"
Object ID	1 Byte	0x00
Object Length	1 Byte	n2
Object Value	n2 Bytes	"Product Id"
Object ID	1 Byte	0x00
Object Length	1 Byte	n3
Object Value	n3 Bytes	"Product Version"

4.9 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

E-Mail messages

Email messages are triggered by the following events:

- Switching of the Ports
- Exceeding of the max / min values of attached sensors
- State change of digital sensor input ports

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 Ports
- Exceeding of the max / min values of attached sensors
- State change of digital sensor input ports

Syslog messages

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 Ports
- Exceeding of the max / min values of attached sensors
- State change of digital sensor input ports

CE Statement

CE Certification

This equipment complies with the requirements relating to Electromagnetic Compatibility Standards.
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: +49 (0)621 470050

LINDY Electronics Ltd
Sadler Forster Way
Stockton-on-Tees, TS17 9JY
England
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 Rücknahme Elektroschrott und Batterie-Entsorgung

Die Europäische Union hat mit der WEEE Direktive Regelungen für die Verschrottung und das Recycling von Elektro- und Elektronikprodukten geschaffen. Diese wurden im Elektro- und Elektronikgerätegesetz – ElektroG in deutsches Recht umgesetzt. Das Entsorgen von Elektro- und Elektronikgeräten über die Hausmülltonne ist verboten! Diese Geräte müssen den Sammel- und Rückgabesystemen zugeführt werden! Dort werden sie kostenlos entgegen genommen. Die Kosten für den weiteren Recyclingprozess übernehmen die Gerätehersteller.
LINDY bietet deutschen Endverbrauchern ein kostenloses Rücknahmesystem an, beachten Sie bitte, dass Batterien und Akkus den Produkten vor der Rückgabe an das Rücknahmesystem entnommen werden müssen und über die Sammel- und Rückgabesysteme für Batterien separat entsorgt werden müssen. Ausführliche Informationen zu diesen Themen finden Sie stets aktuell auf der LINDY Webseite im Fußbereich.

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.

No. 32662

1st Edition, October 2018

CE

lindy.com