Table of contents

1. Device Description 5
   1.1 Security Advice ................................................................. 6
   1.2 Content of Delivery ............................................................ 6
   1.3 Description ..................................................................... 6
   1.4 Installation ..................................................................... 7
      1.4.1 Terminal Assignment .................................................. 8
   1.5 Redundant Voltage Supply ............................................... 9
   1.6 Technical Specifications .................................................. 10
   1.7 Sensor .......................................................................... 10

2. Operating 13
   2.1 Operating the device directly ........................................... 14
   2.2 Control Panel .................................................................. 14
   2.3 Maintenance ................................................................... 16
      2.3.1 Maintenance Page ....................................................... 18
      2.3.2 Configuration Management ....................................... 19
      2.3.3 Bootloader Activation ................................................ 20

3. Configuration 22
   3.1 Output Ports ................................................................... 23
      3.1.1 Watchdog .................................................................. 24
   3.2 Input Ports ..................................................................... 26
   3.3 Ethernet ........................................................................ 26
      3.3.1 IP Address ................................................................. 27
      3.3.2 IP ACL ...................................................................... 28
      3.3.3 HTTP ....................................................................... 29
   3.4 Protocols ....................................................................... 30
      3.4.1 Console ...................................................................... 30
      3.4.2 Syslog ........................................................................ 31
      3.4.3 SNMP ........................................................................ 31
      3.4.4 Radius ....................................................................... 33
      3.4.5 Modbus TCP ............................................................. 34
   3.5 Sensors ......................................................................... 35
      3.5.1 Port Switching ............................................................ 36
   3.6 E-Mail ............................................................................ 37
   3.7 Front Panel .................................................................... 38

4. Specifications 39
   4.1 IP ACL .......................................................................... 40
   4.2 IPv6 .............................................................................. 40
# Table of contents

4.3 Radius ........................................................................................................................................... 41
4.4 Automated Access ......................................................................................................................... 41
4.5 SNMP ........................................................................................................................................... 42
  4.5.1 Device MIB 7213 .................................................................................................................. 44
  4.5.2 Device MIB 7214 .................................................................................................................. 45
4.6 SSL .............................................................................................................................................. 47
4.7 Console ....................................................................................................................................... 49
  4.7.1 Console Cmd 7213 .............................................................................................................. 52
  4.7.2 Console Cmd 7214 .............................................................................................................. 56
4.8 Modbus TCP ............................................................................................................................... 61
4.9 Messages ................................................................................................................................... 65

5. Support ....................................................................................................................................... 67
  5.1 Data Security .............................................................................................................................. 68
  5.2 Contact ..................................................................................................................................... 68
  5.3 Declaration of Conformity .......................................................................................................... 69
  5.4 FAQ .......................................................................................................................................... 69

Index ............................................................................................................................................. 70
Device Description
Device Description

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.
- The device may only be connected via a low voltage power supply to 230V AC (50 Hz or 60 Hz) power supply sockets.
- The device is intended for indoor use only. Do NOT install them in an area where excessive moisture or heat is present.
- Because of safety and approval issues it is not allowed to modify the device without our permission.
- The device is NOT a toy. It has to be used or stored out of range of children.
- Care about packaging material. Plastics has to be stored out of range of children. Please recycle the packaging materials.
- In case of further questions, about installation, operation or usage of the device, which are not clear after reading the manual, please do not hesitate to ask our support team.

1.2 Content of Delivery

The package includes:

- Expert Sensor Box 7213 / 7214
- AC Adaptor (12V DC, 1 A) (only ESB 7213-1 / 72113-2 / 7213-3 / 7214-1 / 72114-2 / 7214-3)
- Quick Start Guide
- CD-ROM with Manual and Software tools

1.3 Description

Depending on the model, the Expert Sensor Box 7213 / 7214 offers several environmental sensors. The device has the following features:

Devices with voltage input:
- Temperature Sensor (Expert Sensor Box 7213-1 / 7214-1)
- Sensors for temperature and humidity (Expert Sensor Box 7213-2 / 7214-2)
- Sensors for temperature, humidity and air pressure (Expert Sensor Box 7213-3 / 7214-3)

Devices with additional Power-over-Ethernet (PoE):
- Temperature Sensor (Expert Sensor Box 7213-11 / 7214-11)
- Sensors for temperature and humidity (Expert Sensor Box 7213-12 / 7214-12)
- Sensors for temperature, humidity and air pressure (Expert Sensor Box 7213-13 / 7214-13)
Device Description

General:
- Connection for 2 optional sensors for ambient monitoring (temperature, humidity and air pressure)
- Easy and flexible configuration via web browser, Windows or Linux program
- Generation of messages (e-mail, syslog and SNMP traps) depending on sensor values
- Firmware update possible during operation via Ethernet
- IPv6-ready
- HTTP / HTTPS, E-mail (SSL, STARTTLS), DHCP, Syslog
- SNMPv1, v2c, v3 (traps)
- Modbus TCP Support
- Console Commands with telnet support and serial interface.
- TLS 1.0, 1.1, 1.2
- Access protection through IP access control
- Low self-consumption
- Controllable via iOS and Android App Gude Control
- Developed and produced in Germany

Additionally with Expert Sensor Box 7214:
- An additional input for redundant voltage supply (12 V DC 1 A)
- A switchable, potential-free relay output with change-over contact (NO and NC), high switching capacity 36 V, 3 A
- The relay has high contact reliability even at very small loads
- Switch state and switch-on delay (0 ... 9999 seconds) can be set for the relay output after power failure
- Programmable on/off sequence
- A watchdog (ICMP / TCP) can be assigned to the output port
- Passive signal input for polling NO/NC devices (e.g., smoke detector, leak sensor, door contact)
- The signal input has a 12 V connector for supplying the NO/NC devices

1.4 Installation

1. Connector Sensor Port 1
2. Connector Sensor Port 2
3. Ethernet connector (RJ45) (with Pwr3 = only devices with PoE)
4. Status LED
5. Connector (Pwr1) for power supply 12 V DC, 1 A
Device Description

1. Housing for integrated Sensor
2. Connector (Pwr2) for power supply 12 V DC, 1 A (only ESB 7214)
3. Passive input (only ESB 7214)
4. Potential-free relay output (only ESB 7214)
5. Select Button

Power Supply

If the device has PoE or a second input for the supply voltage, all voltage sources can be connected at the same time. This allows redundancy in the power supply.

Start-up the device

- Connect the device (Pwr1 oder Pwr2) to the AC Adaptor (12 V DC, 1 A).
- Optional connect the device to a second AC Adaptor (12 V DC, 1 A).
- Plug the network cable into the Ethernet (RJ45).
- Attach the optional external sensors to the connectors.
- Connect the passive inputs and relay outputs to compatible devices.

1.4.1 Terminal Assignment

The terminal assignment of the terminals is printed on the housing surface:
**Device Description**

The digital signal input (input ports) goes to the logic state "LOW" when the pin "In" and the center pin "GND" are bridged, otherwise the state is "HI". The text outputs associated with the "LOW" and "HI" states can be defined in the Input Ports configuration. In the default configuration, the logic states are inverted so that the state "HI" is assumed for a bridged contact.

This means that there is only a connection between the center pin (COM) and the NC-pin (Normally Closed) for the output ports in the "Off" state. If the relay is in the "On" state, then there is only contact from the center pin (COM) to the NO-pin (Normally Open).

As an alternative to the connection of "In" and "GND", voltages of up to 24 V (\(V_{\text{In}}\)) can be connected to the input "In". For voltages less than 4 V the state goes to "LOW", for voltages greater than 8 V the "HI" state is assigned.

1.5 **Redundant Voltage Supply**

If the device and the connected switch support Power-over-Ethernet, the power supply via PoE has priority and the device is powered only via PoE. Alternatively, the device can be supplied via up to two power supply units. If both power supplies (only ESB 7214) are connected at the same time, the current is split up. The current distribution depends on the difference between the output voltages of the two power supplies.
## 1.6 Technical Specifications

| Interfaces | 1 x socket for power supply  
|            | 2 x RJ45 for external sensors  
|            | 1 x Ethernet connector RJ45  
|            | 1 x additional socket for power supply  
|            | 1 x switchable output  
|            | 1 x passive signal input  
| Network connectivity | 10/100 MBit/s 10baseT Ethernet  
| Protocols | TCP/IP, HTTP/HTTPS, SNMP v1/v2c/v3, SNMP traps, Syslog, E-Mail (SMTP), Modbus, Radius  
| Power Supply | AC Adaptor (12V DC, 1 A)  
| PoE Module (not all models) | 802.3af (802.3at Type 1) PoE, Class 0  
| Environment | 0°C - 50 °C  
|            | -20°C - 70 °C  
|            | 0% - 95% (non-condensing)  
| Case | Powdered steel case  
| Measurements | 80 mm x 100 mm x 34 mm (H x W x D)  
|            | 90 mm x 100 mm x 34 mm (H x W x D) (with flaps)  
| Weight | approx. 280g  

## 1.7 Sensor

Two external sensors can be connected to the Expert Sensor Box 7213 / 7214. The following sensors are currently available.
### Device Description

#### Humidity/Temperature Sensor 7102 (End-of-Life)

<table>
<thead>
<tr>
<th>Cable length</th>
<th>Connector</th>
<th>Temperature range</th>
<th>Air humidity range (non-condensing)</th>
<th>Air pressure range (full)</th>
<th>Air pressure range (ext)</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>= 2m</td>
<td>RJ45</td>
<td>-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)</td>
<td>0-100%, ±3% (maximum) and ±2% (typical)</td>
<td>±1 hPa (typical) at 300 ... 1100 hPa, 0 ... +40 °C</td>
<td>±1.7 hPa (typical) at 300 ... 1100 hPa, -20 ... 0 °C</td>
<td>IP68</td>
</tr>
</tbody>
</table>

---

### Product Table

<table>
<thead>
<tr>
<th>Product Name</th>
<th>7101</th>
<th>7104</th>
<th>7105</th>
<th>7106</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable length</td>
<td>= 2m</td>
<td>= 2m</td>
<td>= 2m</td>
<td>= 2m</td>
</tr>
<tr>
<td>Connector</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
</tr>
<tr>
<td>Temperature range</td>
<td>-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)</td>
<td>-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)</td>
<td>-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)</td>
<td>-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)</td>
</tr>
<tr>
<td>Air humidity range (non-condensing)</td>
<td>-</td>
<td>-</td>
<td>0-100%, ±3% (maximum) and ±2% (typical)</td>
<td>0-100%, ±3% (maximum) and ±2% (typical)</td>
</tr>
<tr>
<td>Air pressure range (full)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>±1 hPa (typical) at 300 ... 1100 hPa, 0 ... +40 °C</td>
</tr>
<tr>
<td>Air pressure range (ext)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>±1.7 hPa (typical) at 300 ... 1100 hPa, -20 ... 0 °C</td>
</tr>
<tr>
<td>Protection</td>
<td>IP68</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
### Device Description

<table>
<thead>
<tr>
<th>Product Name</th>
<th>7201</th>
<th>7202</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable length</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Connector</td>
<td>RJ45</td>
<td>RJ45</td>
</tr>
<tr>
<td>Temperature range</td>
<td>-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)</td>
<td>-20°C to +80°C at ±2°C (maximum) and ±1°C (typical)</td>
</tr>
<tr>
<td>Air humidity range</td>
<td>-</td>
<td>0-100%, ±3% (maximum) and ±2% (typical)</td>
</tr>
</tbody>
</table>

The sensors are detected automatically after connection. The green LED on the RJ45 sensor connector then lights up permanently. If the sensor value is displayed permanently on the display, the green LED flashes. The sensor values are displayed directly on the "Control Panel" website:

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>Temperature °C</th>
<th>Humidity %</th>
<th>Dew Point °C</th>
<th>Dew Diff °C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>7102</td>
<td>25.4</td>
<td>46.9</td>
<td>13.2</td>
<td>12.2</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>Temperature °C</th>
<th>Humidity %</th>
<th>Dew Point °C</th>
<th>Dew Diff °C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>7102</td>
<td>25.5</td>
<td>46.6</td>
<td>13.2</td>
<td>12.3</td>
</tr>
<tr>
<td>24h min</td>
<td>25.4</td>
<td>46.0</td>
<td>13.1</td>
<td>12.2</td>
<td></td>
</tr>
<tr>
<td>24h max</td>
<td>25.9</td>
<td>47.0</td>
<td>13.5</td>
<td>12.5</td>
<td></td>
</tr>
</tbody>
</table>

[Reset] [Reset] [Reset] [Reset] [Reset]
Operating
2 Operating

2.1 Operating the device directly

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.

Switching the relay with the button (only ESB 7214)

Press and hold the button for a total of 6 seconds. After the first 3 seconds the status LED flashes in a long ON, short OFF rhythm. Wait another 3 seconds, and the status LED flashes in a twice short, and once long rhythm. At this moment, press the button once again briefly to switch the relay, or if you wait 6 seconds instead, the device returns to its initial state.

2.2 Control Panel

⚠️ The relay output, the passive signal input and the additional input for the power supply are only available on the Expert Sensorbox 7214. The possibility of power supply via Power-over-Ethernet (PoE) also varies depending on the model.

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

The web page provides an overview of the switching state, the sensor, as well as the external sensors, provided that they are connected. When the port is clicked, a panel with buttons to control the port appears:

![Port Icon]

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.

![Status Icons]

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 port 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". The "Close" button dissolves the panel again.

Batchmode

The port can be set for a selectable period of time to the state "switch on" or "switch off". After the selected time it is automatically switched to the second preselected state.

![Batch Setting]

Optionally the device can be switched via a Perl script or external tools like wget. More information is available on our support wiki at www.gude.info/wiki.

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Logical State</th>
<th>Time Since Transition</th>
<th>Toggle Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input 1</td>
<td>Input</td>
<td>0: off / open</td>
<td>00:35:24</td>
<td>0</td>
</tr>
</tbody>
</table>

The web page contains a status overview of the passive signal input, the time since the last change, and a counter of the switching cycles. The name and text for a logical state of the input is configured in the chapter Configuration-Input Ports.
The voltage inputs (Pwr1 and Pwr2) shows if they are connected to a power supply or Power-over-Ethernet (PoE) is active.

2.3 Maintenance

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

**Maintenance 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 into Bootloader mode (see chapter Bootloader activation). The following functions can be executed using the GBL_Conf.exe application:

- 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)
Operating

- 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 www.gude.info and can also be found on the enclosed CD-ROM.

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 Page or from the Bootloader mode (see chapter Bootloader activation). 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.
2.3.1 Maintenance Page

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

- **Firmware Update**: Start a firmware update.
- **SSL Certificate Upload**: Saves your own SSL certificate. See chapter "SSL" for the generation of a certificate in the right format.
- **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.
- **Restart Device**: Restarts the device without changing the status of the relays.
- **Restore Fab Settings and Restart Device**: Performs a restart and resets the device to factory default.
- **Enter Bootloader Mode**: Jumps into bootloader mode, where additional settings can be made with GBL_Conf.exe.
- **Flush DNS Cache**: All entries in the DNS cache are discarded and address resolutions are requested again.
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:

```plaintext
e-mail enabled set 0
e-mail sender set "" #len: 0..100
e-mail recipient set "" #len: 0..100
e-mail server set "" #len: 0..100
e-mail port set 25
e-mail security set 0 #range: 0..2
e-mail auth set 0 #range: 0..2
e-mail user set "" #len: 0..100
e-mail passwd hash set "" #len: 0..100
e-mail 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-Button)

1) via push button:

- Press and hold the button for 3 seconds until the Status LED flashes slowly. If a display is available, "Press again to jump to BOOTLOADER" appears. Then briefly press the button again to activate the boot loader, or if you wait 3 seconds instead, the device returns to the initial state.

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-Button)**

1) via push button:

- Hold down the button for 3 seconds until the status LED flashes in a long-on, short-out rhythm. If a display is available, "Press again to jump to FIRMWARE" appears. Then briefly press the button again to activate the boot loader, or if you wait 6 seconds instead, the device returns to the initial state.

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 (1-Button)**

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
- Press and hold the button for 6 seconds. After the first 3 seconds, the status LED flashes in a long-on, short-out rhythm, and if a display is present, "Press again to jump to FIRMWARE" appears. Wait another 3 seconds, and the status LED flashes in a twice short, and once long rhythm. For devices with a display "Press again to FABSETTINGS" is shown. At this moment briefly press the button again to activate the factory reset, or if you wait 6 seconds instead, the device returns to the initial state.
- During reset to fabsetting, the status LED flashes rapidly, please wait until the LED blinks slowly (approx. 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 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 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.
**Configuration**

**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.
Configuration

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 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 www.gude.info/wiki.
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.
**Configuration**

**Test Radius Server**

- **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 Username and Password is accepted by the configured Radius Servers.

### 3.4.5 Modbus TCP

**Enable Modbus TCP:** Enables Modbus TCP support.

**Modbus 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

⚠️ This chapter describes in general the configuration of switching actions, using an example for a device with 2 ports. Models with only one port must be abstracted.

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.

![Temperature graph with temperature limits and hysteresis range](image)

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

- **When above Max value:** Switch port 1: Output Port to Off
- **When below Max value:** Switch port 1: Output Port to On
- **When above Min value:** Switch port 2: Output Port to On
- **When below Min value:** Switch port 2: Output Port to Off
Configuration

<table>
<thead>
<tr>
<th>actual temperature</th>
<th>actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>during configuration</td>
<td></td>
</tr>
<tr>
<td>70 °C</td>
<td>Port 1 Off (above max) + Port 2 On (above min)</td>
</tr>
<tr>
<td>45 °C</td>
<td>Port 1 On (below max) + Port 2 On (above min)</td>
</tr>
<tr>
<td>20 °C</td>
<td>Port 1 On (below max) + Port 2 Off (below min)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>from &quot;above max&quot;</th>
<th>to &quot;above max&quot;</th>
<th>to &quot;below max&quot;</th>
<th>to &quot;above min&quot;</th>
<th>to &quot;below min&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1 Off</td>
<td>-</td>
<td>P1 On</td>
<td>P1 On</td>
<td>P1 On + P2 Off</td>
</tr>
<tr>
<td>P1 Off</td>
<td>P2 Off</td>
<td>-</td>
<td>-</td>
<td>P2 Off</td>
</tr>
<tr>
<td>P1 Off + P2 On</td>
<td>P2 On</td>
<td>P2 On</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

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.
**Configuration**

**SMTP Connection Security**: Transmission via SSL or no encryption.

**SMTP Authentication (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

<table>
<thead>
<tr>
<th>Button Lock</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Image" /></td>
</tr>
</tbody>
</table>

**Button Lock**: Disables the front button (activates the key lock) with the exception of the bootloader activation (only ESB 7214).
Specifications
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:

<table>
<thead>
<tr>
<th>Entry in the IP ACL</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.123</td>
<td>the PC with IP Address &quot;192.168.0.123&quot; can access the device</td>
</tr>
<tr>
<td>192.168.0.1/24</td>
<td>all devices of subnet &quot;192.168.0.1/24&quot; can access the device</td>
</tr>
<tr>
<td>1234:4ef0::/64</td>
<td>all devices of subnet &quot;1234:4ef0::/64&quot; can access the device</td>
</tr>
</tbody>
</table>

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

4.2 IPv6

IPv6 Addresses

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

Address Notation

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

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

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

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

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

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

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):

<table>
<thead>
<tr>
<th>Interface</th>
<th>Scope of Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>read / write all configuration data</td>
</tr>
<tr>
<td></td>
<td>read / write all status information</td>
</tr>
<tr>
<td>Console</td>
<td>read / write all configuration data</td>
</tr>
<tr>
<td></td>
<td>read / write all status information</td>
</tr>
<tr>
<td>SNMP</td>
<td>read / write status of Power Ports (relays)</td>
</tr>
<tr>
<td></td>
<td>read / write names of Power Ports (relays)</td>
</tr>
<tr>
<td></td>
<td>read / write status of Port start configuration</td>
</tr>
<tr>
<td></td>
<td>read / write status Buzzer</td>
</tr>
</tbody>
</table>
Specifications

<table>
<thead>
<tr>
<th>Modbus TCP</th>
<th>read / write status of Power Ports (relays)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>read status of Inputs</td>
</tr>
<tr>
<td></td>
<td>read measurement values of external sensors</td>
</tr>
<tr>
<td></td>
<td>read measurement values of all energy sensors</td>
</tr>
</tbody>
</table>

The device can be controlled via HTTP interface with CGI commands and returns the internal configuration and status in JSON format. The structure of the CGI commands and the JSON data is explained in more detail in our Wiki article: http://wiki.gude.info/EPC_HTTP_Interface

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-ussm-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**
Specifications

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-SNMP 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 7213

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 "1.3.6.1.4.1.28507.60.1.1.1.1". A distinction is made in SNMP OID 's in between tables and scalars. OID scalar have the extension ".0" and only specify a value. In SNMP tables the "x" is replaced by an index (1 or greater) to address a value from the table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>OID</th>
<th>Type</th>
<th>Acc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>esb7213TrapCtrl</td>
<td></td>
<td>.66.1.1.1.1.0</td>
<td>Integer32</td>
<td>RW</td>
</tr>
<tr>
<td></td>
<td>0 = off 1 = Ver. 1 2 = Ver. 2c 3 = Ver. 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>esb7213TrapPlIndex</td>
<td></td>
<td>.66.1.1.12.1.1.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
</tbody>
</table>
Specifications

**esb7213TrapAddr**
A unique value, greater than zero, for each receiver slot.

**esb7213POE**
signals POE availability

**esb7213SensorIndex**
None

**esb7213TempSensor**
actual temperature

**esb7213HygroSensor**
actual humidity

**esb7213InputSensor**
logical state of input sensor

**esb7213AirPressure**
actual air pressure

**esb7213DewPoint**
dew point for actual temperature and humidity

**esb7213DewPointDiff**
difference between dew point and actual temperature (Temp - DewPoint)

**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 Sensor Field Table** for the right sensor index

**External Sensor Type Table "\{7x01=0|7x02=1|7x03=2\}"**

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Temperature</td>
<td>7001, 7101, 7201</td>
</tr>
<tr>
<td>1</td>
<td>Temperature, Humidity</td>
<td>7002, 7102, 7202</td>
</tr>
<tr>
<td>2</td>
<td>Temperature, Humidity, Air Pressure</td>
<td>7003, 7103, 7203</td>
</tr>
</tbody>
</table>

**External Sensor Field Table "\{sen_field\}"**

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Temperature</td>
<td>°C</td>
</tr>
<tr>
<td>1</td>
<td>Humidity</td>
<td>%</td>
</tr>
<tr>
<td>2</td>
<td>Digital Input</td>
<td>bool</td>
</tr>
<tr>
<td>3</td>
<td>Air Pressure</td>
<td>hPa</td>
</tr>
<tr>
<td>4</td>
<td>Dew Point</td>
<td>°C</td>
</tr>
<tr>
<td>5</td>
<td>Dew Point Temperature Difference</td>
<td>°C</td>
</tr>
</tbody>
</table>

**4.5.2 Device MIB 7214**

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 "1.3.6.1.4.1.28507.61.1.1.1.1". A distinction is made in SNMP OID 's in between tables and scalars. OID scalar have the extension ".0" and only specify a value. In SNMP tables the "x" is replaced by an index (1 or greater) to address a value from the table.
Specifications

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>OID</th>
<th>Type</th>
<th>Acc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>esb7214TrapCtrl</td>
<td>0 = off 1 = Ver. 1.2 = Ver. 2c 3 = Ver. 3</td>
<td>.67.1.1.1.1.1.0</td>
<td>Integer32</td>
<td>RW</td>
</tr>
<tr>
<td>esb7214TrapIPIndex</td>
<td>A unique value, greater than zero, for each receiver slot</td>
<td>.67.1.1.1.2.1.1.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214TrapAddr</td>
<td>DNS name or IP address specifying one Trap receiver slot. A port can optionally be specified: 'name:port' An empty string disables this slot</td>
<td>.67.1.1.1.2.1.2.x</td>
<td>OCTETS</td>
<td>RW</td>
</tr>
<tr>
<td>esb7214PortNumber</td>
<td>The number of Relay Ports</td>
<td>.67.1.3.1.1.1.0</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214PortIndex</td>
<td>A unique value, greater than zero, for each Relay Port.</td>
<td>.67.1.3.1.2.1.1.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214PortName</td>
<td>A textual string containing name of a Relay Port.</td>
<td>.67.1.3.1.2.1.2.x</td>
<td>OCTETS</td>
<td>RW</td>
</tr>
<tr>
<td>esb7214PortState</td>
<td>current state of a Relay Port</td>
<td>.67.1.3.1.2.1.3.x</td>
<td>INTEGER</td>
<td>RW</td>
</tr>
<tr>
<td>esb7214PortSwitchCount</td>
<td>The total number of switch actions occurred on a Relay Port. Does not count switch commands which will not switch the relay state, so just real relay switches are displayed here.</td>
<td>.67.1.3.1.2.1.4.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214PortStartupMode</td>
<td>set Mode of startup sequence (off, on , remember last state)</td>
<td>.67.1.3.1.2.1.5.x</td>
<td>INTEGER</td>
<td>RW</td>
</tr>
<tr>
<td>esb7214PortStartupDelay</td>
<td>Delay in sec for startup action</td>
<td>.67.1.3.1.2.1.6.x</td>
<td>Integer32</td>
<td>RW</td>
</tr>
<tr>
<td>esb7214PortRepowerTime</td>
<td>Delay in sec for repower port after switching off</td>
<td>.67.1.3.1.2.1.7.x</td>
<td>Integer32</td>
<td>RW</td>
</tr>
<tr>
<td>esb7214ActiveInputs</td>
<td>Number of supported Input Channels.</td>
<td>.67.1.5.6.1.0</td>
<td>Unsigned32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214InputIndex</td>
<td>None</td>
<td>.67.1.5.6.2.1.1.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214Input</td>
<td>Input state of device</td>
<td>.67.1.5.6.2.1.2.x</td>
<td>INTEGER</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214POE</td>
<td>signals POE availability</td>
<td>.67.1.5.10.0</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214SensorIndex</td>
<td>None</td>
<td>.67.1.6.1.1.1.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214TempSensor</td>
<td>actual temperature</td>
<td>.67.1.6.1.1.2.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214HygroSensor</td>
<td>actual humidity</td>
<td>.67.1.6.1.1.3.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214InputSensor</td>
<td>logical state of input sensor</td>
<td>.67.1.6.1.1.4.x</td>
<td>INTEGER</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214AirPressure</td>
<td>actual air pressure</td>
<td>.67.1.6.1.1.5.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214DewPoint</td>
<td>dew point for actual temperature and humidity</td>
<td>.67.1.6.1.1.6.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
<tr>
<td>esb7214DewPointDiff</td>
<td>difference between dew point and actual temperature (Temp - DewPoint)</td>
<td>.67.1.6.1.1.7.x</td>
<td>Integer32</td>
<td>RO</td>
</tr>
</tbody>
</table>

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 Sensor Field Table for the right sensor index

External Sensor Type Table "\{7x01=0\|7x02=1\|7x03=2\}"

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Temperature</td>
<td>7001, 7101, 7201</td>
</tr>
<tr>
<td>1</td>
<td>Temperature, Humidity</td>
<td>7002, 7102, 7202</td>
</tr>
<tr>
<td>2</td>
<td>Temperature, Humidity, Air Pressure</td>
<td>7003, 7103, 7203</td>
</tr>
</tbody>
</table>
Specifications

External Sensor Field Table "\{sen_field\}"

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Temperature</td>
<td>°C</td>
</tr>
<tr>
<td>1</td>
<td>Humidity</td>
<td>%</td>
</tr>
<tr>
<td>2</td>
<td>Digital Input</td>
<td>bool</td>
</tr>
<tr>
<td>3</td>
<td>Air Pressure</td>
<td>hPa</td>
</tr>
<tr>
<td>4</td>
<td>Dew Point</td>
<td>°C</td>
</tr>
<tr>
<td>5</td>
<td>Dew Point Temperature Difference</td>
<td>°C</td>
</tr>
</tbody>
</table>

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_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_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
Specifications

- 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 -----", 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.
Specifications

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 [27].

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. It is not necessary to use Telnet, in Raw Mode a simple TCP/IP connection is sufficient to send commands. The communication can also be performed automated (e.g. via scripting languages). The console features are configured through the web interface [35].

Command Set

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>back</td>
<td>go back one level</td>
</tr>
<tr>
<td>help</td>
<td>all commands of the actual level</td>
</tr>
<tr>
<td>help all</td>
<td>show all commands</td>
</tr>
<tr>
<td>logout</td>
<td>logout (only when login required)</td>
</tr>
<tr>
<td>quit</td>
<td>quit console</td>
</tr>
</tbody>
</table>

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:
 Specifications

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:

<table>
<thead>
<tr>
<th>Base</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>decimal (10)</td>
<td>11</td>
</tr>
<tr>
<td>hexadecimal (16)</td>
<td>0xb</td>
</tr>
<tr>
<td>octal (8)</td>
<td>013</td>
</tr>
<tr>
<td>binary (2)</td>
<td>0b1011</td>
</tr>
</tbody>
</table>

 Bit Field Parameter

Some parameters can take several values at the same time. In the following example, all values between 0 and 5 can be set. In the help, this can be recognized by the fact that the values are not separated by the "|" character, but by commas.

"{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"

To set EVT_SYSLOG and EVT_EMAIL in a command, you can use the following syntax:

>extsensor 1 2 0 events type set "EVT_SYSLOG,EVT_EMAIL"
OK.

or numeric

>extsensor 1 2 0 events type set "0,2"
OK.

Additionally you can set all values with "ALLSET" or encode any bit pattern as hexadecimal with a syntax like "#7f1a".

 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.
Specifications

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.

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

⚠️ 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.

Bundled Information
Specifications

The syntax of console commands does not make it easy to output bundled information with few commands. The following special commands make this easier:

a) External Sensors

>extsensor all show
E=1,L="7106",0="21.3°C",1="35.1%",3="1013hPa",4="5.2°C",5="16.0°C"
E=2,L="7102",0="21.2°C",1="35.4%",4="5.3°C",5="15.9°C"

The command lists one connected external sensor per line, and the individual measured values are separated by commas after the label name. The digit before the equal sign corresponds to the index field in the External Sensor Table.

b) Line Sensors

>linesensor all "0,1,2,3,12" show
L=1,L="Power Port",0="13000Wh",1="0W",2="225V",3="0A",12="998218s"
L=2,L="Power Port",0="13000Wh",1="0W",2="223V",3="0A",12="996199s"

This command outputs all line sensor values in one line. A list of all fields (according to the energy sensor table) is transferred as parameter. In this example these are the fields Absolute Active Energy (0), Power Active (1), Voltage (2), Current (3) and Reset Time (12).

c) Port Sensors

>portsensor all "0,1,2,3,12" show
P=1,L="Power Port",0="13000Wh",1="0W",2="225V",3="0A",12="998218s"
P=2,L="Power Port",0="13000Wh",1="0W",2="223V",3="0A",12="996199s"
... 
P=12,L="Power Port",0="13000Wh",1="0W",2="225V",3="0A",12="998218s"

This command outputs all port sensor values in one line. A list of all fields (according to the energy sensor table) is passed as parameter. In this example these are the fields Absolute Active Energy (0), Power Active (1), Voltage (2), Current (3) and Reset Time (12).

d) Displaying Port Relays

>port all state 0 show
P1=ON,P2=OFF,P3=ON,P4=OFF,P5=OFF,P6=OFF,P7=OFF,P8=ON

The command "port all state {MODE0=0|MODE1=1|MODE2=2} show" returns the switching state of all relays in 3 possible formats.

e) Switching Port Relays

#port all state set "1,2,12" 1

OK.

The command syntax "port all state set "(port_list)" (OFF=0|ON=1)" sets a list of ports to ON=1 or OFF=0.

4.7.1 Console Cmd 7213

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>logout</td>
<td>go to login prompt when enabled</td>
<td>2</td>
</tr>
</tbody>
</table>
### Specifications

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>quit</strong></td>
<td>quits telnet session - nothing in serial console</td>
</tr>
<tr>
<td><strong>back</strong></td>
<td>back one cmd level</td>
</tr>
<tr>
<td><strong>help</strong></td>
<td>show all cmds from this level</td>
</tr>
<tr>
<td><strong>help all</strong></td>
<td>show all cmds</td>
</tr>
<tr>
<td><strong>console</strong></td>
<td>enters cmd group &quot;console&quot;</td>
</tr>
<tr>
<td><strong>console version</strong></td>
<td>shows unique console version number</td>
</tr>
<tr>
<td>**console telnet enabled set {OFF=0</td>
<td>ON=1}**</td>
</tr>
<tr>
<td><strong>console telnet enabled show</strong></td>
<td>shows if telnet enabled</td>
</tr>
<tr>
<td><strong>console telnet port set {ip_port}</strong></td>
<td>sets telnet port</td>
</tr>
<tr>
<td><strong>console telnet port show</strong></td>
<td>shows telnet port</td>
</tr>
<tr>
<td>**console telnet raw set {OFF=0</td>
<td>ON=1}**</td>
</tr>
<tr>
<td><strong>console telnet raw show</strong></td>
<td>shows if raw mode enabled</td>
</tr>
<tr>
<td>**console telnet echo set {OFF=0</td>
<td>ON=1}**</td>
</tr>
<tr>
<td><strong>console telnet echo show</strong></td>
<td>shows if echo enabled</td>
</tr>
<tr>
<td>**console telnet activeNeg set {OFF=0</td>
<td>ON=1}**</td>
</tr>
<tr>
<td><strong>console telnet activeNeg show</strong></td>
<td>shows if active negotiation enabled</td>
</tr>
<tr>
<td>**console telnet login set {OFF=0</td>
<td>ON=1}**</td>
</tr>
<tr>
<td><strong>console telnet login show</strong></td>
<td>shows if login enabled</td>
</tr>
<tr>
<td>**console telnet login local set {OFF=0</td>
<td>ON=1}**</td>
</tr>
<tr>
<td><strong>console telnet login local show</strong></td>
<td>shows if local login enabled</td>
</tr>
<tr>
<td>**console telnet login radius set {OFF=0</td>
<td>ON=1}**</td>
</tr>
<tr>
<td><strong>console telnet login radius show</strong></td>
<td>shows if RADIUS login enabled</td>
</tr>
<tr>
<td>**console telnet login delay set {OFF=0</td>
<td>ON=1}**</td>
</tr>
<tr>
<td><strong>console telnet login delay show</strong></td>
<td>shows if login delay enabled</td>
</tr>
<tr>
<td><strong>console telnet user set &quot;{username}&quot;</strong></td>
<td>sets login user name</td>
</tr>
<tr>
<td><strong>console telnet user show</strong></td>
<td>shows login user name</td>
</tr>
<tr>
<td><strong>console telnet passwd set &quot;{passwd}&quot;</strong></td>
<td>sets login password</td>
</tr>
<tr>
<td><strong>console telnet passwd hash set &quot;{passwd}&quot;</strong></td>
<td>sets crypted SMTP password</td>
</tr>
<tr>
<td><strong>console telnet passwd hash show</strong></td>
<td>shows login hashed password</td>
</tr>
<tr>
<td><strong>email</strong></td>
<td>enters cmd group &quot;email&quot;</td>
</tr>
<tr>
<td>**email enabled set {OFF=0</td>
<td>ON=1}**</td>
</tr>
<tr>
<td><strong>email enabled show</strong></td>
<td>shows if email is enabled</td>
</tr>
<tr>
<td><strong>email sender set &quot;{email_addr}&quot;</strong></td>
<td>sets email sender address</td>
</tr>
<tr>
<td><strong>email sender show</strong></td>
<td>shows email sender address</td>
</tr>
<tr>
<td><strong>email recipient set &quot;{email_addr}&quot;</strong></td>
<td>sets email recipient address</td>
</tr>
<tr>
<td><strong>email recipient show</strong></td>
<td>shows email recipient address</td>
</tr>
<tr>
<td><strong>email server set &quot;{dns_name}&quot;</strong></td>
<td>sets email SMTP server address</td>
</tr>
<tr>
<td><strong>email server show</strong></td>
<td>shows email SMTP server address</td>
</tr>
<tr>
<td><strong>email port set {ip_port}</strong></td>
<td>sets email SMTP port</td>
</tr>
<tr>
<td><strong>email port show</strong></td>
<td>shows email SMTP port</td>
</tr>
<tr>
<td>**email security set {NONE=0</td>
<td>STARTTLS=1</td>
</tr>
<tr>
<td><strong>email security show</strong></td>
<td>shows SMTP connection security</td>
</tr>
<tr>
<td>**email auth set {NONE=0</td>
<td>PLAIN=1</td>
</tr>
<tr>
<td><strong>email auth show</strong></td>
<td>shows email authentication</td>
</tr>
<tr>
<td><strong>email user set &quot;{username}&quot;</strong></td>
<td>sets SMTP username</td>
</tr>
<tr>
<td><strong>email user show</strong></td>
<td>shows SMTP username</td>
</tr>
<tr>
<td><strong>email passwd set &quot;{passwd}&quot;</strong></td>
<td>sets SMTP password</td>
</tr>
<tr>
<td><strong>email passwd show&quot;&quot;</strong></td>
<td>shows SMTP password</td>
</tr>
<tr>
<td><strong>email testmail</strong></td>
<td>sends test email</td>
</tr>
<tr>
<td><strong>ethernet</strong></td>
<td>enters cmd group &quot;ethernet&quot;</td>
</tr>
<tr>
<td><strong>ethernet mac show</strong></td>
<td>shows MAC address</td>
</tr>
<tr>
<td><strong>ethernet link show</strong></td>
<td>shows ethernet link state</td>
</tr>
<tr>
<td>**ethernet phyprefer set {10MBIT_HD=0</td>
<td>10MBIT_FD=1</td>
</tr>
<tr>
<td><strong>ethernet phyprefer show</strong></td>
<td>shows preferred speed for PHY Auto Negotiation</td>
</tr>
<tr>
<td><strong>ethernet poe show</strong></td>
<td>shows if Power-over-Ethernet is activated</td>
</tr>
<tr>
<td><strong>extsensor</strong></td>
<td>enters cmd group &quot;extsensor&quot;</td>
</tr>
<tr>
<td><strong>extsensor {port_num} {sen_field} value show</strong></td>
<td>shows sensor value</td>
</tr>
<tr>
<td><strong>extsensor {port_num} {sen_type} label set &quot;{name}&quot;</strong></td>
<td>sets sensor name to label</td>
</tr>
<tr>
<td><strong>extsensor {port_num} {sen_type} label show</strong></td>
<td>shows label of sensor</td>
</tr>
<tr>
<td><strong>extsensor {port_num} {sen_type} type show</strong></td>
<td>shows type of sensor</td>
</tr>
<tr>
<td>**extsensor {port_num} {sen_type} {sen_field} events set {off=0</td>
<td>on=1}**</td>
</tr>
<tr>
<td><strong>extsensor {port_num} {sen_type} {sen_field} events show</strong></td>
<td>shows if sensor events are enabled</td>
</tr>
<tr>
<td><strong>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}</strong></td>
<td>shows what event types are enabled</td>
</tr>
<tr>
<td><strong>extsensor {port_num} {sen_type} {sen_field} events type show</strong></td>
<td>shows what event types are enabled</td>
</tr>
</tbody>
</table>
Specifications

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} minval set {num} sets minimum value for sensor 6
extsensor {port_num} {sen_type} {sen_field} minval 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 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

ip4 enters cmd group "ip4"
ip4 hostname set {"name"} sets device hostname
ip4 hostname show shows device hostname
ip4 address set {"ip_address"} sets IPv4 address
ip4 address show shows IPv4 address
ip4 netmask set {"ip_address"} sets IPv4 netmask
ip4 netmask show shows IPv4 netmask
ip4 gateway set {"ip_address"} sets IPv4 gateway address
ip4 gateway show shows IPv4 gateway address
ip4 dns set {"ip_address"} sets IPv4 DNS server address
ip4 dns show shows IPv4 DNS server address
ip4 dhcp enabled set {OFF=0|ON=1} enables IPv4 DHCP on/off
ip4 dhcp enabled show shows IPv4 DHCP state

ip6 enters cmd group "ip6"
ip6 enabled set {OFF=0|ON=1} enables IPv6 on/off
ip6 enabled show shows if IPv6 is enabled
ip6 routadv enabled set {OFF=0|ON=1} enables IPv6 router advertisement
ip6 routadv enabled show shows IPv6 router advertisement state
ip6 dhcp enabled set {OFF=0|ON=1} enables IPv6 DHCP on/off
ip6 dhcp enabled show shows if IPv6 DHCP is enabled
ip6 address show shows all IPv6 addresses
ip6 gateway show shows all IPv6 gateways
ip6 dns show shows all IPv6 DNS server
ip6 manual enabled set {OFF=0|ON=1} enables manual IPv6 addresses
ip6 manual enabled show shows if manual IPv6 addresses are enabled
ip6 manual address {1..4} set {"ip_address"} sets manual IPv6 address
ip6 manual address {1..4} show shows manual IPv6 address
ip6 manual gateway set {"ip_address"} sets manual IPv6 gateway address
ip6 manual gateway show shows manual IPv6 gateway address
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

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} enables 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
Specifications

modbus port set <ip_port>  sets Modbus TCP port
modbus port show  shows Modbus TCP port

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
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  shows if SNMP GET cmds are enabled
snmp snmpset enabled set {OFF=0|ON=1}  enables SNMP SET cmds on/off
snmp snmpset enabled show  shows if SNMP SET cmds are enabled
snmp snmpv2 public set "<text>"  sets SNMP v2 public community
snmp snmpv2 public show  shows SNMP v2 public 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 authpasswd set "<passwd>"  sets SNMP v3 authentication password
snmp snmpv3 authpasswd hash set "<passwd>"  sets SNMP v3 authentication hashed password
snmp snmpv3 privpasswd set "<passwd>"  sets SNMP v3 privacy 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  shows address and port of SNMP trap receiver (trap_num)

syslog
syslog enabled set {OFF=0|ON=1}  enables syslog msgs on/off
syslog enabled show  shows if syslog enabled
syslog server set "<dns_name>"  sets address of syslog server
syslog server show  shows address of syslog server

system
system restart  restarts device
system fabsettings  restore fab settings and restart device
Specifications

system bootloader enters bootloader mode
system flushdns flush DNS cache
system uptime number of seconds the device is running

vt100 enters cmd group "vt100"
vt100 echo set {OFF=0|ON=1} sets 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}"

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Temperature</td>
<td>7001, 7101, 7201</td>
</tr>
<tr>
<td>0</td>
<td>Temperature</td>
<td>7004, 7104, 7204</td>
</tr>
<tr>
<td>1</td>
<td>Temperature, Humidity</td>
<td>7002, 7102, 7202</td>
</tr>
<tr>
<td>1</td>
<td>Temperature, Humidity</td>
<td>7005, 7105, 7205</td>
</tr>
<tr>
<td>2</td>
<td>Temperature, Humidity, Air Pressure</td>
<td>7006, 7106, 7206</td>
</tr>
</tbody>
</table>

External Sensor Field Table "{sen_field}"

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Temperature</td>
<td>°C</td>
</tr>
<tr>
<td>1</td>
<td>Humidity</td>
<td>%</td>
</tr>
<tr>
<td>2</td>
<td>Digital Input</td>
<td>bool</td>
</tr>
<tr>
<td>3</td>
<td>Air Pressure</td>
<td>hPa</td>
</tr>
<tr>
<td>4</td>
<td>Dew Point</td>
<td>°C</td>
</tr>
<tr>
<td>5</td>
<td>Dew Point Temperature Difference</td>
<td>°C</td>
</tr>
</tbody>
</table>

4.7.2 Console Cmd 7214

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>logout</td>
<td>go to login prompt when enabled</td>
<td>2</td>
</tr>
<tr>
<td>quit</td>
<td>quits telnet session - nothing in serial console</td>
<td>2</td>
</tr>
<tr>
<td>back</td>
<td>back one cmd level</td>
<td>2</td>
</tr>
<tr>
<td>help</td>
<td>show all cmds from this level</td>
<td>2</td>
</tr>
<tr>
<td>help all</td>
<td>show all cmds</td>
<td>2</td>
</tr>
<tr>
<td>console</td>
<td>enters cmd group &quot;console&quot;</td>
<td></td>
</tr>
<tr>
<td>console version</td>
<td>shows unique console version number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>console telnet enabled set {OFF=0</td>
<td>ON=1}</td>
</tr>
<tr>
<td></td>
<td>console telnet enabled show</td>
<td>shows if telnet enabled</td>
</tr>
<tr>
<td></td>
<td>console telnet port set {ip_port}</td>
<td>sets telnet port</td>
</tr>
<tr>
<td></td>
<td>console telnet port show</td>
<td>shows telnet port</td>
</tr>
<tr>
<td></td>
<td>console telnet raw set {OFF=0</td>
<td>ON=1}</td>
</tr>
<tr>
<td></td>
<td>console telnet raw show</td>
<td>shows if raw mode enabled</td>
</tr>
</tbody>
</table>
Specifications

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

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  shows email authentication
email user set "{username}"  sets SMTP username
email user show  shows SMTP username
email passwd set "{passwd}"  sets SMTP password
email passwd show  shows SMTP password
email password hash set "{passwd}"  sets encrypted 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
ethernet poe show  shows if Power-over-Ethernet is activated

extsensor  enters cmd group "extsensor"
extsensor (port_num) (sen_field) value show  shows sensor value
nextsensor (port_num) (sen_type) label set "{name}"  sets sensor name to label
nextsensor (port_num) (sen_type) label show  shows label of sensor
nextsensor (port_num) (sen_type) type show  shows type of sensor
nextsensor (port_num) (sen_type) (sen_field) events set {off=0|on=1}  enables sensor events on/off
nextsensor (port_num) (sen_type) (sen_field) events show  shows if sensor events are enabled
nextsensor (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
nextsensor (port_num) (sen_type) (sen_field) maxval set {num}  sets maximum value for sensor
nextsensor (port_num) (sen_type) (sen_field) maxval show  shows maximum value for sensor
nextsensor (port_num) (sen_type) (sen_field) minval set {num}  sets minimum value for sensor
nextsensor (port_num) (sen_type) (sen_field) minval show  shows minimum value for sensor
nextsensor (port_num) (sen_type) (sen_field) hyst set {num}  sets hysteresis value for sensor
nextsensor (port_num) (sen_type) (sen_field) hyst show  shows hysteresis value for sensor
nextsensor (port_num) (sen_type) (sen_field) sets Port for Power Port Switching actions
### Specifications

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`{BELOWMIN=0</td>
<td>ABOVEMIN=1</td>
</tr>
<tr>
<td>`{BELOWMIN=0</td>
<td>ABOVEMIN=1</td>
</tr>
<tr>
<td>`{BELOWMIN=0</td>
<td>ABOVEMIN=1</td>
</tr>
<tr>
<td>`{BELOWMIN=0</td>
<td>ABOVEMIN=1</td>
</tr>
<tr>
<td>`{BELOWMIN=0</td>
<td>ABOVEMIN=1</td>
</tr>
<tr>
<td>`{BELOWMIN=0</td>
<td>ABOVEMIN=1</td>
</tr>
<tr>
<td><code>extsensor {port_num} {sen_type} {sen_field}</code></td>
<td></td>
</tr>
<tr>
<td><code>extsensor {port_num} {sen_type} {sen_field}</code></td>
<td>sets Port state for Power Port Switching actions</td>
</tr>
<tr>
<td><code>extsensor {port_num} {sen_type} {sen_field}</code></td>
<td>shows Port for Power Port Switching actions</td>
</tr>
<tr>
<td><code>extsensor period set </code>{24H=0</td>
<td>12H=1</td>
</tr>
<tr>
<td><code>extsensor period show</code></td>
<td>shows sensor Min/Max measurement period</td>
</tr>
<tr>
<td><code>http</code></td>
<td>enters cmd group &quot;http&quot;</td>
</tr>
<tr>
<td><code>http server set </code>{HTTP_BOTH=0</td>
<td>HTTPS_ONLY=1</td>
</tr>
<tr>
<td><code>http server show</code></td>
<td>shows webserver accepting connection types</td>
</tr>
<tr>
<td><code>http port set </code>{ip_port}``</td>
<td>sets http port</td>
</tr>
<tr>
<td><code>http port show</code></td>
<td>shows http port</td>
</tr>
<tr>
<td><code>http portssl set </code>{ip_port}``</td>
<td>sets https port</td>
</tr>
<tr>
<td><code>http portssl show</code></td>
<td>shows https port</td>
</tr>
<tr>
<td><code>http ajax enabled set </code>{OFF=0</td>
<td>ON=1}``</td>
</tr>
<tr>
<td><code>http admin enabled show</code></td>
<td>shows if admin password enabled</td>
</tr>
<tr>
<td><code>http passwd enabled set </code>{OFF=0</td>
<td>ON=1}``</td>
</tr>
<tr>
<td><code>http passwd enable show</code></td>
<td>shows if http password enabled</td>
</tr>
<tr>
<td><code>http passwd user set </code>{passwd}``</td>
<td>sets http user password</td>
</tr>
<tr>
<td><code>http passwd admin set </code>{passwd}``</td>
<td>sets http admin password</td>
</tr>
<tr>
<td><code>http passwd hash user set </code>{passwd}``</td>
<td>sets hashed http user password</td>
</tr>
<tr>
<td><code>http passwd admin set </code>{passwd}``</td>
<td>sets hashed http admin password</td>
</tr>
<tr>
<td><code>input</code></td>
<td>enters cmd group &quot;input&quot;</td>
</tr>
<tr>
<td><code>input {port_num} state show</code></td>
<td>shows input state</td>
</tr>
<tr>
<td>`input all state {MODE0=0</td>
<td>MODE1=1</td>
</tr>
<tr>
<td><code>input {port_num} name set </code>{name}``</td>
<td>sets sensor name to label</td>
</tr>
<tr>
<td><code>input {port_num} name show</code></td>
<td>shows label of sensor</td>
</tr>
<tr>
<td><code>input {port_num} invert enabled set </code>{off=0</td>
<td>on=1}``</td>
</tr>
<tr>
<td><code>input {port_num} invert enabled show</code></td>
<td>shows if input inverted</td>
</tr>
<tr>
<td>`input {port_num} label {LOW=0</td>
<td>HIGH=1}<code>set</code>{name}`</td>
</tr>
<tr>
<td>`input {port_num} label {LOW=0</td>
<td>HIGH=1}` show</td>
</tr>
<tr>
<td><code>input {port_num} events set </code>{off=0</td>
<td>on=1}``</td>
</tr>
<tr>
<td><code>input {port_num} events show</code></td>
<td>shows if input events are enabled</td>
</tr>
<tr>
<td><code>input {port_num} events type set </code>{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}``</td>
<td>enables different event types</td>
</tr>
<tr>
<td><code>input {port_num} events type show</code></td>
<td>shows what event types are enabled</td>
</tr>
<tr>
<td><code>input {port_num} port set </code>{LOW=0</td>
<td>HIGH=1}<code> </code>{port_num}``</td>
</tr>
<tr>
<td><code>input {port_num} port show</code></td>
<td>shows Port for Power Port Switching actions</td>
</tr>
<tr>
<td><code>input {port_num} port state set </code>{OFF=0</td>
<td>ON=1</td>
</tr>
<tr>
<td><code>input {port_num} port state show</code></td>
<td>shows Port for Power Port Switching actions</td>
</tr>
<tr>
<td><code>input volt3 state show</code></td>
<td>shows state of 3V input voltage `{ON=1</td>
</tr>
<tr>
<td><code>input volt12 state set </code>{OFF=0</td>
<td>VLO=1</td>
</tr>
<tr>
<td><code>input volt12 state show</code></td>
<td>shows state of 12V input voltage `{OFF=0</td>
</tr>
</tbody>
</table>

### ip4

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip4 hostname set </code>{name}``</td>
<td>sets device hostname</td>
</tr>
<tr>
<td><code>ip4 hostname show</code></td>
<td>shows device hostname</td>
</tr>
<tr>
<td><code>ip4 address set </code>{ip_address}``</td>
<td>sets IPv4 address</td>
</tr>
<tr>
<td><code>ip4 address show</code></td>
<td>shows IPv4 address</td>
</tr>
<tr>
<td><code>ip4 netmask set </code>{ip_address}``</td>
<td>sets IPv4 netmask</td>
</tr>
<tr>
<td><code>ip4 netmask show</code></td>
<td>shows IPv4 netmask</td>
</tr>
<tr>
<td><code>ip4 gateway set </code>{ip_address}``</td>
<td>sets IPv4 gateway address</td>
</tr>
<tr>
<td><code>ip4 gateway show</code></td>
<td>shows IPv4 gateway address</td>
</tr>
<tr>
<td><code>ip4 dns set </code>{ip_address}``</td>
<td>sets IPv4 DNS server address</td>
</tr>
<tr>
<td><code>ip4 dns show</code></td>
<td>shows IPv4 DNS server address</td>
</tr>
<tr>
<td><code>ip4 dhcp enabled set </code>{OFF=0</td>
<td>ON=1}``</td>
</tr>
<tr>
<td><code>ip4 dhcp enabled show</code></td>
<td>shows IPv4 DHCP state</td>
</tr>
</tbody>
</table>

### ip6

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip6</code></td>
<td>enters cmd group &quot;ip6&quot;</td>
</tr>
</tbody>
</table>
Specifications

```
ip6 enabled set {OFF=0|ON=1}          enables IPv6 on/off
ip6 enabled show                      shows if IPv6 is enabled
ip6 routadv enabled set {OFF=0|ON=1}  enables IPv6 router advertisement
ip6 routadv enabled show              shows IPv6 router advertisement state
ip6 dhcp enabled set {OFF=0|ON=1}     enables IPv6 DHCP on/off
ip6 dhcp enabled show                 shows if IPv6 DHCP is enabled
ip6 address show all                 show all IPv6 addresses
ip6 gateway show all                 show all IPv6 gateways
ip6 dns show                          show all IPv6 DNS servers
ip6 manual enabled set {OFF=0|ON=1}   enables manual IPv6 addresses
ip6 manual enabled show               shows if manual IPv6 addresses are enabled
ip6 manual address (1..4) set "(ip_address)"  sets manual IPv6 address
ip6 manual address (1..4) show        shows manual IPv6 address
ip6 manual gateway set "(ip_address)" sets manual IPv6 gateway address
ip6 manual gateway show               shows manual IPv6 gateway address
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
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
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|ON=1} {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_TCP=0|WD_ICMP=0}  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 pingretryset {num}  sets port watchdog ping retries
port (port_num) watchdog pingretryset 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  shows port watchdog retry boot timeout
```
### Specifications

**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
shows 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 encrypted 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
shows if SNMP GET cmds are enabled

snmp snmpset enabled set {OFF=0|ON=1}
enables SNMP SET cmds on/off

snmp snmpset enabled show
shows if SNMP SET cmds are enabled

snmp snmpv2 enabled set {OFF=0|ON=1}
enables SNMP v2 on/off

snmp snmpv2 enabled show
shows if SNMP v2 is enabled

snmp snmpv2 public set "(text)"
enables SNMP v3 is enabled

snmp snmpv2 public show
shows if SNMP v3 is enabled

snmp snmpv2 private set "<text>"
sets SNMP v2 public community

snmp snmpv2 private show
shows SNMP v2 private community

snmp snmpv3 enabled set {OFF=0|ON=1}
enables SNMP v3 private community

snmp snmpv3 enabled show
shows SNMP v3 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}
enables SNMP v3 authentication

snmp snmpv3 authalg show
shows SNMP v3 authentication algorithm

snmp snmpv3 privalg show
shows SNMP v3 privacy algorithm

snmp snmpv3 privalg set "(text)"
sets SNMP v3 privacy algorithm

snmp snmpv3 privpasswd set "(passwd)"
sets SNMP v3 private password

snmp snmpv3 privpasswd show
shows SNMP v3 private password

snmp snmpv3 auth passwd set "(passwd)"
sets SNMP v3 authentication password

snmp snmpv3 auth passwd show
shows SNMP v3 authentication password

snmp snmpv3 auth passwd hash set "(passwd)"
sets SNMP v3 authentication hashed password

snmp snmpv3 auth passwd hash show
shows SNMP v3 authentication hashed password

snmp trap type set {NONE=0|V1=1|V2=2|V3=3}
sets type of SNMP traps

snmp trap type show
shows 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
shows 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
shows 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
### Specifications

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system uptime</td>
<td>number of seconds the device is running</td>
</tr>
<tr>
<td>vt100</td>
<td>enters cmd group &quot;vt100&quot;</td>
</tr>
<tr>
<td>vt100 echo set</td>
<td>sets console echo state</td>
</tr>
<tr>
<td>vt100 echo show</td>
<td>shows console echo state</td>
</tr>
<tr>
<td>vt100 numeric set</td>
<td>sets numeric mode</td>
</tr>
<tr>
<td>vt100 numeric show</td>
<td>shows numeric mode state</td>
</tr>
<tr>
<td>vt100 reset</td>
<td>resets terminal</td>
</tr>
</tbody>
</table>

### 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}"

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Temperature</td>
<td>7001, 7101, 7201</td>
</tr>
<tr>
<td>0</td>
<td>Temperature</td>
<td>7004, 7104, 7204</td>
</tr>
<tr>
<td>1</td>
<td>Temperature, Humidity</td>
<td>7002, 7102, 7202</td>
</tr>
<tr>
<td>1</td>
<td>Temperature, Humidity</td>
<td>7005, 7105, 7205</td>
</tr>
<tr>
<td>2</td>
<td>Temperature, Humidity, Air Pressure</td>
<td>7006, 7106, 7206</td>
</tr>
</tbody>
</table>

#### External Sensor Field Table "{sen_field}"

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Temperature</td>
<td>°C</td>
</tr>
<tr>
<td>1</td>
<td>Humidity</td>
<td>%</td>
</tr>
<tr>
<td>2</td>
<td>Digital Input</td>
<td>bool</td>
</tr>
<tr>
<td>3</td>
<td>Air Pressure</td>
<td>hPa</td>
</tr>
<tr>
<td>4</td>
<td>Dew Point</td>
<td>°C</td>
</tr>
<tr>
<td>5</td>
<td>Dew Point Temperature Difference</td>
<td>°C</td>
</tr>
</tbody>
</table>

### 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 Gude devices. Depending on the device type, some
ports or certain sensors are not available.

**Address Range:**

<table>
<thead>
<tr>
<th>Device Resource</th>
<th>Start</th>
<th>End</th>
<th>Modbus Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power/Output Ports</td>
<td>0x000</td>
<td>0x3ff</td>
<td>Coils</td>
</tr>
<tr>
<td>DC Inputs</td>
<td>0x400</td>
<td>0x7ff</td>
<td>Discrete Inputs</td>
</tr>
<tr>
<td>Info Area</td>
<td>0x000</td>
<td>0x005</td>
<td>Input Registers</td>
</tr>
<tr>
<td>External Sensors</td>
<td>0x100</td>
<td>0x1ff</td>
<td>Input Registers</td>
</tr>
<tr>
<td>Line Energy Sensors</td>
<td>0x400</td>
<td>0x3ff</td>
<td>Input Registers</td>
</tr>
<tr>
<td>Port Energy Sensors</td>
<td>0x3a00</td>
<td>0x6ff</td>
<td>Input Registers</td>
</tr>
</tbody>
</table>

These functions are supported:

- **Read Coils (0x01)**

  Reads the state of the ports (relay):

<table>
<thead>
<tr>
<th>Request Code</th>
<th>1 Byte</th>
<th>0x01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Address</td>
<td>2 Bytes</td>
<td>0x000 to 0x3ff</td>
</tr>
<tr>
<td>Quantity of coils</td>
<td>2 Bytes</td>
<td>1 to 0x400</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response Code</th>
<th>1 Byte</th>
<th>0x01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte count</td>
<td>1 Byte</td>
<td>n</td>
</tr>
<tr>
<td>Coil Status</td>
<td>n Byte</td>
<td>each Bit represents a state</td>
</tr>
</tbody>
</table>

- **Read Discrete Inputs (0x02)**

  Reads state informations:

<table>
<thead>
<tr>
<th>Request Code</th>
<th>1 Byte</th>
<th>0x02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Address</td>
<td>2 Bytes</td>
<td>0x400 to 0x7ff</td>
</tr>
<tr>
<td>Quantity of Inputs</td>
<td>2 Bytes</td>
<td>1 to 0x400</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response Code</th>
<th>1 Byte</th>
<th>0x02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte count</td>
<td>1 Byte</td>
<td>n</td>
</tr>
<tr>
<td>Input Status</td>
<td>n Byte</td>
<td>each Bit represents a state</td>
</tr>
</tbody>
</table>

**Address**

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x400 to 0x7ff</td>
</tr>
<tr>
<td>0x800</td>
</tr>
<tr>
<td>0x801</td>
</tr>
<tr>
<td>0x1000 to 0x100f</td>
</tr>
</tbody>
</table>

- **Write Single Coil (0x05)**

  Sets the state of a port (relay):

<table>
<thead>
<tr>
<th>Request Code</th>
<th>1 Byte</th>
<th>0x05</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Address</td>
<td>2 Bytes</td>
<td>0x000 to 0x3ff</td>
</tr>
<tr>
<td>Output Value</td>
<td>2 Bytes</td>
<td>0x00000 or 0xff00</td>
</tr>
</tbody>
</table>
Specifications

<table>
<thead>
<tr>
<th>Response Code</th>
<th>1 Byte</th>
<th>0x05</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Address</td>
<td>2 Bytes</td>
<td>n</td>
</tr>
</tbody>
</table>

- **Write Multiple Coils (0x0F)**

Sets the state of several ports (relays):

<table>
<thead>
<tr>
<th>Request Code</th>
<th>1 Byte</th>
<th>0x0f</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Address</td>
<td>2 Bytes</td>
<td>0x00 to 0x3ff</td>
</tr>
<tr>
<td>Quantity of Outputs</td>
<td>2 Bytes</td>
<td>1 to 0x400</td>
</tr>
<tr>
<td>Byte count</td>
<td>1 Byte</td>
<td>n</td>
</tr>
<tr>
<td>Outputs Value</td>
<td>n x 1 Byte</td>
<td>each Bit represents a state</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response Code</th>
<th>1 Byte</th>
<th>0x0f</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Address</td>
<td>2 Bytes</td>
<td>0x00 to 0x3ff</td>
</tr>
<tr>
<td>Quantity of Outputs</td>
<td>2 Bytes</td>
<td>1 to 0x400</td>
</tr>
</tbody>
</table>

- **Read Input Registers (0x04)**

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

<table>
<thead>
<tr>
<th>Request Code</th>
<th>1 Byte</th>
<th>0x04</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Address</td>
<td>2 Bytes</td>
<td>0x0000 to 0xffff</td>
</tr>
<tr>
<td>Quantity of Inputs</td>
<td>2 Bytes</td>
<td>1 to 0x7d</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response Code</th>
<th>1 Byte</th>
<th>0x04</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte count</td>
<td>1 Byte</td>
<td>2 x n</td>
</tr>
<tr>
<td>Input Status</td>
<td>n x 2 Byte</td>
<td>16-bit or 32-bit data</td>
</tr>
</tbody>
</table>

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

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

**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):
Specifications

0x100 + Port * 8 + Offset

<table>
<thead>
<tr>
<th>Offset</th>
<th>Sensor Field</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Temperature</td>
<td>0.1 °C</td>
</tr>
<tr>
<td>1</td>
<td>Humidity</td>
<td>0.1 %</td>
</tr>
<tr>
<td>2</td>
<td>Digital Input</td>
<td>bool</td>
</tr>
<tr>
<td>3</td>
<td>Air Pressure</td>
<td>1 hPa (millibar)</td>
</tr>
<tr>
<td>4</td>
<td>Dew Point</td>
<td>0.1 °C</td>
</tr>
<tr>
<td>5</td>
<td>Dew Point Difference</td>
<td>0.1 °C</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Offset</th>
<th>Sensor Field</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Absolute Active Energy</td>
<td>Wh</td>
</tr>
<tr>
<td>1</td>
<td>Power Active</td>
<td>W</td>
</tr>
<tr>
<td>2</td>
<td>Voltage</td>
<td>V</td>
</tr>
<tr>
<td>3</td>
<td>Current</td>
<td>mA</td>
</tr>
<tr>
<td>4</td>
<td>Frequency</td>
<td>0.01 hz</td>
</tr>
<tr>
<td>5</td>
<td>Power Factor</td>
<td>0.001</td>
</tr>
<tr>
<td>6</td>
<td>Power Angle</td>
<td>0.1 degree</td>
</tr>
<tr>
<td>7</td>
<td>Power Apparent</td>
<td>VA</td>
</tr>
<tr>
<td>8</td>
<td>Power Reactive</td>
<td>VAR</td>
</tr>
<tr>
<td>9</td>
<td>Absolute Active Energy Resettable</td>
<td>Wh</td>
</tr>
<tr>
<td>10</td>
<td>Absolute Reactive Energy</td>
<td>VARh</td>
</tr>
<tr>
<td>11</td>
<td>Absolute Reactive Energy Resettable</td>
<td>VARh</td>
</tr>
<tr>
<td>12</td>
<td>Reset Time - sec. since last Energy Counter Reset</td>
<td>s</td>
</tr>
<tr>
<td>13</td>
<td>Forward Active Energy</td>
<td>Wh</td>
</tr>
<tr>
<td>14</td>
<td>Forward Reactive Energy</td>
<td>VARh</td>
</tr>
<tr>
<td>15</td>
<td>Forward Active Energy Resettable</td>
<td>Wh</td>
</tr>
</tbody>
</table>
## Specifications

<table>
<thead>
<tr>
<th>No.</th>
<th>Specification</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Forward Reactive Energy Resettable</td>
<td>VARh</td>
</tr>
<tr>
<td>17</td>
<td>Reverse Active Energy</td>
<td>Wh</td>
</tr>
<tr>
<td>18</td>
<td>Reverse Reactive Energy</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Reverse Active Energy Resettable</td>
<td>Wh</td>
</tr>
<tr>
<td>20</td>
<td>Reverse Reactive Energy Resettable</td>
<td>VARh</td>
</tr>
<tr>
<td>21</td>
<td>Residual Current Type A</td>
<td>mA</td>
</tr>
<tr>
<td>22</td>
<td>Neutral Current</td>
<td>mA</td>
</tr>
<tr>
<td>23</td>
<td>Residual Current Type B RMS</td>
<td>0.1 mA</td>
</tr>
<tr>
<td>24</td>
<td>Residual Current Type B DC</td>
<td>0.1 mA</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Request Code</th>
<th>1 Byte</th>
<th>0x2b</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEI Type</td>
<td>1 Byte</td>
<td>0x0e</td>
</tr>
<tr>
<td>Read Dev ID</td>
<td>1 Byte</td>
<td>0x01</td>
</tr>
<tr>
<td>Object Id</td>
<td>1 Byte</td>
<td>0x00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response Code</th>
<th>1 Byte</th>
<th>0x2b</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEI Type</td>
<td>1 Byte</td>
<td>0x0e</td>
</tr>
<tr>
<td>Read Dev ID</td>
<td>1 Byte</td>
<td>0x01</td>
</tr>
<tr>
<td>Conformity Level</td>
<td>1 Byte</td>
<td>0x01</td>
</tr>
<tr>
<td>More Follows</td>
<td>1 Byte</td>
<td>0x00</td>
</tr>
<tr>
<td>NextObjectID</td>
<td>1 Byte</td>
<td>0x00</td>
</tr>
<tr>
<td>Number of Objects</td>
<td>1 Byte</td>
<td>0x03</td>
</tr>
<tr>
<td>Object ID</td>
<td>1 Byte</td>
<td>0x00</td>
</tr>
<tr>
<td>Object Length</td>
<td>1 Byte</td>
<td>n1</td>
</tr>
<tr>
<td>Object Value</td>
<td>n1 Bytes</td>
<td>&quot;Company Id&quot;</td>
</tr>
<tr>
<td>Object ID</td>
<td>1 Byte</td>
<td>0x00</td>
</tr>
<tr>
<td>Object Length</td>
<td>1 Byte</td>
<td>n2</td>
</tr>
<tr>
<td>Object Value</td>
<td>n2 Bytes</td>
<td>&quot;Product Id&quot;</td>
</tr>
<tr>
<td>Object ID</td>
<td>1 Byte</td>
<td>0x00</td>
</tr>
<tr>
<td>Object Length</td>
<td>1 Byte</td>
<td>n3</td>
</tr>
<tr>
<td>Object Value</td>
<td>n3 Bytes</td>
<td>&quot;Product Version&quot;</td>
</tr>
</tbody>
</table>

## 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
- Loss / return of voltage at power supply (only ESB 7214)
- 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 (e.g. 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
- Loss / return of voltage at power supply (only ESB 7214)
- Exceeding of the max / min values of attached sensors
- State change of digital sensor input ports
5 Support

You will find the latest product software on our website at www.gude.info available for download. If you have further questions about installation or operation of the unit, please contact our support team. Furthermore, we present in our support wiki at www.gude.info/wiki FAQs and configuration examples.

5.1 Data Security

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

- Check that the HTTP password is switched on.
- Set up your own HTTP password.
- Allow access to HTTP via SSL only.
- Authentication and encryption is activated in SNMPv3.
- SNMP v2 access is disabled.
- enable STARTTLS or SSL in the e-mail configuration.
- Archive configuration files securely.
- In the IP ACL, enter only the devices that require access to HTTP or SNMP.
- Because Telnet is unencrypted, only use it in a secure environment.
- Since Modbus TCP is not encrypted, only activate it in a secure environment.
- Activate "Message Authentication" in RADIUS.

When accessed from the Internet

- Use a randomized password with at least 32 characters.
- If possible, place the device behind a firewall.

5.2 Contact

GUDE Systems GmbH
Von-der-Wettern-Straße 23
51149 Cologne
Germany

Phone: +49-221-912 90 97
Fax: +49-221-912 90 98
E-Mail: mail@gude.info
Internet: www.gude.info
shop.gude.info

Managing Director: Dr.-Ing. Michael Gude

District Court: Köln, HRB-Nr. 17 7 84
WEEE-number: DE 58173350
Value added tax identification number (VAT): DE 122778228
5.3 Declaration of Conformity

This product from the Expert Sensor Box 7213 / 7214 series is in conformity with the European directives for CE marking applicable to this product. The complete CE declaration of conformity for this product can be found on the website www.gude.info in the download section of the product.

5.4 FAQ

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

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

2. Why does it sometimes take so long to configure new SNMPv3 passwords on the website?

   The authentication methods "SHA-384" and "SHA-512" are calculated purely in software, and can not use the crypto hardware. On the configuration page, e.g. "SHA-512", needs up to 45 seconds to calculate the key.

3. Can you enter multiple e-mail recipients?

   - Yes. In the E-Mail configuration in the Recipient Address field, it is possible to enter multiple e-mail addresses separated by commas. The input limit is 100 characters.

4. Why did the MIB tables change after the firmware update?

   Since the number of possible event types was increased, the previous trap design resulted in an excess of trap definitions: See Change in Trap Design.
Index

- A -
  Antenna terminal 7
  automated Access 41

- B -
  Bootloader Mode 16, 20
  Button Lock 38

- C -
  Certificate-Upload 16, 18
  clear DNS-Cache 18
  Configuration Management 19
  Content of Delivery 6
  creating certificates 47

- D -
  Data Security 68
  Declaration of Conformity 69
  Default Display 38
  Description 6
  device MIB 44

- E -
  E-Mail 37
  Ethernet connector 7

- F -
  Factory Reset 16
  FAQ 69
  Firmware Upload 16
  Firmware-Update 18

- G -
  GBL_Conf.exe 16

- H -
  HTTP 29
  HTTPS 29

- I -
  Installation 7
  IP-ACL 28, 40
  IP-Address 27
  IPv6 40

- L -
  load Configuration 18

- M -
  Maintenance 16
  messages 65
  Modbus TCP 61

- O -
  Ok button 7
  Operating the device directly 14

- P -
  Power Ports 23

- R -
  Radius 41
  Redundant Voltage Supply 9
  Restart 18
  RS232 connector 7

- S -
  Security Advice 6
  Select button 7
  Sensors 10, 35
  signal strength 7
  SIM card slot 7
  SNMP 31, 42
  SSL 47
  Start-up the device 7
  Status LED 7
  Status-LED 14
  syslog 31
Index

- T -
  Technical Specifications     10
  Terminal Assignment     8
  TLS     47

- W -
  Watchdog     24