

Manual



Expert Net Control 2304



© 2023 GUDE Systems GmbH
Manual Ver. 1.2.0
from Firmware Ver. 1.2



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 | 8 |
| 1.4.1 | Connection Example | 9 |
| 1.5 | Technical Specifications | 10 |
| 1.5.1 | Input Behavior | 11 |
| 1.6 | Sensor | 11 |
| 1.6.1 | Calibration | 14 |
| 2. | Operating | 15 |
| 2.1 | Operating the device directly | 16 |
| 2.2 | Control Panel | 16 |
| 2.3 | Maintenance | 18 |
| 2.3.1 | Maintenance Page | 21 |
| 2.3.2 | Configuration Management | 22 |
| 2.3.3 | Bootloader Activation | 23 |
| 3. | Configuration | 26 |
| 3.1 | Output Ports | 27 |
| 3.1.1 | Watchdog | 28 |
| 3.2 | Input Ports | 30 |
| 3.3 | Ethernet | 31 |
| 3.3.1 | IP Address | 31 |
| 3.3.2 | IP ACL | 33 |
| 3.3.3 | HTTP | 34 |
| 3.4 | Protocols | 35 |
| 3.4.1 | Console | 36 |
| 3.4.2 | Syslog | 37 |
| 3.4.3 | SNMP | 37 |
| 3.4.4 | Radius | 38 |
| 3.4.5 | Modbus TCP | 40 |
| 3.4.6 | MQTT | 41 |
| 3.5 | Clock | 42 |
| 3.5.1 | NTP | 42 |
| 3.5.2 | Timer | 43 |
| 3.5.3 | Timer Configuration | 43 |
| 3.6 | Sensors | 50 |
| 3.6.1 | Port Switching | 51 |
| 3.7 | E-Mail | 52 |

Table of contents

| | | |
|--------------|---------------------------------|-----------|
| 3.8 | Front Panel | 54 |
| 4. | Specifications | 55 |
| 4.1 | Automated Access | 56 |
| 4.2 | Console | 56 |
| 4.2.1 | SSH | 61 |
| 4.2.2 | Console Cmd 2304 | 62 |
| 4.3 | HTTP Authentication | 72 |
| 4.4 | IP ACL | 74 |
| 4.5 | IPv6 | 74 |
| 4.6 | Messages | 75 |
| 4.7 | Modbus TCP | 76 |
| 4.7.1 | Sensor Tables | 83 |
| 4.8 | MQTT | 83 |
| 4.8.1 | Example HiveMQ | 85 |
| 4.9 | Radius | 86 |
| 4.10 | SNMP | 87 |
| 4.10.1 | Device MIB 2304 | 90 |
| 4.11 | SSL | 91 |
| 5. | Support | 94 |
| 5.1 | Data Security | 95 |
| 5.2 | HTTP Performance | 95 |
| 5.3 | Contact | 96 |
| 5.4 | Declaration of Conformity | 96 |
| 5.5 | FAQ | 97 |
| Index | | 99 |

Device Description

1 Device Description

1.1 Security Advice

- The device may only be used for its intended purpose.
- The device must be mounted in a housing / control cabinet in the end application and must not be accessible during operation.
- Never work when voltage is applied.
- The device may only be installed and used by qualified personnel. The manufacturer accepts no liability for damage or injury caused by improper use of the device.
- It is not possible for the customer to repair the device. Repairs may only be carried out by the manufacturer.
- The device may only be connected to a 100 - 240 volt AC mains supply (50 - 60 Hz).
- The device may only be operated on the mains supply on a circuit with a fuse protection of max. 16 A.
- The power cables and plugs used must be in perfect condition.
- The device is only intended for use in dry and clean environments.
- The thermal specifications must be observed.
- Please observe the other instructions in the manual for proper handling of the device.
- Please also observe the safety instructions and operating instructions of the other devices that are connected to the device.
- Due to safety and approval issues, it is not allowed to modify the device without our consent.
- The device is not a toy. It must not be stored or operated within the reach of children.
- Do not leave packaging material lying around carelessly. Plastic sheets/bags, Styrofoam parts, etc. could become a dangerous toy for children. Please recycle the packaging material.
- If you are not sure about the correct connection or if any questions arise that are not clarified by the operating instructions, please contact our support.
- Please never leave connected devices that may cause damage unattended.
- Only connect electrical devices that do not have a limited duty cycle. This means that all connected electrical devices must be able to withstand a continuous switch-on without causing damage in the event of a fault.

1.2 Content of Delivery

The package includes:

- **Expert Net Control 2304**
- Quick Start Guide

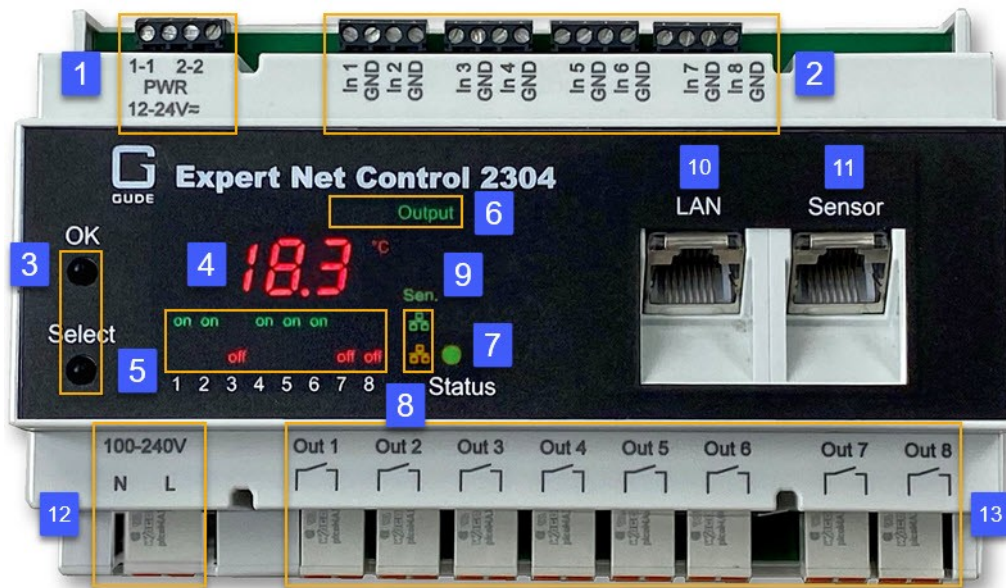
1.3 Description

The **Expert Net Control 2304** can switch 8 different relay outputs and monitor 8 passive signal inputs. The device has the following features:

Device Description

- 8 switchable, potential-free relay outputs, switching voltage 230 V AC 16 A / 24 V DC, 10 A
- Relays dispose of high contact reliability also at very small loads
- 8 passive inputs for monitoring NO and NC devices, e.g. door contacts, smoke detectors etc.
- Operation with 230 V AC or 24 V DC voltage
- Optional sensor for environmental monitoring
- Console commands via SSH and Telnet
- SSH support with public key and passwords
- Individually parameterisable switch-on delay of all outputs
- Programmable timetables and turn-on/turn-off sequences
- Individually adjustable watchdog for each output, which switches depending on accessibility (network ping)
- Dual TCP/IP stack with IPv4 and IPv6 support (IPv6-ready)
- Control and monitoring of the device via Ethernet with an integrated web server with SSL encryption (TLS 1.1, 1.2, 1.3)
- Control and configuration with CGI parameters and JSON messages via HTTP (REST API)
- SNMP (v1, v2c and v3, traps)
- MQTT 3.1.1 Support
- Modbus TCP support
- Radius support
- Generation of messages (e-mail, syslog and SNMP traps) and switching of relays depending on sensor measurement limits
- Firmware update during operation via Ethernet possible
- Encrypted e-mails (SSL, STARTTLS)
- Access protection through IP access control
- Low own consumption
- Developed and produced in Germany

1.4 Installation



1. Low voltage power supply
2. 8x passive inputs (each with GND)
3. Pushbuttons for Select and OK
4. 4x 7-segment display (partly with unit LEDs e.g. "°C")
5. 8x plain text displays (on/off) for the status of inputs and outputs
6. Indicators ("Input" or "Output") for the 8 plain text displays (on/off)
7. Status LED
8. Ethernet port status and activity (green and orange)
9. External sensor ("Sen.") plugged in indicator
10. Network connection (RJ45)
11. Sensor connection (RJ45)
12. AC mains power supply
13. 8x relay switching contacts (NO)

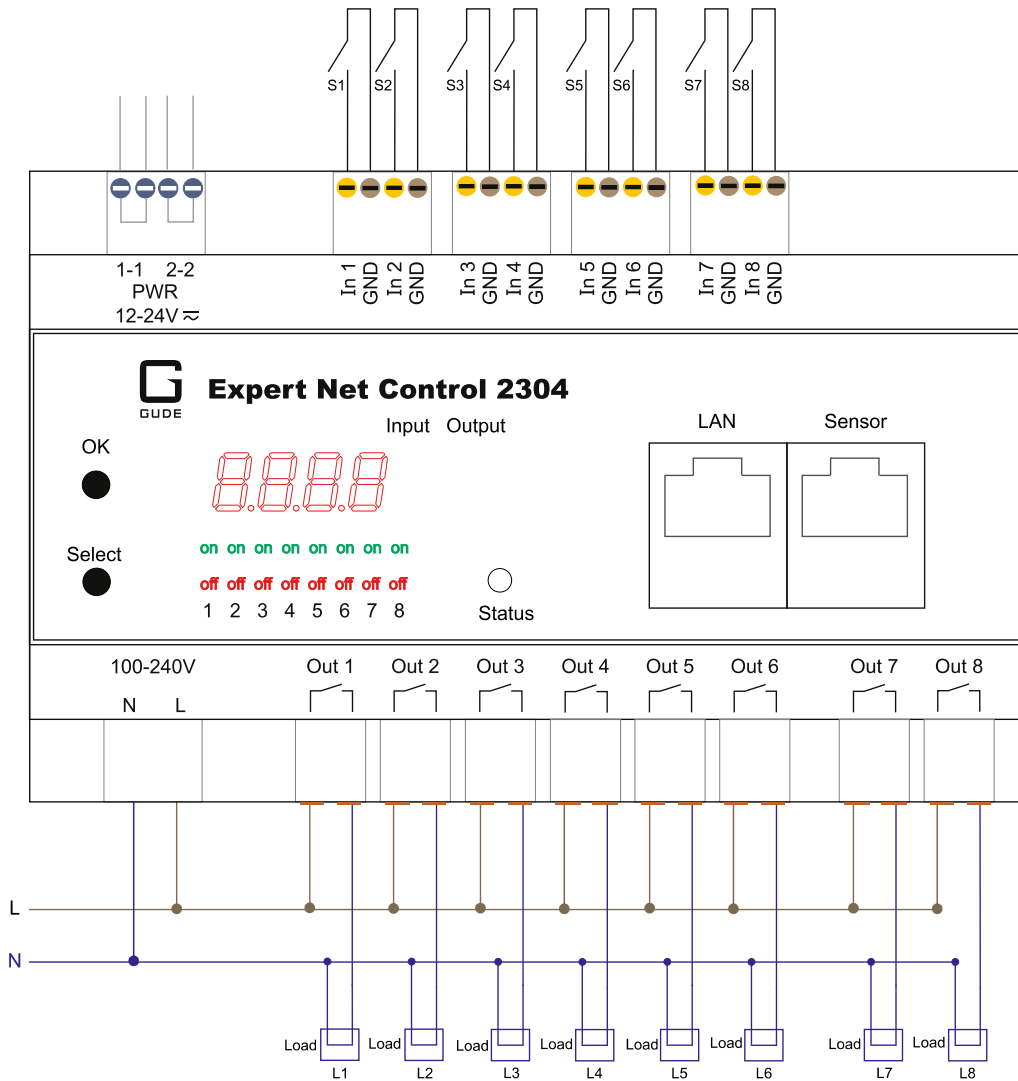
Commissioning

- Connect the device to the mains supply or to a suitable low voltage source (see technical data).
- Plug the network cable into the Ethernet socket (RJ45).
- Connect the relays to the loads that are to be operated.
- Establish contact between the lines to be monitored and the digital inputs.
- Connect a sensor (if available).

Device Description

1.4.1 Connection Example

Here is an example with block diagram in which the device is supplied with 230V AC and in which eight AC loads (L1 - L8) are connected. In addition, the inputs are assigned eight switches (S1 - S8).



⚠ As an alternative to connecting "In 1-8" and "GND", voltages can also be fed in between "In 1-8" and GND. The maximum input voltage is 24V, voltages below 3V are detected as LOW state, and voltages above 8V are detected as HI.

1.5 Technical Specifications

| | |
|---|---|
| Connections | 1 x Ethernet connection RJ45 1 x RJ45 for external sensor 1 x AC mains connection, picoMAX 7.5 1 x low voltage, AK1350 8 x inputs In1 ... In8, AK1350 8 x relay switching contacts NO, picoMAX 5.0 |
| Network connection | 10baseT / 100baseTX Ethernet |
| Relay outputs Out1 ... Out8 | max. 240V AC 16A, 50/60Hz 24V DC 10A |
| Inputs In1 ... In8 | screw terminal, AK1350/..DS-3.5-GREY digital input, internal pull-up active: max. 24V, < 3V LOW, > 8V HI passive: switching contact |
| Power supply | internal power supply: 100V to 240V AC -15% ... +10%, 50/60 Hz, max 0.3A |
| | Low voltage: 12V to 24V AC -10% ... +10%, 50/60Hz, max 0.8A 12V to 24V DC -5% ... +25%, max 0.8A internal fuse protection: 1.75A Typical I^2t (A ² s) = 1.5 |
| Protection class | Class II |
| Environment • Ambient temperature • Storage temperature • Humidity | 0°C to 50°C -20°C - 70°C 0% - 95% (non-condensing) |
| Housing | White plastic |
| Dimensions | 143mm x 65mm x 90mm (L x H x D) |
| Weight | approx. 400g |


| AK1350 /DS-3.5-GREY | |
|---|--|
| Connection technology | Screw terminal |
| Solid conductor | 0.08 ... 1.5 mm ² solid conductor |
| Fine-stranded conductor (flexible) | 0.08 ... 1.5 mm ² fine-stranded conductor |
| Fine stranded conductor; wire end ferrule | 0.14 ... 0.5 mm ² fine-stranded conductor |
| Stripping length | 5.0 mm |
| Torque | 0.25 Nm |
| Screw Size | M2 |

| picoMAX® eCOM 5.0 and 7.5 | |
|---|---|
| Connection technology | Push-in CAGE CLAMP® |
| Actuation type | Push-button |
| Solid conductor | 0.2 ... 2.5 mm ² / 24 ... 12 AWG |
| Fine-stranded conductor | 0.2 ... 2.5 mm ² / 24 ... 12 AWG |
| Fine stranded conductor; with insulated ferrule | 0.25 ... 1.5 mm ² |
| Stripping length | 9.0 ... 10.0 mm |

Device Description

1.5.1 Input Behavior

| Input | Logic | Logic inverted (Fabdefault) |
|--------------------------------------|---|---|
| open closed | High / on / closed Low / off / open | low / off / open High / on / closed |
| Voltage < 3V > 8V otherwise | Low / off / open High / on / closed undefined | High / on / closed Low / off / open undefined |

 Event messages are generated when the logic changes. In the sensor configuration the logic can be inverted. So that "High" appears when the input is closed, the logic is configured as inverted as fabdefault. In protocols with numeric values (e.g. SNMP or ModbusTCP) a "1" is considered as High, and a "0" as Low.

1.6 Sensor

One external sensor can be connected to the **Expert Net Control 2304**. The following sensors are currently available



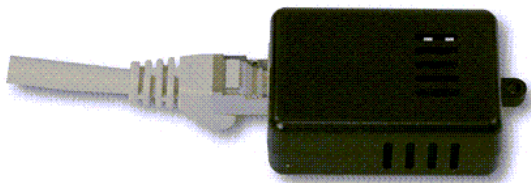
7101



7104 - 7106

Device Description

| Product Name | 7101 (End-of-Life) | 7104-1 | 7105-1 | 7106-1 |
|-------------------------------------|---|---|---|---|
| Calibrated Sensor | - | 7104-2 | 7105-2 | 7106-2 |
| Cable Length | ≈ 2m | ≈ 2m | ≈ 2m | ≈ 2m |
| Connector | RJ45 | RJ45 | RJ45 | RJ45 |
| temperature range | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) |
| air humidity range (non-condensing) | - | - | 0-100%, ±3% (typical), 10-80% ±2% (typical) | 0-100%, ±3% (typical), 10-80% ±2% (typical) |
| air pressure range (full) | - | - | - | ± 1 hPa (typical) at 300 ... 1100 hPa, 0 ... +40 °C |
| air pressure range (ext) | - | - | - | ± 1.7 hPa (typical) at 300 ... 1100 hPa, -20 ... 0 °C |
| Protection | IP68 | - | - | - |



7201, 7202



7205, 7206

| Product Name | 7201 (End-of-Life) | 7202 (End-of-Life) | 7205 | 7206 |
|-------------------------------------|---|---|---|---|
| Connector | RJ45 | RJ45 | RJ45 | RJ45 |
| temperature range | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) |
| air humidity range (non-condensing) | - | 0-100%, ±3% (typical) | 0-100%, ±3% (typical), 10-80% ±2% (typical) | 0-100%, ±3% (typical), 10-80% ±2% (typical) |
| air pressure range (full) | - | - | - | ± 1 hPa (typical) at 300 ... 1100 hPa, 0 ... +40 °C |
| air pressure range (ext) | - | - | - | ± 1.7 hPa (typical) at 300 ... 1100 hPa, -20 ... 0 °C |

Device Description



7207, 7209, 7210


| Product Name | 7207 | 7209 | 7210 |
|-------------------------------------|---|---|---|
| Connector | RJ45 | RJ45 | RJ45 |
| temperature range | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) | -20°C to +80°C at ±2°C (maximum) and ±1°C (typical) |
| air humidity range (non-condensing) | - | 0-100%, ±3% (typical), 10-80% ±2% (typical) | 0-100%, ±3% (typical), 10-80% ±2% (typical) |
| air pressure range (full) | - | - | ± 1 hPa (typical) at 300 ... 1100 hPa, 0 ... +40 °C |
| air pressure range (ext) | - | - | ± 1.7 hPa (typical) at 300 ... 1100 hPa, -20 ... 0 °C |
| Inputs | 2x | 2x | 2x |

Technical data inputs

| | |
|----------|--|
| Inputs | digital input, internal pull-up active: max. 24V, < 3V Low, > 8V High passive: switching contact |
| Terminal | 3-pole - AK1550/3-3.5-GREEN |

Behavior inputs

| Input | Logic | Logic inverted (Fabdefault) |
|--------------------------------------|---|---|
| open closed | High / on / closed Low / off / open | low / off / open High / on / closed |
| Voltage < 3V > 8V otherwise | Low / off / open High / on / closed undefined | High / on / closed Low / off / open undefined |

 Event messages are generated when the logic changes. In the sensor configuration the logic can be inverted. So that "High" appears when the input is closed, the logic is configured as inverted as fabdefault. In protocols with numeric values (e.g. SNMP or

Device Description

ModbusTCP) a "1" is considered as High, and a "0" as Low.

Sensor in web interface

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

| Id | Name | Temperature °C | Humidity % | Dew Point °C | Dew Diff °C | Pressure hPa |
|---------|----------------------|-------------------|---------------|-----------------|----------------|-----------------|
| 1: 7106 | 7106 | 22.5 | 34.2 | 5.9 | 16.6 | 1013.8 |

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

| Id | Name | Temperature °C | Humidity % | Dew Point °C | Dew Diff °C | Pressure hPa |
|---------|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|
| 1: 7106 | 7106 | 22.5 | 34.4 | 6.1 | 16.5 | 1013.8 |
| | 30m min | 0.0 | 34.1 | 5.9 | 16.4 | 125.0 |
| | 30m max | 22.6 | 34.7 | 6.2 | 300.0 | 1013.8 |
| | <input type="button" value="Reset"/> | <input type="button" value="Reset"/> | <input type="button" value="Reset"/> | <input type="button" value="Reset"/> | <input type="button" value="Reset"/> | <input type="button" value="Reset"/> |

If external sensors with inputs are connected, these are also added on the "Control Panel" web page:

| Port | Name | logical state | time since transition | toggle count |
|--------------|--------------|-----------------|-----------------------|--------------|
| 2: 7207 - I1 | Extern Input | ● 0: off / open | 1d 03:48:48 | 0 |
| 2: 7207 - I2 | Extern Input | ● 0: off / open | 1d 03:48:48 | 0 |

1.6.1 Calibration

From this firmware version it is possible to store a value offset in the sensor for internal sensors (Expert Sensor Box) or external sensors. This offset is zero ex works, because the sensors are normally not calibrated. The offset can be specified by the following commands via Telnet / SSH:

```
extsensor {port_num} {sen_field} calib set {float}  
extsensor {port_num} {sen_field} calib show
```



For internal sensors (such as the Expert Sensor Box), the internal sensor port is 1.

External Sensor Field Table "{sen_field}".


| Index | Description | Unit |
|-------|--------------|------|
| 0 | Temperature | °C |
| 1 | Humidity | % |
| 3 | Air pressure | hPa |

Operating

2 Operating

2.1 Operating the device directly

Port Switching

The current switching state of the output is indicated by the corresponding plain text displays (port LEDs). If the green "on" LED is lit, the port is switched on, if the red "off" LED is lit, the output port is switched off. The buttons "Select" and "Ok" are located on the device. If you press "select", you can select the following modes one after the other (in the front panel  configuration you can deactivate the modes "All on" or "All off").

1. All on (PALL in the display): All LEDs flash green. If you press the "Ok" button for 2.5 seconds, all ports are switched on.
2. All off (PALL in the display): All LEDs flash red. If you hold the "Ok" button for 2.5 seconds, all ports are switched off.
3. If you press "Select" again, the LED for the first output starts flashing, i.e. the output is selected. Press "Select" again to select the next output. Pressing and holding the "Ok" button for one second will toggle the state of the selected output.



If the ports are already "All on" or "All off", the corresponding mode is skipped.

Status-LED

The Status LED shows the different states of the device:

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

2.2 Control Panel

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

on 1:Output Port

on 2:Output Port

off 3:Output Port

off 4:Output Port

off 5:Output Port

off 6:Output Port

off 7:Output Port

off 8:Output Port

All On All Off

| Port | Name | logical state | time since transition | toggle count |
|---------|-------|-----------------|-----------------------|--------------|
| Input 1 | Input | ● 0: off / open | 00:03:07 | 0 |
| Input 2 | Input | ● 0: off / open | 00:03:07 | 0 |
| Input 3 | Input | ● 0: off / open | 00:03:07 | 0 |
| Input 4 | Input | ● 0: off / open | 00:03:07 | 0 |
| Input 5 | Input | ● 0: off / open | 00:03:07 | 0 |
| Input 6 | Input | ● 0: off / open | 00:03:07 | 0 |
| Input 7 | Input | ● 0: off / open | 00:03:07 | 0 |
| Input 8 | Input | ● 0: off / open | 00:03:07 | 0 |

The web page provides an overview of the switching state, as well as the external sensor, provided that it is connected. When a single port is clicked at the **Expert Net Control 2304**, a panel with buttons to control a single port appear:

off 1: Output Port

On Off Reset Batch Close

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



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



The ports can be switched manually with the "On" and "Off" buttons. If the port is turned on, it can be turned off by pressing the "Reset" button, until after a delay it turns itself on again. The delay time is determined by the parameter Reset Duration, which is described in the chapter "Configuration - Output Ports^[27]". The "Close" button dissolves the panel again.

Batchmode

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

off 1: Output Port On Off Reset Batch Close
switch on , wait 5 sec(s) , switch off Ok

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.

| Port | Name | null | time since transition | toggle count |
|---------|-------|-----------------|-----------------------|--------------|
| Input 1 | Input | ● 0: off / open | 00:30:54 | 0 |
| Input 2 | Input | ● 0: off / open | 00:30:54 | 0 |
| Input 3 | Input | ● 0: off / open | 00:30:54 | 0 |
| Input 4 | Input | ● 0: off / open | 00:30:54 | 0 |
| Input 5 | Input | ● 0: off / open | 00:30:54 | 0 |
| Input 6 | Input | ● 0: off / open | 00:30:54 | 0 |
| Input 7 | Input | ● 0: off / open | 00:30:54 | 0 |
| Input 8 | Input | ● 0: off / open | 00:30:54 | 0 |

The website contains a status overview of all passive signal inputs, the time since the last change, and a counter of switching changes. The name and text for a logical state of each input can be configured in the chapter Configuration-Input Ports^[30].

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^[21].


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^[21], 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".

 During a firmware update, old data formats are sometimes converted to new structures. If an older firmware is newly installed, the configuration data and the energy meters may be lost! If the device then does not run correctly, please restore the factory settings (e.g. from the Maintenance Page^[21]).

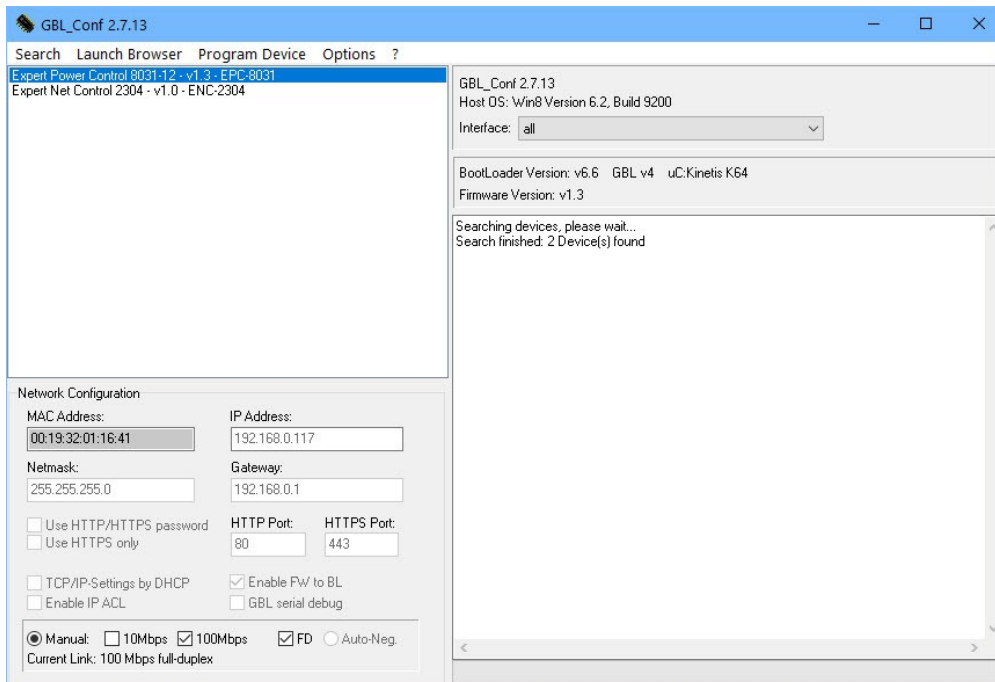
Actions in Bootloader mode

If the web interface of the device is no longer accessible, the device can be put into Bootloader mode (see chapter Bootloader activation^[23]). 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
- Allow jump from firmware to bootloader
- 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-systems.com.




Interface GBL_Conf

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

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

The new network configuration is now displayed.

 Changing the configuration with gbl_conf.exe is explicitly only allowed in bootloader mode!

Factory Reset

The device can be reset to the factory default via the web interface from the Maintenance Page^[21] or from the Bootloader mode (see chapter Bootloader activation^[23]). 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

Choose File Upload

SSL Certificate Upload

Choose File Upload

Config Import File Upload

Choose File Upload

[Config File Export](#)

Restart / Fab-Settings

Restart Device Restore Fab Settings and Restart Device

Enter Bootloader Mode Flush DNS Cache

Service Data


- Config/Status View: [status.html](#)
- Config/Status Download: [export.json](#)

Firmware Update: Start a firmware update.


SSL Certificate Upload: Saves your own SSL certificate. See chapter "SSL⁹¹" for the generation of a certificate in the right format.

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

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

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

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

 Some functions such as a firmware update or changing of the IP-address and HTTP settings require a restart of the device. A jump to the boot loader or a restart of the device lead by no means to a change of the relay states.

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

factory default^[24].

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

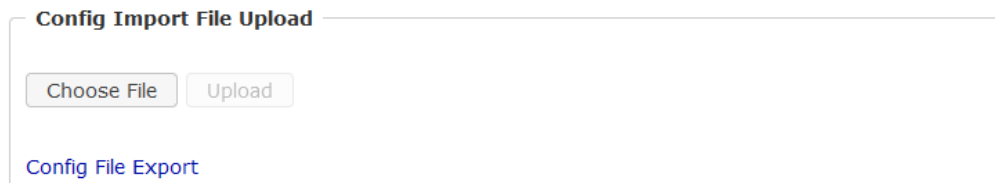
Flush DNS Cache: All entries in the DNS cache are discarded and address resolutions are requested again.

Config/Status View: [status.html](#): Displays the status.html page with the JSON data.

Config/Status Download: [export.json](#): Direct file download of JSON data from status.html.


2.3.2 Configuration Management

The device configuration can be saved and restored in the maintenance area^[21].



The screenshot shows a web interface for configuration management. At the top, there is a header 'Config Import File Upload'. Below this header, there are two buttons: 'Choose File' and 'Upload'. At the bottom of the interface, there is a link labeled 'Config File Export'.

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

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

Editing the configuration file

It is possible to customize a saved configuration file with a text editor for your own needs. For example, one scenario would be to use a script language to automate the creation of many customized versions of a configuration, then equip a large number of devices with an individualized configuration. Also Upload and restart with CGI commands can be done in scripting languages. With use of the comment sign "#" you can quickly hide single commands or add personal notes.

If you modify a configuration file manually, it is not always clear which limits are allowed for parameters. After uploading and restarting, commands with invalid parameters are ignored. Therefore, the generated configuration includes comments describing the boundaries of the parameters. Where "range:" refers to a numeric value, and "len:" to a text parameter. E.g:

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

The command "system fabsettings" from the beginning of a generated configuration file

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

No output of default values

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

Configuration via Telnet

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

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

An example:

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

2.3.3 Bootloader Activation

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

Activation of the Bootloader Mode

1) via push button:


- Hold both buttons for 3 seconds

2) or


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

3) by Software:


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

 This function is only possible if "Enable FW to BL" was activated in the application "GBL_Conf.exe" before, while the device was already in the bootloader.

4) via web interface:

Press "Enter Bootloader Mode" on the maintenance  web page.

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

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

Abandonment of the Bootloader Mode

1) via push button:


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

2) or

- Remove and connect the power supply without operating a button

3) by Software:

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

 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.

Factory Reset

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

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

1) via push button:

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

2) by Software:

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

Configuration

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

The screenshot shows a configuration window titled "Output Ports". It contains the following fields and options:

- Choose Output Port to configure:** A dropdown menu with "1: Output Port" selected.
- Label:** A text input field containing "Output Port".
- Coldstart status:** Radio buttons for "on", "off", and "remember last state" (which is selected).
- Coldstart delay:** A text input field containing "0" followed by "s".
- Repower delay:** A text input field containing "0" followed by "s".
- Reset action duration:** A text input field containing "10" followed by "s".
- Enable watchdog:** Radio buttons for "yes" and "no" (which is selected).

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.

Coldstart status: 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.

Coldstart 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 action 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.

Enable watchdog: Activates the watchdog function for this output port.

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 power port reset, the display will remain orange until the device is rebooted and responds again to ping requests. This will prevent a premature watchdog reset of the port, e.g. when a server needs a long time for a file check.

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

Enable watchdog: Enables the watchdog function for this Power 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 Power Port is turned off and switched back on after the time set in Reset Duration. In mode Switch off once when host down the Power 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 Power 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.

count PING requests as unreplied when ethernet link down: If the Ethernet link of the device is not active, watchdog monitoring is not possible and the watchdog function is not activated. If this option is activated, a watchdog is also triggered if the Ethernet link is down.

3.2 Input Ports

Output Ports · [Input Ports](#)

Configuration - Input Ports

Input:

Input Name:

Inverted input: yes no

Input HI text message:

Input LOW text message:

Enable value-threshold message trigger: yes no

On input is HI: Switch port to

On input is LOW: Switch port to

Enable time-interval message trigger: yes no

every second(s)

for Console- and MQTT channels

Enable value-delta message trigger: yes no

every input state change

for Console- and MQTT channels

Message channels: Syslog SNMP Email Console

MQTT:

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

Input Name: A name with a maximum of 15 characters can be assigned here for each of the input ports. The name can be used to facilitate identification of the device connected to the port.

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

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

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

Enable value-threshold message trigger: Generates messages when the inputs change.

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.

Enable time interval message trigger: Generates console (Telnet/SSH) and MQTT messages within time intervals.

Enable value-delta message trigger: Generates console (Telnet/SSH) and MQTT messages when an input changes.

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

3.3 Ethernet

3.3.1 IP Address

[IP Address](#) · [IP ACL](#) · [HTTP Server](#)

Hostname

Hostname:

IPv4

Use IPv4 DHCP: yes no

IPv4 Address:

IPv4 Netmask:

IPv4 Gateway address:

IPv4 DNS address:

MAC address: 00:19:32:01:1e:52

IPv6


Use IPv6 Protocol: yes no

Use IPv6 Router Advertisement: yes no

Use DHCP v6: yes no

Use manual IPv6 address settings: yes no

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: With "yes" the TCP/IP settings are 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 no DHCP server is available, the last IP address is used. However, the DHCP client tries to reach a DHCP server again every 5 minutes. The DHCP request lasts one minute until it is aborted. During this time the IP-address is not accessible! It is therefore essential to deactivate DHCP for static IP addresses!

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.

IPv6 status

Current IPv6 status:

| | |
|------------------|---|
| IPv6 Addr: | fe80::219:32ff:fe00:996d 2007:7dd0:ffcl:l:219:32ff:fe00:996d |
| IPv6 DNS Server: | 2007:7dd0:ffcl:1:20c:29ff:feaf:93c |
| IPv6 Router: | fe80::20c:29ff:feaf:93c |

 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

IPv6 (manual)

| | | |
|-----------------------|--|------|
| IPv6 Addresses: | <input type="text" value="2007:7dd0:ffc1:0:219:32ff:fe00:996d"/> | / 64 |
| | <input type="text"/> | / 64 |
| | <input type="text"/> | / 64 |
| | <input type="text"/> | / 64 |
| IPv6 DNS addresses: | <input type="text" value="2007:7dd0:ffc1:0:20c:29fffeaf:93c"/> | |
| | <input type="text"/> | |
| IPv6 Gateway address: | <input type="text" value="fe80::20c:29ff:feaf:93c"/> | |

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.

PHY Setting

PHY preferences can be set for 10 Mbps or 100 Mbps, half-duplex or full-duplex. Advertising means that a proposal for the connection is made, which can be rejected by the remote terminal (e.g. the switch).

PHY Settings

Actual Speed: 100 Mbps
Actual Duplex Mode: Full Duplex

Change Settings (Advertising):

3.3.2 IP ACL

[IP Address](#) · [IP ACL](#) · [HTTP Server](#)

ICMP Ping

Reply ICMP ping requests: yes no


IP Access Control List


Enable IP filter: yes no

| | | | |
|---------------------------------|---|---|---|
| 1. Grant IP access to host/net: | <input type="text" value="1234::4ef0:eec1:0:219:32ff:fe00:f124"/> | - | + |
| 2. Grant IP access to host/net: | <input type="text" value="192.168.1.84"/> | - | + |
| 3. Grant IP access to host/net: | <input type="text" value="mypc.locdom"/> | - | + |
| 4. Grant IP access to host/net: | <input type="text" value="192.168.1.0/24"/> | - | + |
| 5. Grant IP access to host/net: | <input type="text" value="1234:4ef0:eecl:0::/64"/> | - | + |

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

HTTP Server option: HTTP + HTTPS
 HTTP redirects to HTTPS
 HTTPS only HTTP only

Server port HTTP:
Server port HTTPS:
Supported TLS versions:

HTTP Password

Enable password protection: yes no
Use radius server passwords: yes no
Use locally stored passwords: yes no

Set new **admin** password: (32 characters max)
Repeat **admin** password:

Set new **user** password: (32 characters max)
Repeat **user** password:

Session Timeout (admin): (seconds)
Session Timeout (user): (seconds)
Select Authentication Mode:


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.

Supported TLS versions: Limits the supported TLS versions.


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.

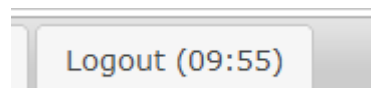
Enable password protection: Password access protection can be activated. If the admin password is assigned, you can only log in by entering this password to change settings. Users can log in by entering the user password in order to query the status information and initiate switching operations.

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.



If a password is activated, the web session is automatically terminated after a timeout and you are redirected to the login page. A timeout of "0" disables the automatic logout.

Session Timeout (admin): Logout time for the admin.

Session Timeout (user): Logout time for the user.

Select Authentication Mode: Sets the session authentication mode. For details see HTTP Authentication.

3.4 Protocols

3.4.1 Console

[Console](#) · [Syslog](#) · [SNMP](#) · [Radius](#) · [Modbus](#) · [MQTT](#)

TCP/IP Console

Enable Telnet: yes no
Telnet TCP port:
Raw mode: yes no
Active negotiation: yes no
Activate echo: yes no
Push messages: yes no
Delay after 3 failed logins: yes no

Enable SSH: yes no
SSH TCP port:
Activate echo: yes no
Push messages: yes no

Require user login (Telnet/SSH): yes no
Use radius server passwords: yes no
Use locally stored passwords: yes no
Username:
Set new password: (32 characters max)
Repeat password:
Upload new SSH public key:

Enable Telnet: Enables Telnet console .

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

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

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

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

Require user login: Username and password are required.

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

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

Use locally stored passwords: Username and password are stored locally

3.4.2 Syslog

[Console](#) · [Syslog](#) · [SNMP](#) · [Radius](#) · [Modbus](#) · [MQTT](#)

Syslog

Enable Syslog: yes no

Syslog server:

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

[Console](#) · [Syslog](#) · [SNMP](#) · [Radius](#) · [Modbus](#) · [MQTT](#)

SNMP

Enable SNMP options: SNMP get SNMP set

SNMP UDP port:

sysContact:

sysName:

sysLocation:

SNMP v2

Enable SNMP v2: yes no

SNMP v2 public Community: (16 char. max)

SNMP v2 private Community: (16 char. max)

SNMP v3

Enable SNMP v3: yes no

SNMP v3 Username: (32 char. max)

SNMP v3 Authorization Algorithm:

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

Repeat **Authorization** password:

SNMP v3 Privacy Algorithm:

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

Repeat **Privacy** password:

SNMP Traps

Send SNMP Traps:

SNMP trap receiver 1 :

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

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

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

sysContact: Value of RFC 1213 sysContact.

sysName: Value of RFC 1213 sysName.

sysLocation: Value of RFC 1213 sysLocation.

Enable SNMP v2: Activates SNMP v2.



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

Community public: The community password for SNMP GET requests.

Community private: The community password for SNMP SET requests.

Enable SNMP v3: Activates SNMP v3.

SNMP v3 Username: The SNMP v3 User Name.

SNMP v3 Authorization Algorithm: The selected Authentication Algorithm.

SNMP v3 Privacy Algorithm: SNMP v3 Encryption Algorithm..



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



The calculation of the password hashes varies with the selected algorithms. If the Authentication or Privacy algorithms are changed, the passwords must be re-entered in the configuration dialog. "SHA-384" and "SHA512" are calculated purely in software. If "SHA-512" is set on the configuration page, the time for the key generation may take once up to approx. 45 seconds.

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

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

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

More information about SNMP settings are available from our support or can be found on the Internet at www.gude.info/wiki.

3.4.4 Radius

Radius

Enable Radius Client: yes no

Authentication Protocol: PAP CHAP

Use Message Authentication: yes no

Default Session Timeout:

Primary Server:

Set new shared secret:

Repeat new shared secret:

Timeout:

Retries:

Use backup server: yes no

Backup Server:

Set new shared secret:

Repeat new shared secret:

Timeout:

Retries:

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. For compatibility reasons, only use ASCII characters.

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. For compatibility reasons, only use ASCII characters.

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

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

Test Radius Server

Test Username:

Test Password:

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

[Console](#) · [Syslog](#) · [SNMP](#) · [Radius](#) · [Modbus](#) · [MQTT](#)

Modbus TCP

Enable Modbus TCP: yes no

Modbus TCP port:

Enable Modbus TCP: Enables Modbus TCP support.

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

3.4.6 MQTT

MQTT

Enable MQTT: yes no

Broker:

TLS: yes no

TCP Port: (Default: 8883)

Username:

Set new password:

Repeat password:

Client ID:

Quality of Service (QoS): ▾

Keep-alive ping interval: s (minimum 10s)

Topic Prefix:
de/gudesystems/epc/00:19:32:01:16:41

Permit CLI commands: yes no

Publish device data summary interval: s (0=disabled)

Enable MQTT: Enables MQTT support.

Broker: DNS or IP address of the MQTT broker.


TLS: Turns on TLS encryption.

Mode TCP port: The TCP/IP port number of the broker.

Username: The MQTT username.

password: The password for the username.

Client ID: The MQTT client ID.

 The client IDs of a user must be different! If two clients of a user have the same name, the connection of one client is normally terminated.

Quality of Service (QoS): Sets the QoS value (0 or 1) of the MQTT publishes.

Keep-alive ping interval: This defines the time interval in which the client sends an MQTT ping.

Topic prefix: Defines the beginning of the topic with which all messages are sent. The strings **[mac]** and **[host]** symbolize the MAC address or the hostname of the device.

Permit CLI commands: Enables the execution of console commands.

Publish device data summary interval: Time interval in which messages with the global status of the device are sent.

MQTT Logs

- MQTT client connected
- MQTT sending client id:'client_1641' username:'epc-user'
- MQTT broker connected
- MQTT broker DNS resolved
- MQTT broker DNS not yet resolved
- MQTT resolving host 'f3c06b76137c48439e81c18b11bd06ab.s1.eu.hivemq.cloud' TCP port 8883

MQTT Broker Status

- Broker DNS ready, connected since 71 seconds
- Last publish 11 seconds ago

MQTT Logs: Outputs individual log messages about the connection setup.

MQTT Broker Status: Time information about connection duration, the last publish and the last keep-alive.

3.5 Clock

3.5.1 NTP

[NTP](#) · [Timer](#)

NTP

Enable Time Synchronization: yes no

Primary NTP server:

· reply 12s ago, 59ms signal delay
· Mon Oct 11 2021 13:49:46 GMT+0200 (Central European Summer Time)

Backup NTP server:

Timezone:

Timezone:

Daylight Saving Time (DST): yes no

Clock

Current Systemtime (UTC): 11:49:59 11.10.2021 (1633952999)

Current Localtime: 13:49:59 11.10.2021

Browstime: 13:49:58 11.10.2021

Set clock:

Enable Time Synchronization: Enables the NTP protocol.

Primary NTP server: IP address of the first NTP server.

Backup NTP server: IP address of the second NTP server. Used when the first NTP server does not respond.

Timezone: The set time zone for the local time.

Daylight Saving Time: If enabled, the local time is converted to Central European Summer Time.

set manually: The user can set a time manually.

set to Browsetime: Sets the time corresponding to web browser.



If Time synchronization is enabled, a manual time will be overwritten at the next NTP synchronization.

3.5.2 Timer

Timer - Basic Settings

Enable Timer: yes no

Syslog verbosity level:

Timer - Rules

Enable Timer: enables or disables all timers globally.

Syslog verbosity level: Sets the verbosity level for timer syslog output.

New Rule simple Timer: Shows a dialog for a simple timer rule.

New Rule advanced Timer: Brings up the dialog for advanced timer settings.

3.5.3 Timer Configuration

In the timer configuration you have three options: Create a simple timer, add a complex timer, or change an existing configuration.



Timer rules are only executed if the device has a valid time. See configuration NTP [42](#).



The number of timers is limited to 32.



This instruction chapter applies to all Gude devices. For devices without switchable ports you can only create a complex timer. For an action there is only the register "Action CLI" available, and not the register "Action PortSwitch".

Timer - Basic Settings

Enable Timer: yes no

Syslog verbosity level:

Timer - Rules

New Rule: simple Timer

New Rule: advanced Timer

Creating a simple timer

If you activate "New Rule: simple Timer" the following dialog is displayed:

Timer Rule

Switch

From : To :

On weekdays: Mon Tue Wed Thu Fri Sat Sun

You set here which port should be switched for which time period, and on which days of the week the rule is active. In this example the period 9:00 to 17:00 is changed to 9:30 to 11:00 compared to the default input mask. Also, this rule should not be applied on Saturday and Sunday. The rule we have now says that every day, except Saturday and Sunday, port 1 will be switched on at 9:30 and switched off after 1.5 hours. Clicking on "Save" saves this rule.

Timer - Rules

🕒 Rule 1: Port On

🕒 Rule 2: Port Off

New Rule: simple Timer

New Rule: advanced Timer

We have now created 2 rules, one for when the port is turned on and the second for when it is turned off.

Creating a complex timer

If you create a complex timer or change an existing timer, you will always see an extended dialog. Here, ports can be switched as well as other actions can be executed via

CLI commands. The setting of the switching times is more granular.

Timer - Rule 1: Port On

Trigger: Date/Time Pattern Options Action PortSwitch Action Cli

Hours:
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23

Minutes:
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29
30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59


Days:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Month
01 02 03 04 05 06 07 08 09 10 11 12

Days of week:
Mon Tue Wed Thu Fri Sat Sun

Delete Save Cancel

You can see here the extended representation of the first rule of the simple timer from the previous example. The action is started every day of every month at 9:30. The weekdays Saturday and Sunday are excluded. An existing rule can be removed with the "Delete" button.

 If a rule is deleted, the following rules move up. The numbering of the following rules also changes by one. This also applies to the index in the console commands.

Timer - Rule 1: Port On

Trigger: Date/Time Pattern Options Action PortSwitch Action Cli

Rule Name: Port On

Rule Valid from: [] to [] dd.mm.yyyy

Random Trigger Probability: 100


Random Trigger Jitter: 0 secs

enable trigger: yes no

Action mode: Switch Power Ports Perform CLI Cmd

Delete Save Cancel

The button enable trigger allows to switch a timer on and off without the need to completely delete or recreate the rule. A simple timer is directly "enabled", for a newly created complex timer "enable trigger" must be switched on manually. You can set a probability and a jitter for the timer rules. This makes random events possible. In this example the rule is executed with 100% probability. A jitter of 0 means that the action takes place exactly at the programmed time. Ports are switched as action mode, alternatively a console command (CLI Cmd) can be executed.

 After changes to existing timers, the "Rule Name" may no longer be meaningful. To keep the overview, it may be useful to adjust the name.

Timer - Rule 1: Port On

Trigger: Date/Time Pattern Options **Action PortSwitch** Action Cli

Switch Power Ports Action1:


| | | | | | | | | | | | |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| On | On | On | On | On | On | On | On | On | On | On | On |
| Off | Off | Off | Off | Off | Off | Off | Off | Off | Off | Off | Off |

Switch Power Ports Action2:

| | | | | | | | | | | | |
|-----|---|---|---|---|---|---|---|---|---|---|---|
| On | - | - | - | - | - | - | - | - | - | - | - |
| Off | - | - | - | - | - | - | - | - | - | - | - |

Between Action1 and Action 2 : wait hour(s) ▾

The switching function can be set in more detail on the "Action PortSwitch" register. Port 1 is switched on. You could extend the rule and switch more ports on or off. Additionally you can set a time for a batchmode in the field after "Between Action1 and Action 2 : wait", which starts "Action 2" after expired time. However, the batch mode has the disadvantage that it is not automatically restarted when the device is rebooted. Also, the port is locked against manual operation on the web page as long as the batch mode is running.

 The "Action PortSwitch" function is only available for devices with switchable ports.

Extending a rule

For demonstration purposes, here is an extension to the simple timer from the previous example:

Timer - Rule 1: Port On

Trigger: **Date/Time Pattern** Options Action PortSwitch Action Cli

Hours:
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23


Minutes:
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29
30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59


Days:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

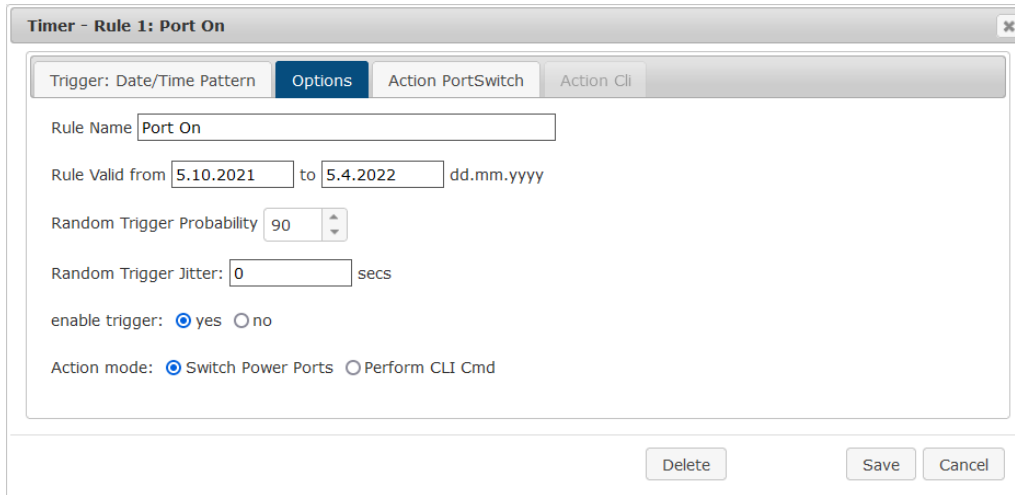
Month
01 02 03 04 05 06 07 08 09 10 11 12

Days of week:
Mon Tue Wed Thu Fri Sat Sun

The action is now started not only at 9:30, but also at 17:30 There are other changes: The timer is only active between October and December, also the action does not take place on the first day of a month.

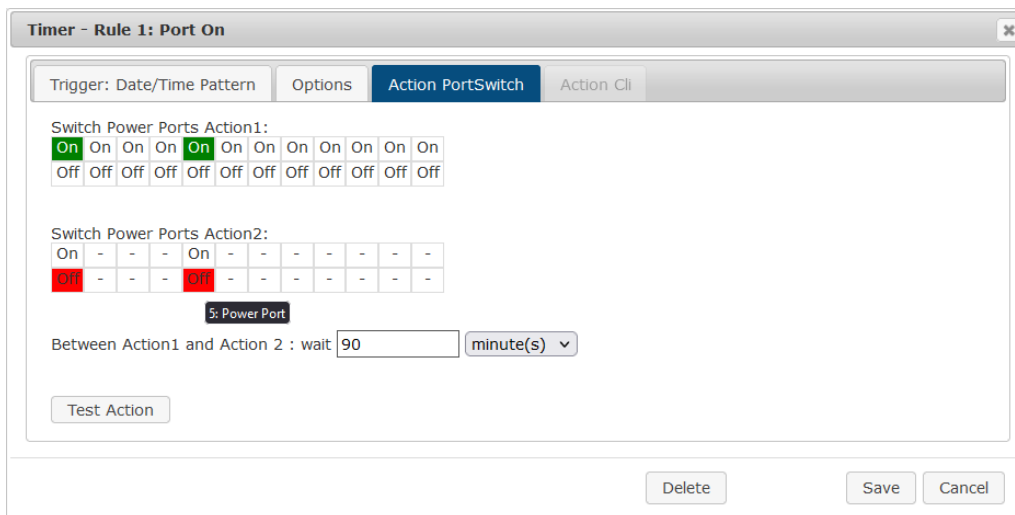
 Since all fields in the mask are always considered, it is not possible to define the times 9:30 and 17:10 in a single timer rule. You need a second rule for this. If you set the hours 9 and 17, as well as the minutes 10 and 30, then the four times 9:10, 9:30, 17:10 and 17:30 would be programmed.

 To change a field in this input mask without changing the state of the other fields, the Ctrl key must be pressed during the mouse click.




The screenshot shows the 'Timer - Rule 1: Port On' configuration window with the 'Options' tab selected. The 'Rule Name' is 'Port On'. The 'Rule Valid from' is '5.10.2021' and 'to' is '5.4.2022' in dd.mm.yyyy format. 'Random Trigger Probability' is set to 90. 'Random Trigger Jitter' is 0 secs. 'enable trigger' is set to 'yes'. 'Action mode' is 'Switch Power Ports'. Buttons for 'Delete', 'Save', and 'Cancel' are at the bottom.


For this rule, on the "Options" tab, the time period is limited to the range between 5.10.2021 and 5.4.2022. In this example, the timer rule is only executed with a probability (Random Trigger Probability) of 90%.



The screenshot shows the 'Timer - Rule 1: Port On' configuration window with the 'Action PortSwitch' tab selected. It displays two action tables for 'Switch Power Ports'. Action 1 shows a row of 12 'On' buttons and a row of 12 'Off' buttons. Action 2 shows a row of 12 buttons where the 1st and 5th are 'On' and the others are '-'. A tooltip '5: Power Port' is shown over the 5th button. Below the tables, 'Between Action1 and Action 2 : wait' is set to 90 'minute(s)'. A 'Test Action' button is present. 'Delete', 'Save', and 'Cancel' buttons are at the bottom.

In this example, port 1 and port 5 are enabled and disabled after 90 minutes by batch mode.

 Action 2 is realized internally by a batch mode. This does not continue to run if a restart of the device has taken place in the meantime.

 A popup on the mouse pointer shows the port number of the field.

Console Commands

The screenshot shows a configuration window titled "Timer - Rule 1: Port On". It has four tabs: "Trigger: Date/Time Pattern", "Options", "Action PortSwitch", and "Action Cli". The "Action Cli" tab is selected. Inside the main area, there is a text box labeled "Perform CLI Command:" containing the text "port 1 reset" and "port 3 state set 1". Below the text box is a "Test Action" button. At the bottom right of the window are "Delete", "Save", and "Cancel" buttons.

Instead of switching a port, one or more console commands can be executed. These commands are entered in the "Action CLI" register. The "Action Cli" tab can only be selected if the option "Perform CLI Cmd" is activated in "Options".

Example Switching a Port on a Date

If you want to switch on a timer on a certain date at a certain time and switch it off at a later time, you cannot do it directly with a simple timer. Therefore it can be useful to create the timer as a simple timer first, and then customize it in the advanced dialog.

The screenshot shows a configuration window titled "Timer Rule". It has a "Switch" dropdown set to "3: Power Port" and an "On" dropdown set to "On". Below this, there are "From" and "To" time selectors. "From" is set to "09:25" and "To" is set to "17:30". Underneath, there are checkboxes for "On weekdays:" with all days (Mon, Tue, Wed, Thu, Fri, Sat, Sun) checked. At the bottom right are "Save" and "Cancel" buttons.

Switch port 3 on every day at 9:25, and off again at 17:30. You save.

The screenshot shows a configuration window titled "Timer - Rule 3: Port On". It has four tabs: "Trigger: Date/Time Pattern", "Options", "Action PortSwitch", and "Action Cli". The "Options" tab is selected. Inside the main area, there is a "Rule Name" field with "Port On" entered. Below it is a "Rule Valid from" field with "24.10.2022" and a "to" field with "24.10.2022" and "dd.mm.yyyy" label. There is a "Random Trigger Probability" spinner set to "100" and a "Random Trigger Jitter" field set to "0" with "secs" label. Below these are "enable trigger:" radio buttons with "yes" selected and "no" unselected. At the bottom, there are "Action mode:" radio buttons with "Switch Power Ports" selected and "Perform CLI Cmd" unselected. At the bottom right are "Delete", "Save", and "Cancel" buttons.

Then call up the two timer rules you created ("On" and "Off") and enter the date on which the switching operation is to take place in the "Options" tab.

Example blind control

Timer - Rule 3: Port On

Trigger: Date/Time Pattern **Options** Action PortSwitch Action Cli

Rule Name: Random Trigger Port 1

Rule Valid from: [] to [] dd.mm.yyyy

Random Trigger Probability: 100

Random Trigger Jitter: 1800 secs

enable trigger: yes no

Action mode: Switch Power Ports Perform CLI Cmd

Delete Save Cancel

You can use the jitter e.g. for a shutter control. In the classic example of a shutter control, you do not always want to raise and lower the shutters at the same time in order to confuse potential burglars. The jitter of 1800 seconds means that the action is executed randomly in a period between 30 minutes before and 30 minutes after the programmed time. The probability (Random Trigger Probability) of execution here is 100%.

3.6 Sensors

Sensors Config

Sensor: 1: 7106 - 7106 ▾
Sensor Name: 7106
Select Sensor Field: Temperature (°C) ▾

Enable value-threshold message trigger: yes no
Maximum value: 65.0 °C
Minimum value: 25.0 °C
Hysteresis: 3.0 °C

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 ▾

Enable time-interval message trigger: yes no
every 10 second(s)
for Console- and MQTT channels

Enable value-delta message trigger: yes no
every value step of 5.0 °C
for Console- and MQTT channels

Message channels: Syslog SNMP Email Console
 MQTT: normal MQTT message ▾
 Beeper: Beeper mode : continous ▾
 Flashing display

Misc sensor options

Min/Max measurement period: 24 Hours ▾
Allow beeper for other alarms: yes no

Sensor: Selects a sensor type 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 adjustable sensor name.

Sensor Name: Changeable name for this sensor. For example, you can give the temperature and the humidity a different name, even if they belong to the same sensor.

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

Enable value-threshold message trigger: Enables monitoring of sensor threshold values.

Maximum/Minimum value: Adjustable threshold values at which messages should be sent via console (Telnet/SSH), SNMP trap, Syslog, MQTT or e-mail.

Hysteresis: Defines the distance that must be exceeded after a limit value of an external sensor has been exceeded in order to signal that the limit value has fallen below.

When above/below Min/Max value Switch Port: Switches a port depending on the exceeding or falling below of a limit value.

Enable time interval message trigger: Generates console (Telnet/SSH) and MQTT messages within time intervals.

Enable value-delta message trigger: Generates console (Telnet/SSH) and MQTT messages when a sensor value deviates by a delta value.

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

For the beeper, you can choose between a continuous and an interrupted tone. Flashing display causes the 7-segment display to flash. Pressing a front panel button resets the beeper and the flashing display.

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

Allow beeper for other alarms: Switches on the beeper for all messages when the sensor limits are exceeded. In addition, in Message channels can be configured for each sensor individually whether and which type of buzzer should be activated.

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
...

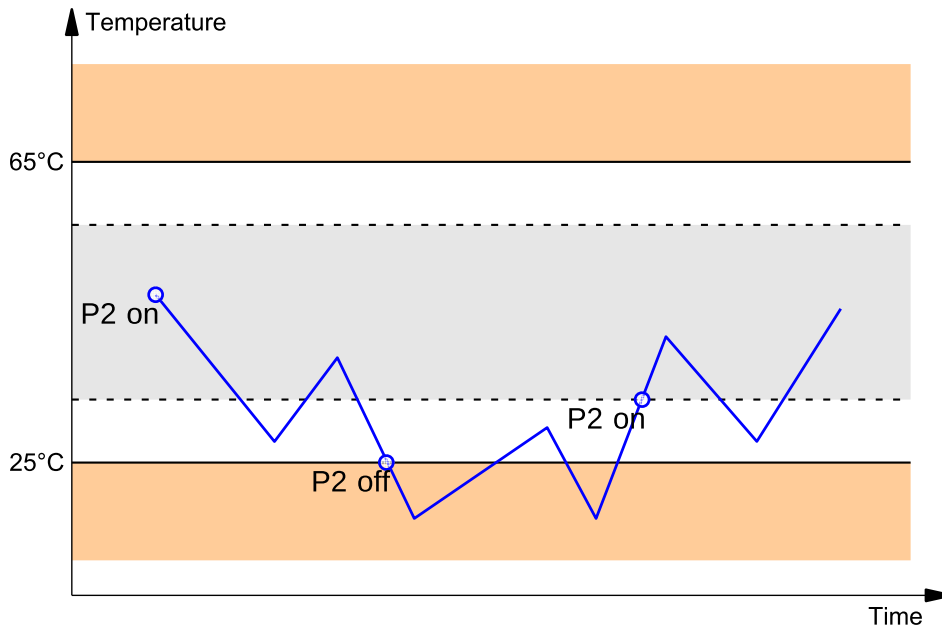
49.1 °C - is below the upper limit, but in the hysteresis range
49.0 °C - is below the upper limit, but in the hysteresis range
48.9 °C - a message is generated for underrunning the upper limit inclusive hysteresis range
...

3.6.1 Port Switching

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

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

Configuration




- When above Max value: Switch port to
- When below Max value: Switch port to
- When above Min value: Switch port to
- When below Min value: Switch port to

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

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

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

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

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

3.7 E-Mail

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

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

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

Sender address: The E-Mail address of the sender.

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

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

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


SMTP Connection Security: Transmission via SSL or no encryption.

SMTP 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.

3.8 Front Panel

Front Panel

Button Lock: yes no

Allow switching all ports: yes no

Display 1 default: ▾

LED Mode: ▾

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

Allow switching all ports: Allows to switch all ports on or off with the front panel buttons.

Display 1 default: Selects the view of sensor values for the display.


LED Mode: Allows configuration of the mode of what the 8x on/off indicators display: Alternately every 5 seconds the output ports and the input ports, or only output ports, or only input ports.

Specifications




4 Specifications

4.1 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.

 This chapter is general for all Gude devices. Depending on the device model are ports, certain sensors or other features not available.

List of different access options:

| Interface | Scope of Access |
|--|---|
| HTTP | read / write status of Power Ports (relays or eFuses) read / write all configuration data read / write all status information (full access to the device) |
| Console  | read / write status of Power Ports (relays or eFuses) read / write all configuration data read / write all status information (full access to the device) |
| SNMP  | read / write status of Power Ports (relays or eFuses) read / write names of Power Ports (relays or eFuses) read / write status of Port start configuration read / write status Buzzer read / write configuration of power sources (EPC 8291) read / write fan configuration (EPC 8291) read measurement values of external sensors read measurement values of all energy sensors read NTP time and status resetting the energy meters read the status of Overvoltage Protection |
| Modbus TCP  | read / write status of Power Ports (relays or eFuses) read status of Inputs read / write configuration of power sources (EPC 8291) read / write fan configuration (EPC 8291) read measurement values of external sensors read measurement values of all energy sensors read the status of Overvoltage Protection |
| MQTT | Execute console commands |

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

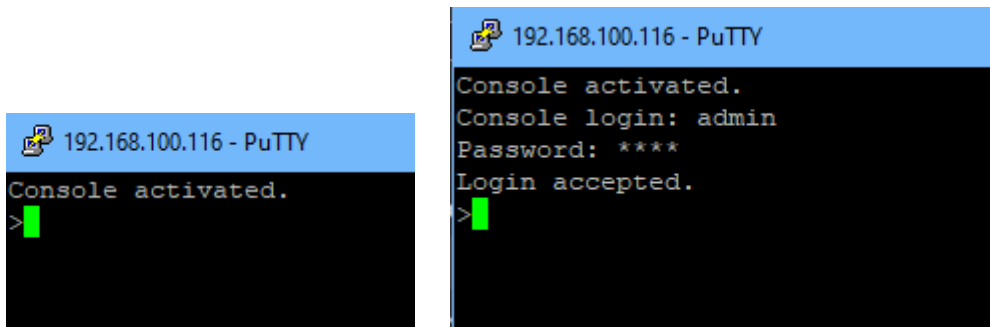
4.2 Console

For the configuration and control of the device, there is a set of commands with paramet-

ers that can be entered through a console. The console is available via SSH or 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^[36].

Login

A ssh / telnet log in can be configured with password or without:



Command Set

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

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

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

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

Parameter

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

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

the following instruction pairs are equivalent:

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

or

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

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

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

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.

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 there is no need to filter the sent characters to process the return values.

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

Editing

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

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

 This chapter is general for all Gude devices. Depending on the device type, ports or

certain sensors may not be available.

Sensor Examples

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.

```
>extsensor 1 0 value show
```

Displays temperature of the sensor at Port 1

b) Line Sensors


 For devices with 230V input metering (Metered PDU).

```
>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).

```
>linesensor 1 "0,1,2,3,12" show
>linesensor 1 1 show
```

These variants give the sensor values of the field list or of a sensor at Line-In 1.

 For devices with Overvoltage Protection, the "linesensor all" command also outputs the state of the protection ("OVP=x"). A "1" means ok, a "0" a failure of the protection.

c) Port Sensors

 For devices with 230V output metering (Outlet-Metered PDU).

```
>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="225V",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).

```
>portsensor 2 "0,1,2,3,12" show
>portsensor 2 1 show
```

These variants give the sensor values of the field list or a sensor to at Outlet Port 2.



The following examples refer to Gude devices that have switchable ports.

d) Displaying Port Relays

```
>port all state 1 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.

4.2.1 SSH

The device supports SSH-2 connections with either public key authentication or user name and password. The "login" must be enabled for SSH. Users and passwords can be stored locally or retrieved via a radius server. If you want to use SSH in a terminal, [Activate echo](#) should be enabled.

Public Keys

The following public keys are accepted:

| Key type | Length |
|----------|------------|
| RSA | 2048, 4096 |
| ECDSA | 256, 384 |

Generation with PuTTYgen

Specifications

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAKA926b1dwfApsq1ra3Hzw
+tL5mdXuqglDgQ1Db7Klm16mqmzGoVBX6kmVWmx2XRucTUQohrVzvqAUj
+38VtDLcTIXbtZS7i7WrqDdougl28k5Jx7JORpMuNGBLOsdPK5KNeYm9SPo8wltN0
pc04U3r9unNjqTar2cXqui4XHdvvFr0dByaaeR3yBWjivdv46uuXaia2T4p6Ou4Pkys0/b
/AnBVSw2SeRNiVVoEAUx8eXrIRkVhrXZtzGaxK2xDE3l9Ziz//xt79o6V7yih00ROuf1bit
```

Key fingerprint:

Key comment:

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Generated keys can be copied directly from e.g. PuTTYgen,

Upload new SSH public key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAA
ADAQABAAABAQDTliqb/
```

Delete public key

and inserted into the Configuration - Console input field. Public keys are accepted in SSH2 or OpenSSH format.

Generation with ssh-keygen

The tool ssh-keygen is mostly shipped with Linux and Windows to generate SSH keys. Here is an example to generate an ECDSA 384 key.

```
ssh-keygen -t ecdsa -b 384 -f ssh.key
```

In the file ssh.pub is then the private key, the content of ssh.key.pub is inserted into the field "Upload SSH public key:".

Upload new SSH public key:

```
ecdsa-sha2-nistp384
AAAAE2VjZHNhLXNoYTl
tbmlzdHAzODQAAAAIbm
```

Delete public key

4.2.2 Console Cmd 2304

| Command | Description | Note |
|---------|-------------|------|
|---------|-------------|------|

Specifications

| | | |
|--|--|---|
| logout | go to login prompt w hen enabled | 2 |
| quit | quits telnet session - nothing in serial console | 2 |
| back | back one cmd level | 2 |
| help | show all cmds from this level | 2 |
| help all | show all cmds | 2 |
| <hr/> | | |
| clock | enters cmd group "clock" | |
| clock ntp enabled set {OFF=0 ON=1} | enables ntp | |
| clock ntp enabled show | show s if ntp enabled | |
| clock timezone set {minutes} | sets timezone | |
| clock timezone show | show s timezone | |
| clock dst enabled set {OFF=0 ON=1} | enables dst | |
| clock dst enabled show | show s if dst is enabled | |
| clock manual set "{hh:mm:ss yyyy-mm-dd}" | sets time and date manually | |
| clock show | show s actual time and date | |
| clock ntp server {PRIMARY=0 BACKUP=1} set "{dns_name}" | sets ntp server name | |
| clock ntp server {PRIMARY=0 BACKUP=1} show | show s ntp server name | |
| <hr/> | | |
| console | enters cmd group "console" | |
| console version | show s unique console version number | |
| console telnet enabled set {OFF=0 ON=1} | enables telnet on/off | |
| console telnet enabled show | show s if telnet enabled | |
| console telnet port set {ip_port} | sets telnet port | |
| console telnet port show | show s telnet port | |
| console telnet raw set {OFF=0 ON=1} | sets raw mode (disables editing) on/off | |
| console telnet raw show | show s if raw mode enabled | |
| console telnet echo set {OFF=0 ON=1} | enables echo on/off | |
| console telnet echo show | show s if echo enabled | |
| console telnet activeneg set {OFF=0 ON=1} | enables telnet active negotiation (IAC) on/off | |
| console telnet activeneg show | show s if active negotiation enabled | |
| console telnet login set {OFF=0 ON=1} | enables login on/off | |
| console telnet login show | show s if login enabled | |
| console telnet login local set {OFF=0 ON=1} | enables local login on/off | |
| console telnet login local show | show s if local login enabled | |
| console telnet login radius set {OFF=0 ON=1} | enables login for RADIUS on/off | |
| console telnet login radius show | show s 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 | show s if login delay enabled | |
| console telnet pushmsgs config set {OFF=0 ON=1} | enables persistent push msgs | |
| console telnet pushmsgs config show | show s if persistent push msgs are enabled | |
| console telnet pushmsgs set {OFF=0 ON=1} | enables temporary push msgs | |
| console telnet pushmsgs show | show s if temporary push msgs are enabled | |
| console telnet user set "{username}" | sets login user name | |
| console telnet user show | show s login user name | |
| console telnet passw d set "{passw d}" | sets login passw ord | |
| console telnet passw d hash set "{passw d}" | sets login hashed passw ord | |
| console ssh enabled set {OFF=0 ON=1} | enables SSH | |
| console ssh enabled show | show s if SSH enabled | |
| console ssh port set {ip_port} | sets SSH port | |
| console ssh port show | show s SSH port | |
| console ssh echo set {OFF=0 ON=1} | enables echo on/off | |
| console ssh echo show | show s if echo enabled | |
| console ssh pushmsgs config set {OFF=0 ON=1} | enables persistent push msgs | |
| console ssh pushmsgs config show | show s if persistent push msgs are enabled | |
| console ssh pushmsgs set {OFF=0 ON=1} | enables temporary push msgs | |
| console ssh pushmsgs show | show s if temporary push msgs are enabled | |
| console ssh public hash set "{passw d}" | sets hash of SSH public key | |
| console ssh public hash show | show s hash of SSH public key | |
| <hr/> | | |
| email | enters cmd group "email" | |
| email enabled set {OFF=0 ON=1} | enables email on/off | |
| email enabled show | show s if email is enabled | |
| email sender set "{email_addr}" | sets email sender address | |

Specifications

| | | |
|--|---|---|
| email sender show | show s email sender address | |
| email recipient set "{email_addr}" | sets email recipient address | |
| email recipient show | show s email recipient address | |
| email server set "{dns_name}" | sets email SMTP server address | |
| email server show | show s email SMTP server address | |
| email port set {ip_port} | sets email SMTP port | |
| email port show | show s email SMTP port | |
| email security set {NONE=0 STARTTLS=1 SSL=2} | sets SMTP connection security | |
| email security show | show s SMTP connection security | |
| email auth set {NONE=0 PLAIN=1 LOGIN=2} | sets email authentication | |
| email auth show | show email authentication | |
| email user set "{username}" | sets SMTP username | |
| email user show | show s SMTP username | |
| email passw d set "{passw d}" | sets SMTP passw ord | |
| email passw d hash set "{passw d}" | sets crypted SMTP passw ord | |
| email testmail | send test email | |
| | | |
| ethernet | enters cmd group "ethernet" | |
| ethernet mac show | show s MAC address | |
| ethernet link show | show s 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 | show s preferred speed for PHY Auto Negotiation | |
| | | |
| extinput | enters cmd group "extinput" | |
| extinput {port_num} {inp_num} state show | show s input state | |
| extinput all state {MODE0=0 MODE1=1 MODE2=2} show | show s input state of all ports in 3 different view modes | 4 |
| extinput {port_num} {inp_num} name set "{name}" | sets sensor name to label | |
| extinput {port_num} {inp_num} name show | show s label of sensor | |
| extinput {port_num} {inp_num} invert enabled set {OFF=0 ON=1} | inverts input on/off | |
| extinput {port_num} {inp_num} invert enabled show | show s if input inverted | |
| extinput {port_num} {inp_num} label {LOW=0 HIGH=1} set "{name}" | sets input low /high text | |
| extinput {port_num} {inp_num} label {LOW=0 HIGH=1} show | show s input low /high text | |
| extinput {port_num} {inp_num} events set {OFF=0 ON=1} | enables input events on/off | |
| extinput {port_num} {inp_num} events show | show s if input events are enabled | |
| extinput {port_num} {inp_num} events type set "{EVT_SY SLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_BEEPER=5,EVT_DISPLAY=6,EVT_CONSOLE=7,EVT_MQTT=8}" | enables different event types | |
| extinput {port_num} {inp_num} events type show | show s w hat event types are enabled | |
| extinput {port_num} {inp_num} publish mode set {NONE=0 INTERVAL=1 DELTA=2 INTERV_DELTA=3} | sets publish mode | |
| extinput {port_num} {inp_num} publish mode show | show s publish mode | |
| extinput {port_num} {inp_num} publish mqtt retain set {OFF=0 ON=1} | sets mqtt retain | |
| extinput {port_num} {inp_num} publish mqtt retain show | show s if mqtt retain set | |
| extinput {port_num} {inp_num} publish timer set {num_secs} | sets publish time interval | |
| extinput {port_num} {inp_num} publish timer show | show s publish time interval | |
| extinput {port_num} {inp_num} {LOW=0 HIGH=1} port set {port_num} | sets Port for Pow er Port Sw itching actions | |
| extinput {port_num} {inp_num} {LOW=0 HIGH=1} port show | show s Port for Pow er Port Sw itching actions | |
| extinput {port_num} {inp_num} {LOW=0 HIGH=1} state set {OFF=0 ON=1 DISABLED=2} | sets Port state for Pow er Port Sw itching actions | |
| extinput {port_num} {inp_num} {LOW=0 HIGH=1} state show | show s Port state for Pow er Port Sw itching actions | |

Specifications

| | | |
|--|--|---|
| extsensor | enters cmd group "extsensor" | |
| extsensor all show | shows all values from connected external sensors | |
| extsensor all show | shows all plugged sensors and fields | |
| extsensor {port_num} {sen_field} value show | shows sensor value | 6 |
| extsensor {port_num} {sen_type} label set "{name}" | sets sensor name to label | 6 |
| extsensor {port_num} {sen_type} label show | shows label of sensor | 6 |
| extsensor {port_num} type show | shows type of sensor | |
| extsensor {port_num} {sen_type} {sen_field} events set {off=0 on=1} | enables sensor events on/off | 6 |
| extsensor {port_num} {sen_type} {sen_field} events show | shows if sensor events are enabled | 6 |
| extsensor {port_num} {sen_type} {sen_field} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5,EVT_DISPLAY=6,EVT_CONSOLE=7,EVT_MQTT=8}" | enables different event types | 6 |
| extsensor {port_num} {sen_type} {sen_field} events type show | shows what event types are enabled | 6 |
| extsensor {port_num} {sen_type} {sen_field} events beeper mode set {CONTINUOUS=0 INTERMITTENT=1} | sets beeper tone | |
| extsensor {port_num} {sen_type} {sen_field} events beeper mode show | shows beeper tone | |
| 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 hysteresis value for sensor | 6 |
| extsensor {port_num} {sen_type} {sen_field} hyst show | shows hysteresis value for sensor | 6 |
| extsensor {port_num} {sen_type} {sen_field} publish mode set {NONE=0 INTERVAL=1 DELTA=2 INTERV_DELTA=3} | sets publish mode | |
| extsensor {port_num} {sen_type} {sen_field} publish mode show | shows publish mode | |
| extsensor {port_num} {sen_type} {sen_field} publish mqtt retain set {OFF=0 ON=1} | sets mqtt retain | |
| extsensor {port_num} {sen_type} {sen_field} publish mqtt retain show | shows if mqtt retain set | |
| extsensor {port_num} {sen_type} {sen_field} publish timer set {num_secs} | sets publish time interval | |
| extsensor {port_num} {sen_type} {sen_field} publish timer show | shows publish time interval | |
| extsensor {port_num} {sen_type} {sen_field} publish delta set {float} | sets publish delta value | |
| extsensor {port_num} {sen_type} {sen_field} publish delta show | shows publish delta value | |
| extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port set {port_num} | sets Port for Power Port Switching actions | 6 |
| extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port show | shows Port for Power Port Switching actions | 6 |
| extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} state set {OFF=0 ON=1 DISABLED=2} | sets Port state for Power Port Switching actions | 6 |

Specifications

| | | |
|--|--|---|
| extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} state show | shows Port state for Power Port Switching actions | 6 |
| extsensor period set {24H=0 12H=1 2H=2 1H=3 30MIN=4} | sets sensor Min/Max measurement period | |
| extsensor period show | shows sensor Min/Max measurement period | |
| extsensor beeper set {OFF=0 ON=1} | enables beeper sensor alarms | |
| extsensor beeper show | shows if beeper sensor alarms are enabled | |
| extsensor {port_num} {sen_field} calib set {float} | sets calibration offset for temperature or humidity | |
| extsensor {port_num} {sen_field} calib show | shows calibration offset for temperature or humidity | |
| http | enters cmd group "http" | |
| http server set {HTTP_BOTH=0 HTTPS_ONLY=1 HTTP_ONLY=2 HTTPS_REDIR=3} | sets accepted connection types | |
| http server show | shows accepted 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 tls mode set {TLS12=0 TLS13_12=1 TLS13=2 TLS13_12_11=3} | restricts TLS mode | |
| http tls mode show | shows TLS mode restriction | |
| http auth mode set {BASIC=0 SESSION=1 SESSION_EXT=2} | sets http session authentication mode | |
| http auth mode show | shows http session authentication mode and compatibility | |
| http passwd enabled set {OFF=0 ON=1} | enables http passwd on/off | |
| http timeout admin set {num_secs} | sets admin session timeout | |
| http timeout admin show | shows admin session timeout | |
| http timeout user set {num_secs} | sets user session timeout | |
| http timeout user show | shows user session timeout | |
| http passwd enabled show | shows if http passwd enabled | |
| http passwd local set {OFF=0 ON=1} | enables local login on/off | |
| http passwd local show | shows if local login enabled | |
| http passwd radius set {OFF=0 ON=1} | enables login for RADIUS on/off | |
| http passwd radius show | shows if RADIUS login enabled | |
| http passwd user set "{passwd}" | sets http user passwd | |
| http passwd admin set "{passwd}" | sets http admin passwd | |
| http passwd hash user set "{passwd}" | sets hashed http user passwd | |
| http passwd hash admin set "{passwd}" | sets hashed http admin passwd | |
| input | enters cmd group "input" | |
| input {port_num} state show | shows input state | |
| input all state {MODE0=0 MODE1=1 MODE2=2} show | shows input state of all ports in 3 different view modes | 4 |
| input {port_num} name set "{name}" | sets sensor name to label | |
| input {port_num} name show | shows label of sensor | |
| input {port_num} invert enabled set {off=0 on=1} | inverts input on/off | |
| input {port_num} invert enabled show | shows if input inverted | |
| input {port_num} label {LOW=0 HIGH=1} set "{name}" | sets input low /high text | |
| input {port_num} label {LOW=0 HIGH=1} show | shows inputs low /high text | |
| input {port_num} events set {off=0 on=1} | enables input events on/off | |
| input {port_num} events show | shows if input events are enabled | |
| input {port_num} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5,EVT_DISPLAY=6,EVT_CONSOLE=7}" | enables different event types | |
| input {port_num} events type show | shows what event types are enabled | |
| input {port_num} {inp_num} publish mode set {NONE=0 INTERVAL=1 DELTA=2 INTERV_DELTA=3} | sets publish mode | |
| input {port_num} {inp_num} publish mode show | shows publish mode | |
| input {port_num} {inp_num} publish mqtt retain set {OFF=0 ON=1} | sets mqtt retain | |

Specifications

| | | |
|---|---|---|
| input {port_num} {inp_num} publish mqtt retain show | shows if mqtt retain set | |
| input {port_num} {inp_num} publish timer set {num_secs} | sets publish time interval | |
| input {port_num} {inp_num} publish timer show | shows publish time interval | |
| input {port_num} {LOW=0 HIGH=1} port set {port_num} | sets Port for Power Port Switching actions | |
| input {port_num} {LOW=0 HIGH=1} port show | shows Port for Power Port Switching actions | |
| input {port_num} {LOW=0 HIGH=1} state set {OFF=0 ON=1 DISABLED=2} | sets Port state for Power Port Switching actions | |
| input {port_num} {LOW=0 HIGH=1} state show | shows Port state for Power Port Switching actions | |
| input volt3 state show | shows state of 3V input voltage {ON=1 VERR=3} | |
| input volt12 state set {OFF=0 VLO=1 VHI=2} | sets state of 12V input voltage | |
| input volt12 state show | shows state of 12V input voltage {OFF=0 VLO=1 VHI=2 VERR=3} incl possible error condition | |
| ip4 | enters cmd group "ip4" | |
| ip4 hostname set "{name}" | sets device hostname | |
| ip4 hostname show | shows device hostname | 3 |
| ip4 address set "{ip_address}" | sets IPv4 address | |
| ip4 address show | shows IPv4 address | 3 |
| ip4 netmask set "{ip_address}" | sets IPv4 netmask | |
| ip4 netmask show | shows IPv4 netmask | 3 |
| ip4 gateway set "{ip_address}" | sets IPv4 gateway address | |
| ip4 gateway show | shows IPv4 gateway address | 3 |
| ip4 dns set "{ip_address}" | sets IPv4 DNS server address | |
| ip4 dns show | shows IPv4 DNS server address | 3 |
| ip4 dhcp enabled set {OFF=0 ON=1} | enables IPv4 DHCP on/off | |
| ip4 dhcp enabled show | shows IPv4 DHCP state | 3 |
| ip6 | enters cmd group "ip6" | |
| ip6 enabled set {OFF=0 ON=1} | enables IPv6 on/off | |
| ip6 enabled show | shows if IPv6 is enabled | 3 |
| ip6 routadv enabled set {OFF=0 ON=1} | enables IPv6 router advertisement | |
| ip6 routadv enabled show | shows IPv6 router advertisement state | 3 |
| ip6 dhcp enabled set {OFF=0 ON=1} | enables IPv6 DHCP on/off | |
| ip6 dhcp enabled show | shows if IPv6 DHCP is enabled | 3 |
| ip6 address show | show all IPv6 addresses | 4 |
| ip6 gateway show | show all IPv6 gateways | 4 |
| ip6 dns show | show all IPv6 DNS server | 4 |
| ip6 manual enabled set {OFF=0 ON=1} | enables manual IPv6 addresses | |
| ip6 manual enabled show | shows if manual IPv6 addresses are enabled | 3 |
| ip6 manual address {1..4} set "{ip_address}" | sets manual IPv6 address | |
| ip6 manual address {1..4} show | shows manual IPv6 address | 3 |
| ip6 manual gateway set "{ip_address}" | sets manual IPv6 gateway address | |
| ip6 manual gateway show | shows manual IPv6 gateway address | 3 |
| ip6 manual dns {1..2} set "{ip_address}" | sets manual IPv6 DNS server address | |
| ip6 manual dns {1..2} show | shows manual IPv6 DNS server address | 3 |
| ipacl | enters cmd group "ipacl" | |
| ipacl ping enabled set {OFF=0 ON=1} | enables ICMP ping on/off | |
| ipacl ping enabled show | shows if ICMP ping enabled | |
| ipacl enabled set {OFF=0 ON=1} | enable IP filter on/off | |
| ipacl enabled show | shows if IP filter enabled | |
| ipacl filter {ipacl_num} set "{dns_name}" | sets IP filter {ipacl_num} | |
| ipacl filter {ipacl_num} show | shows IP filter {ipacl_num} | |
| modbus | enters cmd group "modbus" | |
| modbus enabled set <off=0/on=1> | enables Modbus TCP support | |
| modbus enabled show | shows if Modbus is enabled | |
| modbus port set <ip_port> | sets Modbus TCP port | |
| modbus port show | shows Modbus TCP port | |
| mqtt | enters cmd group "mqtt" | |

Specifications

| | | |
|---|---|---|
| mqtt {broker_idx} enabled set {OFF=0 ON=1} | enable mqtt | |
| mqtt {broker_idx} enabled show | show s if mqtt enabled | |
| mqtt {broker_idx} server set "{dns_name}" | sets broker name | |
| mqtt {broker_idx} server show | show s broker name | |
| mqtt {broker_idx} tls enabled set {OFF=0 ON=1} | enable TLS | |
| mqtt {broker_idx} tls enabled show | show s if TLS enabled | |
| mqtt {broker_idx} port set {ip_port} | set broker TCP/IP port | |
| mqtt {broker_idx} port show | show s broker TCP/IP port | |
| mqtt {broker_idx} user set "{username}" | sets username | |
| mqtt {broker_idx} user show | show s username | |
| mqtt {broker_idx} passw d set "{passw d}" | sets passw ord | |
| mqtt {broker_idx} passw d hash set "{passw d}" | sets hashed passw d | |
| mqtt {broker_idx} client set "{name}" | sets client name | |
| mqtt {broker_idx} client show | show s client name | |
| mqtt {broker_idx} qos set {QOS0=0 QOS1=1} | sets QoS level | |
| mqtt {broker_idx} qos show | show s QoS level | |
| mqtt {broker_idx} keepalive set {num_secs} | sets keep-alive time | |
| mqtt {broker_idx} keepalive show | show s keep-alive time | |
| mqtt {broker_idx} topic set "{name}" | sets topic prefix | |
| mqtt {broker_idx} topic show | shw os topic prefix | |
| mqtt {broker_idx} console enabled set {OFF=0 ON=1} | permit console cmds | |
| mqtt {broker_idx} console enabled show | show s if console cmds allow ed | |
| mqtt {broker_idx} device data timer set {num_secs} | sets telemetry interval | |
| mqtt {broker_idx} device data timer show | show s telemetry interval | |
| port | enters cmd group "port" | |
| port {port_num} state set {OFF=0 ON=1} | sets port to new state | |
| port {port_num} state show | show s 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 | show s all port states in 3 different view modes | 4 |
| port all set {OFF=0 ON=1 OFF_REV=2 ON_REV=3} | sw itch all ports on/off forw ard or reverse | |
| port restart all set {REINIT=0 OFF_REV_REINIT=1 OFF_REINIT=2} | reinit coldstart sequence (optional first all off) | |
| port {port_num} reset | start reset sequence for port | |
| port {port_num} toggle | toggles port | |
| port {port_num} batch set {OFF=0 ON=1} w ait {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 | show s 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 | show s port coldstart initialization | |
| port {port_num} initState delay set {num} | sets port init delay | |
| port {port_num} initState delay show | show s port init delay | |
| port {port_num} repow erdelay set {num} | sets port repow er delay | |
| port {port_num} repow erdelay show | show s port repow er delay | |
| port {port_num} resettime set {num} | sets port reset duration | |
| port {port_num} resettime show | show s port reset duration | |
| port {port_num} w atchdog enabled set {OFF=0 ON=1} | sets port w atchdog to on/off | |
| port {port_num} w atchdog enabled show | show s port w atchdog state | |
| port {port_num} w atchdog mode set {OFF=0 PORT_RESET=1 IP_MS=2 IP_MS_INV=3} | sets port w atchdog mode | |
| port {port_num} w atchdog mode show | show s port w atchdog mode | |
| port {port_num} w atchdog type set {WD_ICMP=0 WD_TCP=1} | sets port w atchdog type | |
| port {port_num} w atchdog type show | show s port w atchdog type | |
| port {port_num} w atchdog link dow n set {OFF=0 ON=1} | sets if w atchdog active w hen eth link dow n | |
| port {port_num} w atchdog link dow n show | show s if w atchdog active w hen eth link dow n | |

Specifications

| | | |
|---|---|--|
| port {port_num} watchdog host set "{dns_name}" | sets port watchdog host target | |
| port {port_num} watchdog host show | show s port watchdog host target | |
| port {port_num} watchdog port set {ip_port} | sets port watchdog TCP port | |
| port {port_num} watchdog port show | show s port watchdog TCP port | |
| port {port_num} watchdog pinginterval set {num} | sets port watchdog ping interval | |
| port {port_num} watchdog pinginterval show | show s port watchdog ping interval | |
| port {port_num} watchdog pingretries set {num} | sets port watchdog ping retries | |
| port {port_num} watchdog pingretries show | show s 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 | show s port watchdog retry booting state | |
| port {port_num} watchdog bootretries set {num} | sets port watchdog retry boot timeout | |
| port {port_num} watchdog bootretries show | show s port watchdog retry boot timeout | |
| radius | | |
| radius | enters cmd group "radius" | |
| radius {PRIMARY=0 SECONDARY=1} enabled set <off=0/on=1> | enables radius client | |
| radius {PRIMARY=0 SECONDARY=1} enabled show | show if radius client enabled | |
| radius {PRIMARY=0 SECONDARY=1} server set "<dns_name>" | sets radius server address | |
| radius {PRIMARY=0 SECONDARY=1} server show | show s radius server address | |
| radius {PRIMARY=0 SECONDARY=1} password set "{password}" | sets radius server shared secret | |
| radius {PRIMARY=0 SECONDARY=1} password hash set "{password}" | 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 | show s server request timeout | |
| radius {PRIMARY=0 SECONDARY=1} retries set {0..99} | sets server number of retries | |
| radius {PRIMARY=0 SECONDARY=1} retries show | show s server number of retries | |
| radius chap enabled set <off=0/on=1> | enables CHAP | |
| radius chap enabled show | show s if CHAP is enabled | |
| radius message auth set <off=0/on=1> | enables request message authentication | |
| radius message auth show | show s if request message authentication is enabled | |
| radius default timeout set {num_secs} | sets default session timeout (when not returned as Session-Timeout Attribute) | |
| radius default timeout show | show s default session timeout | |
| snmp | | |
| snmp | enters cmd group "snmp" | |
| snmp port set {ip_port} | sets SNMP UDP port | |
| snmp port show | show s SNMP UDP port | |
| snmp snmpget enabled set {OFF=0 ON=1} | enables SNMP GET cmds on/off | |
| snmp snmpget enabled show | show if SNMP GET cmds are enabled | |
| snmp snmpset enabled set {OFF=0 ON=1} | enables SNMP SET cmds on/off | |
| snmp snmpset enabled show | show if SNMP SET cmds are enabled | |
| snmp snmpv2 enabled set {OFF=0 ON=1} | enables SNMP v2 on/off | |
| snmp snmpv2 enabled show | show if SNMP v2 is enabled | |
| snmp snmpv2 public set "{text}" | enables SNMP v3 on/off | |
| snmp snmpv2 public show | show if SNMP v3 is enabled | |
| snmp snmpv2 private set "{text}" | sets SNMP v2 private community | |
| snmp snmpv2 private show | show s SNMP v2 public community | |
| snmp system {CONTACT=0 NAME=1 LOCATION=2} set "{text}" | sets sysLocation/sysName/sysContact | |
| snmp system {CONTACT=0 NAME=1 LOCATION=2} show | gets sysLocation/sysName/sysContact | |
| snmp snmpv3 enabled set {OFF=0 ON=1} | sets SNMP v2 private community | |
| snmp snmpv3 enabled show | show s SNMP v2 private community | |
| snmp snmpv3 username set "{text}" | sets SNMP v3 username | |
| snmp snmpv3 username show | show s SNMP v3 username | |

Specifications

| | | |
|---|--|------------|
| snmp snmpv3 authalg set {NONE=0 MD5=1 SHA1=2 SHA256=3 SHA384=4 SHA512=5} | sets SNMP v3 authentication | |
| snmp snmpv3 authalg show | show SNMP v3 authentication algorithm | |
| snmp snmpv3 privalg set {NONE=0 DES=1 3DES=2 AES128=3 AES192=4 AES256=5 AES192*=6 AES256*=7} | sets SNMP v3 privacy algorithm | |
| snmp snmpv3 privalg show | show SNMP v3 privacy algorithm | |
| snmp snmpv3 authpasswd set "{passwd}" | sets SNMP v3 authentication passwd | |
| snmp snmpv3 privpasswd set "{passwd}" | sets SNMP v3 privacy passwd | |
| snmp snmpv3 authpasswd hash set "{passwd}" | sets SNMP v3 authentication hashed passwd | |
| snmp snmpv3 privpasswd hash set "{passwd}" | sets SNMP v3 privacy hashed passwd | |
| snmp trap type set {NONE=0 V1=1 V2=2 V3=3} | sets type of SNMP traps | |
| snmp trap type show | show SNMP trap type | |
| snmp trap receiver {trap_num} set "{dns_name}" | sets address and port of SNMP trap receiver | {trap_num} |
| snmp trap receiver {trap_num} show | show address and port of SNMP trap receiver | {trap_num} |
| syslog | enters cmd group "syslog" | |
| syslog enabled set {OFF=0 ON=1} | enables syslog msgs on/off | |
| syslog enabled show | show if syslog enabled | |
| syslog server set "{dns_name}" | sets address of syslog server | |
| syslog server show | shows address of syslog server | |
| system | enters cmd group "system" | |
| system beeper manual set {OFF=0 ON=1}{millisec} | manually sets beeper with optional duration | |
| system beeper manual show | shows beeper state | |
| system restart | restarts device | |
| system fabsettings | restore fab settings and restart device | |
| system bootloader | enters bootloader mode | |
| system flushdns | flush DNS cache | |
| system uptime | number of seconds the device is running | |
| system name show | shows device name | |
| system version show | shows actual firmware version | |
| system display {disp_num} default extsensor {port_num} {sen_type} set {sen_field} | shows external sensor | |
| system display {disp_num} default set {BLANK=0,LOCAL_TIME=1,UTC_TIME=2} | shows other contents | |
| system display {disp_num} default show | shows default setting for display | |
| system display default hash set "{data}" | sets hashed display setting | |
| system display default hash show | shows hashed display setting | |
| system sensor {VSYS=0 VAUX=1 VMAIN=2 TCPU=3} show | shows internal sensors if model supports it | |
| system {SWITCH_PORT=0} events set {OFF=0 ON=1} | enable global events | |
| system {SWITCH_PORT=0} events show | shows if global events enabled | |
| system {SWITCH_PORT=0} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5,EVT_DISPLAY=6,EVT_CONSOLE=7,EVT_MQTT=8}" | enables different event types | |
| system {SWITCH_PORT=0} events type show | shows what event types are enabled | |
| system {SWITCH_PORT=0} events mqtt retain set {OFF=0 ON=1} | sets mqtt retain | |
| system {SWITCH_PORT=0} events mqtt retain show | shows if mqtt retain set | |
| system display input mode set "{DISP_ALT=0 DISP_PORT=1 DISP_INPUT=2}" | sets ports, inputs or alternating on display | |
| system display input mode show | what is shown on display | |
| system display input delay set "{num_secs}" | sets time for alternating on display | |
| system display input delay show | shows display alternating time | |
| system panel enabled set {OFF=0 ON=1} | blocks panel buttons when not enabled | |
| system panel enabled show | shows if panel buttons are enabled | |
| system panel port all set {OFF=0 ON=1} | enable switch all relays from panel buttons | |

Specifications

| | |
|--|---|
| system panel port all show | show s if siw tch all relays from panel buttons enabled |
| timer | enters cmd group "timer" |
| timer enabled set {OFF=0 ON=1} | enables timer functions |
| timer enabled show | show s if timer a enabled |
| timer syslog facility set {0..23} | sets facility level for timer syslog |
| timer syslog facility show | show s facility level for timer syslog |
| timer syslog verbose set {0..7} | sets verbose level for timer syslog |
| timer syslog verbose show | show s verbose level for timer syslog |
| timer {rule_num} enabled set {OFF=0 ON=1} | enables rule |
| timer {rule_num} enabled show | show s if rule is enabled |
| timer {rule_num} name set "{name}" | sets name of rule |
| timer {rule_num} name show | show s name of rule |
| timer {rule_num} {FROM=0 UNTIL=1} set "{yyyy-mm-dd}" | sets date range of rule |
| timer {rule_num} {FROM=0 UNTIL=1} show | show s date range of rule |
| timer {rule_num} trigger jitter set {0..65535} | sets jitter for rule |
| timer {rule_num} trigger jitter show | show jitter of rule |
| timer {rule_num} trigger random set {0..100} | sets probability for rule |
| timer {rule_num} trigger random show | show s rule probability |
| timer {rule_num} trigger {HOUR=0 MIN=1 SEC=2 DAY=3 MON=4 DOW=5} set "{time_date_list}" | sets time date list |
| timer {rule_num} trigger {HOUR=0 MIN=1 SEC=2 DAY=3 MON=4 DOW=5} show | show s time date list |
| timer {rule_num} action mode set {SWITCH=1 CLI=2} | sets sw itch or cli cmd |
| timer {rule_num} action mode show | show s if sw itch or cli cmd |
| timer {rule_num} action {SWITCH1=0 SWITCH2=1}{OFF=0 ON=1} set "{port_list}" | sets port list for sw itch cmd |
| timer {rule_num} action {SWITCH1=0 SWITCH2=1}{OFF=0 ON=1} show | show s port list for sw itch cmd |
| timer {rule_num} action delay set {0..65535} | delay betw een cmds |
| timer {rule_num} action delay show | show s delay betw een cmds |
| timer {rule_num} action console set "{cmd}" | sets cmd string |
| timer {rule_num} action console show | show s cmd string |
| timer {rule_num} action hash set "{data}" | sets action binary form |
| timer {rule_num} action hash show | show s action binary form |
| timer {rule_num} delete | delete one timer |
| timer delete all | delete all timer |
| vt100 | enters cmd group "vt100" |
| vt100 echo set {OFF=0 ON=1} | sets console echo state |
| vt100 echo show | show s console echo state |
| vt100 numeric set {OFF=0 ON=1} | sets numeric mode |
| vt100 numeric show | show s numeric mode state |
| vt100 reset | resets terminal |

Notes

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

External Sensor Type Table "{sen_type}"

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

| Index | Description | Products |
|-------|-------------------------------------|------------------------|
| 0 | Temperature | 7001, 7101, 7201 |
| 0 | Temperature | 7004, 7104, 7204, 7208 |
| 1 | Temperature, Humidity | 7002, 7102, 7202 |
| 1 | Temperature, Humidity | 7005, 7105, 7205, 7209 |
| 2 | Temperature, Humidity, Air Pressure | 7006, 7106, 7206, 7210 |

External Sensor Field Table "{sen_field}"

| Index | Description | Unit |
|-------|----------------------------------|------|
| 0 | Temperature | °C |
| 1 | Humidity | % |
| 3 | Air Pressure | hPa |
| 4 | Dew Point | °C |
| 5 | Dew Point Temperature Difference | °C |

4.3 HTTP Authentication

In the past, only *HTTP Basic Access Authentication* was supported as password authentication for Gude devices. Now cookie-based *Session Authentication* is used by default. This has the following advantages:


- Clicking on the "Logout" tab now mandatorily results in having to provide user name and password again to get into the device. This is often not the case with Basic Access Authentication because it is under the control of the web browser.
- Session Authentication is less susceptible to cross-site scripting. In addition, enhanced security can be configured by using a CSRF-Token.
- Combined with Session Authentication is a configurable logout time, where the login page is automatically referred to after inactivity.

Configuration of the Session Authentication

Session Timeout (admin): (seconds)
Session Timeout (user): (seconds)
Select Authentication Mode:

You can select the automatic logout times in case of inactivity and the Session Authentication mode in the Ethernet configuration (sub-selection HTTP Server). If the logout time is zero, there is no automatic logout. The authentication modes are:


1. Basic Compatible: Basic Access and Session Authentication are accepted.
2. Session: Only Session Authentication is allowed.
3. Session Extended: A CSRF-Token token is required in addition to Session Authentication.

 Session and Session Extended modes behave slightly differently in the web interface: If you open a new browser tab for a running session in Session mode, no new login

is required. In Session Extended mode, if a new tab is opened, the user name and password must be re-entered. This is because the CSRF-Token is stored locally to the tab in the web browser.

Compatibility with previous Basic Accesses

- In Basic Compatible mode, normal accesses with Basic Access Authentication are possible. Also everything may be accessed with a HTTP GET request. This leads to compatibility with controllers and drivers already on the market that communicate with Gude devices.
- If not accessed with Basic Access Authentication but with Session Authentication, CGI queries with passwords, configuring the device and switching relays are no longer allowed with HTTP GET requests. A POST request must be used.

 If you have logged in to the web interface once with Session Authentication, the system will automatically try to work with Session Authentication. If you want to use Basic Access Authentication, you must first delete the session cookies and then access a page that is not the login page.

Authentication examples

To demonstrate how scripts can perform the different authentication modes, here are command line examples using curl:

Basic Access Authentication

```
curl -u "admin:test" "192.168.0.10/status.json?components=16"
```


Session Authentication with Cookies

```
curl --cookie-jar sess_cook_curl.txt -d "username=admin&password=test" \
  192.168.0.10/login.json
curl --cookie sess_cook_curl.txt 192.168.0.10/status.json?components=16
```

Session authentication with cookies and CSRF-Token

```
curl --cookie-jar sess_cook_curl.txt -d "username=admin&password=test" \
  192.168.0.10/login.json
brings a JSON output like: {"login":1,"sessionidX":"a4b9cfc54b273b2af3ba84b8f413b6e9","user_id":1,"href":"dashboard.html"}

curl --cookie sess_cook_curl.txt -d "components=16&cmd=1&p=1&s=0" -H \
  "sessionidX: a4b9cfc54b273b2af3ba84b8f413b6e9" 192.168.0.10/status.json
```

 In this example, the CSRF-Token sessionidX from the output of the first curl call was added as an additional header in the second curl call.


4.4 IP ACL

IP Access Control List

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

Examples:

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

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

4.5 IPv6

IPv6 Addresses

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

Address Notation

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

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

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

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

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

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

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

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

4.6 Messages

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

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

E-Mail messages

Email messages are triggered by the following events:

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

SNMP Traps

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

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

Syslog messages

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

- Turning on the device
- Enable/disable of syslog in the configuration
- Switching of the Ports
- Exceeding of the max / min values of attached sensors
- State change of digital sensor input ports

| | SNMP Trap | Console | MQTT | Syslog | Email |
|----------------------|-----------|---------|------|--------|-------|
| Global | | | | | |
| Device started | x | x | x | x | x |
| Switch port | x | x | x | x | x |
| Port watchdog status | x | x | x | x | x |

| | | | | | |
|-----------------------------|---|---|---|---|---|
| Syslog switched on/off | | | | x | |
| MQTT connection established | | | x | x | |
| MQTT connection lost | | | | x | |
| Value-Threshold | | | | | |
| external sensors | | | | | |
| Signal inputs | x | x | x | x | x |
| Time-Interval | | | | | |
| external sensors | | | | | |
| Signal inputs | | x | x | | |
| Value-Delta | | | | | |
| external sensors | | | | | |
| Signal inputs | | x | x | | |

SNMP traps

There are common traps for state changes of the same device resource. For example, a SwitchEvtPort trap is sent when a port is turned on or off. The state change itself is conveyed by the supplied data within the trap.

MQTT published data

Messages on the MQTT channel are sent in JSON format.

Example switch a port: `{"type": "portswitch", "idx": 2, "port": "2", "state": 1, "cause": {"id": 2, "txt": "http"}, "ts": 1632}`

Console Push Messages

Push messages can be activated on the console channels (Telnet, SSH or serial console), which output sensor values at timed intervals (every n seconds) or as of a configurable change in the magnitude of the sensor value on that channel. The generated message always starts with a "#" and ends with a CR/LF.

Example: Switch a port: `#port 2 ON`

If you open a telnet or SSH connection, the push messages are either preconfigured, or you switch on the push messages temporarily with `console telnet pushmsgs set 1` (or `console ssh pushmsgs set 1`). From now on, push messages will be sent asynchronously on this channel. The asynchronous nature of the messages can cause problems on a connection if you send commands yourself at the same time. There are then the possibilities:


- Filter all incoming characters between "#" and CR/LF
- or open a second channel (Telnet, SSH, serial) and switch on the push messages there.

4.7 Modbus TCP

 **Important:** All calculations in this chapter are based on addresses starting at "0".

Specifications


For some Modbus TCP Utilities, however, the addresses start at 1, in which case a 1 must be added to the addresses in this chapter. Please try both possibilities for tests!

 **Important:** If an attempt is made to access registers that do not exist for the respective device, then an access error will occur. If a device has e.g. 8 relays, then only the first eight coils can be accessed without error!

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

Address range overview:

| Device Resource | Start | End | Modbus Data Type |
|--------------------------|--------|--------|-------------------|
| Power/Output/eFuse Ports | 0x000 | 0x3ff | Coils |
| DC Inputs | 0x400 | 0x7ff | Discrete Inputs |
| Stop Condition active | 0x800 | 0x800 | Discrete Inputs |
| POE active | 0x801 | 0x801 | Discrete Inputs |
| Status Power Sources | 0x1000 | 0x100f | Discrete Inputs |
| OVP active (Line-Ins) | 0x1010 | 0x101f | Discrete Inputs |
| Fuse ok | 0x1020 | 0x102f | Discrete Inputs |
| ETS Input Power nominal | 0x1030 | 0x1031 | Discrete Inputs |
| eFuse Errors | 0x1100 | 0x11ff | Discrete Inputs |
| Info Area | 0x000 | 0x005 | Input Registers |
| CPU Sensor values | 0x080 | 0x083 | Input Registers |
| External Sensors | 0x100 | 0x1ff | Input Registers |
| Fan Level | 0x200 | 0x20f | Input Registers |
| Line Energy Sensors | 0x400 | 0x39ff | Input Registers |
| Port Energy Sensors | 0x3a00 | 0x81ff | Input Registers |
| Bank Energy Sensors | 0x8200 | 0x823f | Input Registers |
| Power Source Sensors | 0x8240 | 0x827f | Input Registers |
| Residual Current Monitor | 0x8280 | 0x82cf | Input Registers |
| Bank Power Source Select | 0x000 | 0x00f | Holding Registers |
| Fan Mode | 0x010 | 0x01f | Holding Registers |

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

The Unit-ID is ignored because the device is uniquely identified by its IP address.

Supported Modbus TCP Functions

| Function | Request Code |
|------------------------|--------------|
| Read Coils | 0x01 |
| Read Discrete Inputs | 0x02 |
| Write Single Coil | 0x05 |
| Write Multiple Coils | 0x0f |
| Read Input Registers | 0x04 |
| Read Holding Registers | 0x03 |
| Write Holding Register | 0x06 |

Specifications

| | |
|----------------------------------|-------------|
| Write Multiple Holding Registers | 0x10 |
| Read Device Identification | 0x2B / 0x0E |

Coils

| Device Resource | Start | End | Device Function |
|--------------------|-------|-------|----------------------------|
| Power/Output/eFuse | 0x000 | 0x3ff | Coil represents Port State |

Discrete Inputs

| Device Resource | Start | End | Function when set |
|------------------------|--------|--------|----------------------------|
| DC Inputs | 0x400 | 0x7ff | Input logically 1 |
| Stop Condition active | 0x800 | 0x800 | Stop Input active |
| POE active | 0x801 | 0x801 | POE active |
| Status Power Sources | 0x1000 | 0x100f | Power Source active |
| OVP active (Line-Ins) | 0x1010 | 0x101f | OVP active |
| Fuse ok | 0x1020 | 0x1020 | Fuse functional (ETS 8801) |
| ETS Input Power normal | 0x1030 | 0x1031 | Voltage nominal (ETS 8801) |
| eFuse Error | 0x1100 | 0x11ff | eFuse Error (EPC 8291) |

DC Inputs:

The DC inputs can be found in the *Discrete Inputs*. The inputs are arranged as follows:

Input: $0x0400 + \text{Port} * 0x40 + \text{Input-number}$ (starts with zero).

Port is the number of the external sensor port. For inputs permanently installed in the device, Port = 0.

Example for the first input at external input sensor in port 2: $0x400 + 2 * 0x40 + 0 = 0x480$

Status Power Sources:

| Power Sources | Offset |
|-----------------|--------------------------------|
| EPC 8221 / 8226 | 0 = Bank A, 1 = Bank B |
| ENC 2111 / 2191 | 0 = Pwr1, 1 = Pwr2 |
| ESB 7213 / 7214 | 0 = Pwr1, 1 = Pwr2 (only 7214) |

Input Registers

| Device Resource | Start | End | Function |
|-------------------|-------|-------|-----------|
| Info Bereich | 0x000 | 0x005 | see table |
| CPU Sensor values | 0x080 | 0x083 | see table |
| Externe Sensoren | 0x100 | 0x1ff | see table |

Specifications

| | | | |
|--------------------------|--------|--------|-------------------------|
| Fan Level | 0x200 | 0x20f | 0 (aus) bis 3 (maximal) |
| Line Energy Sensors | 0x400 | 0x39ff | see table |
| Port Energy Sensors | 0x3a00 | 0x81ff | see table |
| Bank Energy Sensors | 0x8200 | 0x823f | see table |
| Power Source Sensors | 0x8240 | 0x827f | see table |
| Residual Current Monitor | 0x8280 | 0x82cf | see table |

Info Area

| Address | Width | Information |
|---------|--------|---|
| 0 | 16-bit | Number of Ports (Relay) |
| 1 | 16-bit | Number of Ports (Outlets) with Energy Measurement |
| 2 | 16-bit | Number of Banks |
| 3 | 16-bit | Number of Line-In |
| 4 | 16-bit | Phases per line |
| 5 | 16-bit | Number of Inputs |

Sensor Type Description

| Address | Width | Information |
|------------------|-----------------|-----------------------------|
| 0x080 to 0x083 | 16-bit (signed) | CPU Sensor values |
| 0x100 to 0x1ff | 16-bit (signed) | external Sensors |
| 0x400 to 0x39ff | 32-bit (signed) | Line Energy Sensors |
| 0x3a00 to 0x81ff | 32-bit (signed) | Port Energy Sensors |
| 0x8200 to 0x823f | 16-bit (signed) | Bank Energy Sensors |
| 0x8240 to 0x827f | 16-bit (signed) | Power Source Energy Sensors |
| 0x8280 to 0x82cf | 16-bit (signed) | Residual Current Monitor |


CPU Sensor Values

| Offset | Sensor Field | Unit |
|--------|-----------------|--------|
| 0 | Vsystem | 0.01 V |
| 1 | Vaux | 0.01 V |
| 2 | Vmain | 0.01 V |
| 3 | CPU Temperature | 0.1 °C |

External Sensors:

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

$$0x100 + \text{Port} * 8 + \text{Offset}$$

 In the Expert Sensor Box 7213 / 7214 the internal sensor corresponds to the value Port = 0, and is coded Port = 1 for Sensor 2 and Port = 2 for Sensor 3.


| Offset | Sensor Field | Unit |
|--------|--------------|------|
|--------|--------------|------|

Specifications

| | | |
|---|----------------------|------------------|
| 0 | Temperature | 0.1 °C |
| 1 | Humidity | 0.1 % |
| 2 | Digital Input | bool |
| 3 | Air Pressure | 1 hPa (millibar) |
| 4 | Dew Point | 0.1 °C |
| 5 | Dew Point Difference | 0.1 °C |

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


Energy Sensors:

 This applies to devices that support 230V input measurement (Line) and/or devices that support 230V output measurement (Port).

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: $0x0400 + \text{Line} * 0x120 + \text{Phase} * 0x60 + \text{Offset} * 2$

Port: $0x3a00 + \text{Port} * 0x120 + \text{Phase} * 0x60 + \text{Offset} * 2$

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

Examples:

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


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

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

| Offset | Sensor Field | Unit |
|--------|-------------------------------------|------------|
| 0 | Absolute Active Energy | Wh |
| 1 | Power Active | W |
| 2 | Voltage | V |
| 3 | Current | mA |
| 4 | Frequency | 0.01 hz |
| 5 | Power Factor | 0.001 |
| 6 | Power Angle | 0.1 degree |
| 7 | Power Apparent | VA |
| 8 | Power Reactive | VAR |
| 9 | Absolute Active Energy Resettable | Wh |
| 10 | Absolute Reactive Energy | VARh |
| 11 | Absolute Reactive Energy Resettable | VARh |

Specifications

| | | |
|----|---|--------|
| 12 | Reset Time - sec. since last Energy Counter Reset | s |
| 13 | Forward Active Energy | Wh |
| 14 | Forward Reactive Energy | VARh |
| 15 | Forward Active Energy Resettable | Wh |
| 16 | Forward Reactive Energy Resettable | VARh |
| 17 | Reverse Active Energy | Wh |
| 18 | Reverse Reactive Energy | VARh |
| 19 | Reverse Active Energy Resettable | Wh |
| 20 | Reverse Reactive Energy Resettable | VARh |
| 21 | Residual Current Type A | 0.1 mA |
| 22 | Neutral Current | 0.1 mA |

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

DC Energy Sensors:

With the EPC 8291 / 8290 devices, the voltage and current of the individual banks and voltage sources can be read out. The measured values of the energy sensors are returned as signed 16-bit integers. The following formulas are available for the address (the values for Bank and PowerSrc start at zero):

Bank: $0x8200 + \text{Bank} * 2 + \text{Offset}$

Power Source: $0x8240 + \text{PowerSrc} * 2 + \text{Offset}$

Examples:

"Voltage" at third bank: $0x8200 + 2 * 2 + 0 = 0x8204$

"Current" at first PowerSrc: $0x8240 + 0 * 2 + 1 = 0x8241$

| Offset | Sensor Field | Unit |
|--------|--------------|--------|
| 0 | Voltage | 0.01 V |
| 1 | Current | mA |

Residual Current Monitor Type B (RCMB):

Devices with a Residual Current Monitor Type B (RCMB) module separately measure the RMS and DC fault current components of the input supply. The values are returned as signed 16-bit integers. The following formulas are used for the address (the module number starts at zero):

Bank: $0x8280 + \text{ModuleNo} * 8 + \text{Offset}$.


Examples:

"Residual Current DC" at first module: $0x8280 + 0 * 8 + 1 = 0x8281$.

"Output DC" for second module: $0x8280 + 1 * 8 + 3 = 0x828b$


Specifications

| Offset | Addr. Module 0 | Sensor Field | Unit |
|--------|----------------|-----------------------------|--------|
| 0 | 0x8280 | Residual Current RMS Type B | 0.1 mA |
| 1 | 0x8281 | Residual Current DC Type B | 0.1 mA |
| 2 | 0x8282 | Output RMS | bool |
| 3 | 0x8283 | Output DC | bool |
| 4 | 0x8284 | Module State | |

 Whether a Residual Current Monitor Type B (RCMB) module is present depends on the particular device model.

Holding Registers

| Device Resource | Start | End | Function |
|-------------------|-------|-------|-----------------------------|
| Bank Power Source | 0x000 | 0x00f | Sets Power Source for Bank |
| Fan Mode | 0x010 | 0x01f | 0 = Automatic / 1 = Maximum |

 Bank Power Source applies to EPC 8291 and ETS 8801 models. Only the EPC 8291 model has a fan.


Device Identification

Returns manufacturer name and device identification:

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

| | | |
|-------------------|----------|-------------------|
| Response Code | 1 Byte | 0x2b |
| MEI Type | 1 Byte | 0x0e |
| Read Dev ID code | 1 Byte | 0x01 |
| Conformity Level | 1 Byte | 0x01 |
| More Follows | 1 Byte | 0x00 |
| NextObjectID | 1 Byte | 0x00 |
| Number of Objects | 1 Byte | 0x03 |
| Object ID | 1 Byte | 0x00 |
| Object Length | 1 Byte | n1 |
| Object Value | n1 Bytes | "Company Id" |
| Object ID | 1 Byte | 0x00 |
| Object Length | 1 Byte | n2 |
| Object Value | n2 Bytes | "Product Id" |
| Object ID | 1 Byte | 0x00 |
| Object Length | 1 Byte | n3 |
| Object Value | n3 Bytes | "Product Version" |

4.7.1 Sensor Tables

 **Important:** All calculations in this chapter are based on addresses starting at "0". With some Modbus TCP utilities the addresses start at 1. In this case a 1 must be added to the addresses in this chapter. Please try both possibilities for tests!

External sensors addresses (Input Register)

| Sensor field | Port 1 |
|----------------------|--------|
| Temperature | 0x100 |
| Humidity | 0x101 |
| Digital input | 0x102 |
| Air Pressure | 0x103 |
| Dew Point | 0x104 |
| Dew Point Difference | 0x105 |

A value of 0x8000 means that no sensor is plugged into the corresponding port or the corresponding field in the sensor is not available.

4.8 MQTT

This device supports MQTT 3.1.1 to send configured messages and also to receive commands. This chapter is general for all Gude devices, some Gude models do not have switchable ports.

- Default port for an unencrypted connection is port 1883.
- Default port for a TLS secured connection is port 8883.
- If the broker allows anonymous login, username and password are arbitrary, but a username must be specified.
- If multiple MQTT clients are connected to a broker, the names of the clients must be different. For this reason, "client_xxxx" is generated as the default name. Here "xxxx" are the last 4 digits of the MAC address.

Message format

The MQTT messages of the device are always sent in JSON format. E.G..

```
{"type": "portswitch", "idx": 2, "port": "2", "state": 1, "cause": {"id": 2, "txt": "http"}, "ts": 1632}
```

This is a switching of the second port to the state on. The source of the switching command is CGI ("http"). The index is always numeric, "port" can also be alphanumeric for devices with multiple banks, e.g. "A2". At the end follows a timestamp ("ts"), which indicates the number of seconds the device is on, or unixtime if the device has synchronized with an NTP server.

MQTT Topic Prefix


The topic prefix for the messages can be set in the MQTT configuration. A default would

be e.g. "de/gudesystems/epc/[mac]". Here "[mac]" is a placeholder for the MAC address of the device, another possible placeholder is "[host]", which contains the host name. An example topic for a switching message of the second port would then be:

```
"de/gudesystems/epc/00:19:32:01:16:41/switch/2".
```

Executing console commands


The device can be controlled remotely via MQTT using console commands. A list of all commands can be found in the [Console](#) chapter. Depending on the topic, the commands are accepted in different formats.

 As default the execution of commands is not allowed, but must be enabled in the MQTT configuration! ("Permit CLI commands")

Format 1: Command in JSON Syntax

```
Publish Topic: "de/gudesystems/epc/00:19:32:01:16:41/cmd"  
Publish Message: "{\"type\": \"cli\", \"cmd\": \"port 2 state set 1\", \"id\": 10}"
```

```
Response from device to "de/gudesystems/epc/00:19:32:01:16:41/cmdres"  
"{\"type\": \"cli\", \"cmdres\": [\"OK.\"], \"result\": {\"num\": 0, \"hint\": \"ok\"}, \"id\": 10}"
```

 The JSON object "result" returns whether the command was valid. The object "id" in the command is optional and is passed through in the response from the device. The passed number can help to establish a synchronicity between command and response via the broker.

Format 2: Raw Text


```
Publish Topic: "de/gudesystems/epc/00:19:32:01:16:41/cmd/cli"  
Publish Message: "port 2 state set 1".
```

```
Response from device to "de/gudesystems/epc/00:19:32:01:16:41/cmdres/cli"  
"OK."
```

Format 3: Simplified port switching

```
Publish Topic: "de/gudesystems/epc/00:19:32:01:16:41/cmd/port/2"  
Publish Message: "0" or "1".
```

```
Response from device to "de/gudesystems/epc/00:19:32:01:16:41/cmdres/port/2"  
"0" or "1"
```

 This special form exists only for the port switching commands.

Device Data Summary

In the **Device Data Summary** the most important data of the device are summarized in a JSON object and sent periodically in a configurable time interval. This summary depends on the properties of the device and the connected sensors, and could look like this:

Topic: en/gudesystems/epc/00:19:32:01:16:41/device/telemetry

Message:

```
{
  "type": "telemetry",
  "portstates": [{
    "port": "1",
    "name": "Power Port",
    "state": 1
  }, {
    "port": "2",
    "name": "Power Port",
    "state": 0
  }, {
    "port": "3",
    "name": "Power Port",
    "state": 0
  }, {
    "port": "4",
    "name": "Power Port",
    "state": 0
  }],
  "line_in": [{
    "voltage": 242.48,
    "current": 0.000
  }],
  "sensors": [{
    "idx": 1,
    "name": "7105",
    "data": [{
      "field": "temperature",
      "v": 21.1,
      "unit": "deg C"
    }, {
      "field": "humidity",
      "v": 71.9,
      "unit": "%"
    }, {
      "field": "dew_point",
      "v": 15.8,
      "unit": "deg C"
    }, {
      "field": "dew_diff",
      "v": 5.3,
      "unit": "deg C"
    }
  ]
}],
  "ts": 210520
}
```

4.8.1 Example HiveMQ

What does an MQTT configuration look like using HiveMQ as an example?

Specifications

Cluster Details [Back to clusters](#)

Overview **Access Management** Getting started

Details

Hostname:

Port (TLS): 8883

Port (Websocket + TLS): 8884

Create a free or commercial account at www.hivemq.com and create a new cluster.

Active MQTT Credentials

These credentials give access to publish and subscribe to your HiveMQ Cloud cluster.

| Username | Password | Actions |
|---------------------------------------|--|----------------------------------|
| <input type="text" value="epc-user"/> | <input type="password" value="*****"/> | <input type="button" value="x"/> |

In the "Manage Clusters" section, go to "Access Management" and add an MQTT user with name and password.

MQTT

Enable MQTT: yes no

Broker:

TLS: yes no

TCP Port: (Default: 8883)

Username:

Set new password:

Repeat password:

Client ID:

Quality of Service (QoS): ▾

Keep-alive ping interval: s (minimum 10s)

Topic Prefix:
de/gudesystems/epc/00:19:32:01:16:41

Permit CLI commands: yes no

Publish device data summary interval: s (0=disabled)

In the MQTT configuration of the Gude device, transfer the hostname of the HiveMQ broker, as well as username and password. Additionally activate TLS and set the correct port.

4.9 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. Please set this value to 300 seconds or greater to prevent the radius requests from becoming too large.

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.

4.10 SNMP

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

- GET
- GETNEXT
- GETBULK
- SET

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

MIB Tables

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

SNMP v1 and v2c


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

SNMP v3

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


Authentication

The algorithms "HMAC-MD5-96" and "HMAC-SHA-96" are available for authentication. In addition, the "HMAC-SHA-2" variants (RFC7630) "SHA-256", "SHA-384" and "SHA-512" are implemented.

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

Encryption

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

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

Passwords

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


Security

The following aspects should be considered:

- If encryption or authentication is used, then SNMP v1 and v2c should be turned off. Otherwise the device could be accessed with it.

- If only authentication is used, then the new "HMAC-SHA-2" methods are superior to the MD5 or SHA-1 hashing algorithms. Since only SHA-256 is accelerated in hardware, and SHA-384 and SHA-512 are calculated purely in software, one should normally select SHA-256. From a cryptographic point of view, the security of SHA-256 is sufficient for today's usage.
- For SHA-1, there are a little less attack scenarios than MD5. If in doubt, SHA-1 is preferable.
- Encryption "DES" is considered very unsafe, use only in an emergency for reasons of compatibility!
- For cryptologists it's a debatable point whether "HMAC-MD5-96" and "HMAC-SHA-96" can muster enough entropy for key lengths of "AES-192" or "AES-256".
- From the foregoing considerations, we would recommend at present "HMAC-SHA-96" with "AES-128" as authentication and encryption method.

Change in Trap Design

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

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

NET-SNMP

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

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

or


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

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

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

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

NET-SNMP Examples

 These examples refer to Gude devices that have switchable ports.

Query Power Port 1 switching state:

Specifications

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

4.10.1 Device MIB 2304

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 "1.3.6.1.4.1.28507.101.1.1.1.1". A distinction is made in SNMP OID 's in between tables and scalars. OID scalar have the extension ".0" and only specify a value. In SNMP tables the "x" is replaced by an index (1 or greater) to address a value from the table.

| Name | Description | OID | Type | Acc. |
|--------------------------|--|---------------------|------------|------|
| enc2304TrapCtrl | 0 = off 1 = Ver. 1 2 = Ver. 2c 3 = Ver. 3 | .101.1.1.1.1.0 | Integer32 | RW |
| enc2304TrapIPIndex | A unique value, greater than zero, for each receiver slot. | .101.1.1.1.2.1.1.x | Integer32 | RO |
| enc2304TrapAddr | DNS name or IP address specifying one Trap receiver slot. A port can optionally be specified: 'name:port' An empty string disables this slot. | .101.1.1.1.2.1.2.x | OCTETS | RW |
| enc2304portNumber | The number of Relay Ports | .101.1.3.1.1.0 | Integer32 | RO |
| enc2304PortIndex | A unique value, greater than zero, for each Relay Port. | .101.1.3.1.2.1.1.x | Integer32 | RO |
| enc2304PortName | A textual string containing name of a Relay Port. | .101.1.3.1.2.1.2.x | OCTETS | RW |
| enc2304PortState | current state a Relay Port | .101.1.3.1.2.1.3.x | INTEGER | RW |
| enc2304PortSwitchCount | 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. | .101.1.3.1.2.1.4.x | Integer32 | RO |
| enc2304PortStartupMode | set Mode of startup sequence (off, on , remember last state) | .101.1.3.1.2.1.5.x | INTEGER | RW |
| enc2304PortStartupDelay | Delay in sec for startup action | .101.1.3.1.2.1.6.x | Integer32 | RW |
| enc2304PortRepowerTime | Delay in sec for repower port after switching off | .101.1.3.1.2.1.7.x | Integer32 | RW |
| enc2304PortResetDuration | Delay in sec for turning Port on again after Reset action | .101.1.3.1.2.1.8.x | Integer32 | RW |
| enc2304Buzzer | turn Buzzer on and off | .101.1.3.10.0 | Integer32 | RW |
| enc2304ActiveInputs | Number of supported Input Channels. | .101.1.5.6.1.0 | Unsigned32 | RO |
| enc2304InputIndex | None | .101.1.5.6.2.1.1.x | Integer32 | RO |
| enc2304Input | Input state of device | .101.1.5.6.2.1.2.x | INTEGER | RO |
| enc2304InputName | A textual string containing name of the Input | .101.1.5.6.2.1.32.x | OCTETS | RW |
| enc2304CPUSensorVsystem | System Voltage on CPU Board | .101.1.5.14.1.0 | Gauge32 | RO |
| enc2304CPUSensorVaux | Auxiliary Voltage on CPU Board | .101.1.5.14.2.0 | Gauge32 | RO |

| | | | | |
|------------------------------|---|---------------------|------------|----|
| enc2304CPUSensorVmain | | .101.1.5.14.3.0 | Gauge32 | RO |
| | Main Voltage on CPU Board | | | |
| enc2304CPUSensorTcpu | | .101.1.5.14.4.0 | Integer32 | RO |
| | Temperature on CPU Board | | | |
| enc2304NTPTimeValid | | .101.1.5.15.1.0 | INTEGER | RO |
| | Show if valid Time is received | | | |
| enc2304NTPUnixTime | | .101.1.5.15.2.0 | Unsigned32 | RO |
| | show received NTP time as unixtime (secs since 1 January 1970) | | | |
| enc2304NTPLastValidTimestamp | | .101.1.5.15.3.0 | Unsigned32 | RO |
| | show seconds since last valid NTP timestamp received | | | |
| enc2304SensorIndex | | .101.1.6.1.1.1.x | Integer32 | RO |
| | None | | | |
| enc2304TempSensor | | .101.1.6.1.1.2.x | Integer32 | RO |
| | actual temperature | | | |
| enc2304HygroSensor | | .101.1.6.1.1.3.x | Integer32 | RO |
| | actual humidity | | | |
| enc2304AirPressure | | .101.1.6.1.1.5.x | Integer32 | RO |
| | actual air pressure | | | |
| enc2304Dew Point | | .101.1.6.1.1.6.x | Integer32 | RO |
| | dew point for actual temperature and humidity | | | |
| enc2304Dew PointDiff | | .101.1.6.1.1.7.x | Integer32 | RO |
| | difference between dew point and actual temperature (Temp - Dew Point) | | | |
| enc2304ExtSensorName | | .101.1.6.1.1.32.x | OCTETS | RW |
| | A textual string containing name of a external Sensor | | | |
| enc2304ExtActiveInputs | | .101.1.6.2.1.0 | Unsigned32 | RO |
| | Number of supported Input Channels. | | | |
| enc2304ExtInputIndex | | .101.1.6.2.2.1.1.x | Unsigned32 | RO |
| | None | | | |
| enc2304ExtInput | | .101.1.6.2.2.1.2.x | INTEGER | RO |
| | Input state of device | | | |
| enc2304ExtInputName | | .101.1.6.2.2.1.32.x | OCTETS | RW |
| | A textual string containing name of the Input | | | |
| enc2304ExtInputPortNum | | .101.1.6.2.2.1.33.x | Integer32 | RO |
| | Number of external Sensor Port when value greater zero, else device built-in Input. | | | |
| enc2304ExtInputBlockIndex | | .101.1.6.2.2.1.34.x | Integer32 | RO |
| | Either index of device built-in Input, or index of Input in external sensor. | | | |

4.11 SSL

TLS Standard

The device is compatible with TLS v1.1 to TLS v1.3 standards, but due to lack of security, SSL v3.0, TLS 1.0, and RC4, MD5, SHA1, and DES encryption are disabled. All ciphers use Diffie-Hellman key exchange (Perfect Forward Secrecy).

Creating your own Certificates

The SSL stack is supplied with a specially newly generated self-signed 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 (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 created with "openssl genrsa". The Gude device processes keys in the traditional PKCS#1 format. This can be recognized by the fact that the generated key file starts with "-----BEGIN RSA PRIVATE KEY-----". If the file starts with "-----BEGIN PRIVATE KEY-----", the file is in PKCS#8 format and the key is not recognized. If you have only a key in PKCS#8 format, you can convert it to PKCS#1 with openssl: "**openssl rsa -in pkcs8.key -out pkcs1.key**".

ECC Certificate with Sign Request:

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

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


Linux:

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


Windows:

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

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

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

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

 An uploaded certificate will be preserved, when a device is put back to factory defaults^[24].

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.

Support

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.
- Configure HTTP Extended Session Authentication.
- Allow access to HTTP via SSL (TLS) only.
- Use TLS 1.3 if possible and avoid TLS 1.1.
- Enable authentication and encryption in SNMPv3 and disable SNMP v2 access.
- Enable STARTTLS or SSL in the e-mail configuration.
- Archive configuration files securely, they contain sensitive information.
- In the IP ACL, enter only the devices that require access to HTTP or SNMP.
- Use SSH if possible, since Telnet is not encrypted.
- Set login for telnet or serial console.
- Use MQTT 3.1.1 only with TLS and password.
- Only permit MQTT CLI commands when the broker is trustworthy.
- 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 HTTP Performance

Access to the Gude devices via the REST API can normally be conducted from one source every second with HTTP. If accessed from multiple sources simultaneously, it is recommended to adjust the poll interval accordingly.

SSL (TLS) performance

The initial setup for an SSL (TLS) connection results in numerous crypto operations at the start of the connection. If an RSA 2048 certificate is used, the delay at the beginning is about 2-3 seconds, with RSA 4096 the connection establishment can take up to 10 seconds. The delays result from a limitation of the math unit in the embedded CPU. We therefore recommend an ECC 256 certificate, which is significantly more performant to calculate. Previously established connections TLS connections are stored in a TLS Session Cache (or Session Tickets). However, this cache is not always supported by

browsers, or it expires after only a short time. Especially browsers (HTTPS clients) of other embedded devices (e.g. media controllers) may be limited in the TLS cache.

A remedy for this can be an HTTP keep-alive connection. Once a connection with HTTP keep-alive is opened, it is closed again after 10 seconds if no data is transferred. If you want to receive data periodically, it is therefore recommended to request the data at intervals of less than 10 seconds (e.g. every 5-8 seconds) after establishing the connection with HTTP keep-alive.

Special TLS 1.3 performance problem with Chrome (MS Edge)

When TLS 1.3 and insecure certificates are used in combination with a web browser with Chromium engine (Google Chrome or MS Edge), performance may be affected, resulting in longer loading times. In this constellation, the Chromium Engine does not correctly support the TLS Session Cache (or Session Tickets) and the math unit of the embedded CPU may be overwhelmed with persistent RSA operations. Possible solutions:

- Use secure certificates (official certificate authority or marked as secure in the OS)
- or keep-alive with poll interval less than 10 seconds
- or use of Firefox browser
- or use ECC 256 (no RSA) certificates
- or configure to "TLS v1.2 only"

5.3 Contact

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

Phone: +49-221-985 925 0
Fax: +49-221-985 925 97
E-Mail: info@gude-systems.com
Internet: www.gude-systems.com

Managing Director: Dr.-Ing. Michael Gude, Andreas Boettcher, Philipp Gude

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

5.4 Declaration of Conformity

This product **Expert Net Control 2304** 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-systems.com in the download section of the product.

5.5 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^[18]. 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^[24] as the last option.

2. Why is a device sporadically no longer accessible when DHCP is activated? or Why does the text "DHCP is configured, but DHCP is not responding!" appear?

- If DHCP is enabled but no DHCP server responds, the last IP address continues to be used. However, the DHCP client tries to reach a DHCP server again every 5 minutes. The DHCP request lasts one minute until it is aborted. During this time the IP address is not accessible! With a static IP address, DHCP should therefore be deactivated in the device.

3. What can be done if the device is no longer accessible, but the buttons still respond?

- Entering or leaving the bootloader mode does not change the state of the relays. In the chapter Maintenance^[23] there is a description how to activate the bootloader by pressing the buttons and how to exit the bootloader afterwards. This will restart the firmware without switching relays. However, this procedure does not help if the network itself is incorrectly configured.

4. Where is the serial number stored in the device?

The serial number is not stored in the device, but only visible on the device label. However, you can display the MAC address in the IP address configuration^[31]. If you contact Gude Systems Support with the MAC address, we will be happy to give you the corresponding serial number.

5. 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.

6. 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.

7. 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](#)^[89].

8. Importing an older firmware

- During a firmware update, old data formats are sometimes converted to new structures. If an older firmware is newly installed, the configuration data and the energy meters may be lost! If the device then does not run correctly, please restore the factory settings (e.g. from the [Maintenance Page](#)^[21]). Sometimes the text "**Upload complete, firmware downgrade not compatible**" is displayed during a firmware update. In this special case a downgrade is not possible. This usually happens when a newer hardware component in the device is not supported by an older firmware.

9. Disable switching events

- You can set the sending of syslog, emails etc. when switching ports (only concerns Gude devices with relays) under "System" in the sensor configuration^[50].

- A -

automated Access 56

- B -

Bootloader Mode 18, 23

Button Lock 54

- C -

Certificate-Upload 18, 21

clear DNS-Cache 21

Configuration Management 22

Content of Delivery 6

creating certificates 91

- D -

Data Security 95

Declaration of Conformity 96

Default Display 54

Description 6

device MIB 90

- E -

E-Mail 52

Ethernet connector 8

- F -

Factory Reset 18

FAQ 97

Firmware Upload 18

Firmware-Update 21

- G -

GBL_Conf.exe 18

- H -

HTTP 34

HTTP Authentication 72

HTTP Performance 95

HTTPS 34

- I -

Input Behavior 11

Installation 8

IP-ACL 33, 74

IP-Address 31

IPv6 74

- L -

load Configuration 21

- M -

Maintenance 18

messages 75

Modbus TCP 76

MQTT 41, 83

- N -

NTP 42

- O -

Ok button 8

Operating the device directly 16

- P -

Power Ports 27

- R -

Radius 86

Restart 21

- S -

Security Advice 6

Select button 8

Sensor Calibration 14

Sensors 11, 50

SNMP 37, 87

SSH 61

SSL 91

Start-up the device 8

Status LED 8

Status-LED 16
syslog 37

- T -

Technical Specifications 10
Timer 43
Timer Configuration 43
TLS 91

- W -

Watchdog 28



Expert Net Control 2304
© 2023 GUDE Systems GmbH
8/14/2023