



# Inline Metered PDU, 1U, 1-phase, 16A, 4 x C20, 4 x C19



**User Manual**

**DN-95637**

# Content

<b>1. Device Description</b>	<b>4</b>
1.1. Security Advice	4
1.2. Content of Delivery	4
1.3. Description	4
1.4. Installation	5
1.5. Hotswap Drawer	6
1.6. Technical Specifications	6
1.6.1. Electrical Measurement	7
<b>2. Operating</b>	<b>7</b>
2.1. Operating the device directly	7
2.2. Control Panel	8
2.3. Maintenance	8
2.3.1. Maintenance Page	11
2.3.2. Configuration Management	12
2.3.3. Bootloader Activation	13
<b>3. Configuration</b>	<b>15</b>
3.1. Ethernet	15
3.1.1. IP Address	15
3.1.2. IP ACL	17
3.1.3. HTTP	17
3.2. Protocols	19
3.2.1. Console	19
3.2.2. Syslog	20
3.2.3. SNMP	20
3.2.4. Radius	22
3.2.5. Modbus TCP	23
3.3. Clock	23
3.3.1. NTP	23
3.3.2. Timer	24
3.3.3. Timer Configuration	24
3.4. Sensors	30
3.5. E-Mail	32
3.6. Front Panel	33
<b>4. Specifications</b>	<b>33</b>
4.1. IP ACL	33
4.2. IPv6	34
4.3. Radius	34
4.4. Automated Access	35
4.5. SNMP	35
4.5.1. Device MIB 8341 (DN-95637)	38
4.6. SSL	40
4.7. Console	42
4.7.1. Console Cmd 8341 (DN-95637)	46
4.8. Modbus TCP	54
4.9. Messages	59
<b>5. Support</b>	<b>60</b>

5.1. Data Security .....60  
5.2. FAQ .....61  
5.3. Declaration of Conformity.....62  
5.4. Contact .....62

# 1. Device Description

## 1.1 Security Advice

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

## 1.2 Content of Delivery

The package includes:

- Inline Metered PDU, 1U, 1-phase, 16A, 4 x C20, 4 x C19
- 1 x Power Supply cable (IEC C13, max. 10 A)
- Quick Start Guide

## 1.3 Description

The PDU can meter energy values on 4 different phases (from IEC C20 to IEC C19, max.16 A). The device has the following features:

- Energy Metering of 4 phases and measurement of voltage, current, active power, reactive power, apparent power, frequency, phase angle, power factor.
- Energy meters for all phases, continuously and resettable.
- Measurement of residual current for all phases.
- Hot Swap Drawer - The device electronics, including power supply, can be replaced on a drawer without the need to turn off the PDU consumers.
- Connecting of two optional external sensors to determine the temperature and humidity, or a input switch.
- One three-digit 7-segment LED displays (for display of current, external sensor values, IP-address and device status).

- Dual TCP/IP Stack with IPv4 and IPv6 support.
- Control and monitoring of the device via Ethernet with an integrated web server and SNMP (v1, v2c and v3).
- Control and configuration with CGI parameters and JSON messages via HTTP (REST API)
- Modbus TCP Support.
- Generation of messages (E-Mail, Syslog and SNMP traps) depending on the energy measurement limits, resp. external sensors.
- Console Commands with telnet support.
- Secure e-mails.

## 1.4 Installation

### Front of the device



- 1) Current power consumption of Phase (7-segment LED)
- 2) 8 plain text displays L1 to L4 as voltage indicator (green symbol) and which phase is shown in the display (red symbol)
- 3) Status LED
- 4) Buttons "Select" and "OK"
- 5) Ethernet connector (RJ45)
- 6) External sensor connectors (RJ45)



- 1) – 4) Load outputs for phases L1 to L4 (IEC C19, max. 16 A)

## Rear of the device



- 1) – 4) Load inputs for phases L1 to L4 (IEC C20, max. 16 A)
- 5) Mains supply (IEC C14, max. 10 A)

### Start-up the device

- Connect the power cord (IEC C14, max. 10 A) to the mains supply.
- Plug the network cable into the Ethernet socket (RJ45).
- Insert optional external sensors into the sensor connectors.
- Connect the mains supply with the load inputs (IEC C20, max. 16 A), and the consumers with the load outputs (IEC C19, max. 16 A). The cable connectors are secured as regards their type against unintentional loosening. They must be inserted up to the stop, otherwise there is no secure connection. The plug must not wobble in the socket, or there is no tight connection.

### 1.5 Hotswap Drawer

This PDU is "hot-swap" capable. The device has a removable drawer, on which all of the active electronics, including the power supply, is located. In case of a fault, you can order a replacement electronics from the manufacturer. The devices connected to the ports are not disturbed in the exchange. Specific instructions for replacement of the electronics drawer will be delivered with the exchange electronics. Do not open the drawer without a compelling reason, this can lead to loss of warranty.

### 1.6 Technical Specifications

<b>Interfaces</b>	1 x Ethernet port (RJ45) 1 x Mains supply (IEC C14, max.10 A) 4 x Load inputs (IEC C20, max. 16 A) 4 x Load outputs (IEC C19, max. 16 A) 2 x RJ45 for external sensor
<b>Network connectivity</b>	10/100 Mbit/s 10baseT Ethernet
<b>Protocols</b>	TCP/IP, HTTP/HTTPS, SNMP v1/v2c/v3, SNMP traps, Syslog, E-Mails (SMTP)
<b>Power Supply</b>	Internal power supply (90 - 265 V AC / -15%/+10%)

<b>Environment</b>	
· <b>Operating temperature</b>	0 °C – 50 °C
· <b>Storage temperature</b>	-20 °C – 70 °C
· <b>Humidity</b>	0% - 95 % (non-condensing)
<b>Case</b>	Powder coated, galvanized steel sheet
<b>Measurements</b>	19" (inches), 1 Rack Unit, (Depth 195 mm)
<b>Weight</b>	Approx. 3.3 kg

### 1.6.1 Electrical Measurements

Electrical Measurement Specification				
Category	Range	Unit	Resolution	Inaccuracy (typical)
Voltage	90 – 265	V	0.01	< 1 %
Current	0 – 16	A	0.001	< 1.5 %
Frequency	45 – 65	Hz	0.01	< 0.03 %
Phase	-180 – +180	°	0.1	< 1 %
Active power	0 – 4000	W	1	< 1.5 %
Reactive power	0 – 4000	Var	1	< 1.5 %
Apparent power	0 – 4000	VA	1	< 1.5 %
Power factor	0 – 1	-	0.01	< 3 %
Energy Counter				
Active Energy (total)	9.999.999,999	kWh	0.001	< 1.5 %
Active Energy (temporary)	9.999.999,999	kWh	0.001	< 1.5 %

## 2. Operating

### 2.1 Operating the device directly

#### Power Indicator

If the current is shown on the 7-segment display (see Configuration - sensor), then the measured current values of all phases are displayed in sequential order. When no voltage is measured (smaller 70V) the display will show three dashes, and the green plain text displays L1 to L4 are off. The red plain text displays L1 to L4 symbolize which phase is currently viewable in the display.

## Select Phase

By repeatedly pressing the "Select" button, the phase that appears on the display, can be selected manually. After approx. 60 seconds the running through all phases resumes.

## Display Information

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

## 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.

Control Panel														
Configuration Maintenance Logout														
Line	Line	Voltage	Current	Freq	Phase	active	Power	Power	Residual Current	total Energy	resettable Energy	active	time	
Id	Name	AC rms	AC rms	Hz	°	W	reactive	apparent	AC rms	active	active	kWh	kWh	h:m:s
		V	A				VAR	VA	mA	kWh	kWh			
L1	Meter1	229,3	3,326	50,00	0,0	763	-2	763	1,00	2,7	0,142	0,142	00:15:57	Reset
L2	Meter2	229,3	0,000	50,00	-94,5	0	0	0	1,00	0,0	0,005	0,005	00:15:57	Reset
L3	Meter3	227,6	0,000	50,00	137,9	0	0	0	1,00	0,0	0,005	0,005	00:15:57	Reset
L4	Meter4	8,8	0,000	50,00	-57,3	0	0	0	1,00	0,0	0,006	0,006	00:15:57	Reset
sum			3,326			763				0,0				

auto logout in 219s

The web page provides an overview of the energy measurement values of all phases, as well as the external sensors, provided that they are connected.



The column "Residual Current" is only visible on models that support this feature.

## 2.3 Maintenance

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

### Maintenance in the web interface

The following functions are available from the maintenance web page:

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



## Upload Firmware, Certificate or Configuration

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



Only one upload function can be initiated with a reboot, e.g. 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).

## Actions in Bootloader mode

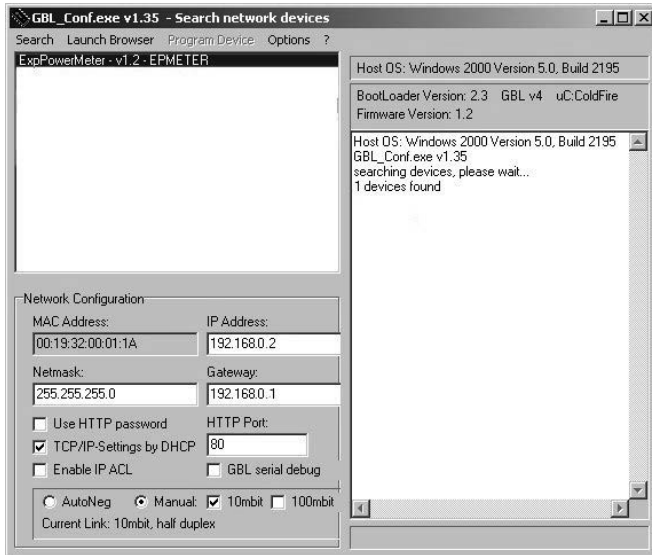
If the web interface of the device is no longer accessible, the device can be put into Bootloader mode (see chapter Bootloader activation). The following functions can be executed using the GBL\_Conf.exe application.

- Set IPv4 address, net-mask and gateway
- Turn HTTP password on and off
- Turn IP-ACL on and off
- Factory Reset
- Jump into the bootloader (can be switched on and off)
- 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.Digitus.info](http://www.Digitus.info) and can also be found on the enclosed CD-ROM.



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.

### Factory Reset

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



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

### 2.3.1 Maintenance Page

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

The screenshot shows a web interface with a navigation bar at the top containing 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. The main content area is divided into four sections:

- Firmware Update:** Contains a 'Browse...' button, the text 'No file selected.', and an 'Upload' button.
- SSL Certificate Upload:** Contains a 'Browse...' button, the text 'No file selected.', and an 'Upload' button.
- Config Import File Upload:** Contains a 'Browse...' button, the text 'No file selected.', and an 'Upload' button. Below this section is a 'Config File Export' label.
- Restart / Fab-Settings:** Contains four buttons: 'Restart Device', 'Restore Fab Settings and Restart Device', 'Enter Bootloader Mode', and 'Flush DNS Cache'.

Firmware Update: Start a firmware update.

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

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.

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

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

### 2.3.2 Configuration Management


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

**Config Import File Upload**

No file selected.

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: (only if "Enable FW to BL" was previously activated in the "GBL\_Conf.exe" application)
  - Start the "GBL\_Conf.exe" program
  - Do a network search with the "Search" menu action
  - Activate in menu "Program Device" the item "Enter Bootloader"

- 4) via web interface:
  - Press "Enter Bootloader Mode" on the maintenance web page.

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



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

### **Abandonment of the Bootloader Mode (1-Button)**

1. via push button:
  - Hold both buttons for 3 seconds (only if the device has 2 buttons)
2. or
  - Remove and connect the power supply without operating a button
3. by Software:
  - Start the "GBL\_Conf.exe" application
  - Do a network search with the "Search" menu action
  - In menu "Program Device" activate the item "Enter Firmware"

### **Factory Reset**

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



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

- 1) via push button:
  - Activate the Bootloader Mode of the device
  - Hold down the button (or the "Select" button for devices with 2 buttons) for 6 seconds. If the push button is recessed, use a pin or paper clip
  - The status LED will blink in a fast rhythm, please wait until the LED blinks slowly (about 5 seconds)
- 2) by Software:
  - Activate the Bootloader Mode of the device
  - "Start the GBL\_Conf.exe" program
  - In menu "Program Device" activate the item "Reset to Fab Settings"
  - The status LED will blink in a fast rhythm, please wait until the LED blinks slowly (about 5 seconds)

### 3. Configuration

#### TCP/IP configuration by DHCP

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

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

#### 3.1 Ethernet

##### 3.1.1 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:

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

Use IPv6 Protocol: Activates IPv6 usage.

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

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

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

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

**IPv6 status**

- Current IPv6 status:

IPv6 Addr:  
fe80::219:32ff:fe00:996d  
2007:7dd0:ffc1:1:219:32ff:fe00:996d

IPv6 DNS Server:  
2007:7dd0:ffc1:1:20c: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:  / 64  
 / 64  
 / 64  
 / 64
- IPv6 DNS addresses:
- IPv6 Gateway address:

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



### 3.1.2 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

- Grant IP access to host/net:
- Grant IP access to host/net:
- Grant IP access to host/net:
- Grant IP access to host/net:
- Grant IP access to host/net:

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.

### 3.1.3 HTTP

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

**HTTP**

• HTTP Server option:  HTTP + HTTPS  HTTPS only  HTTP only

• Server port HTTP:

• Server port HTTPS:

• Enable Ajax autorefresh:  yes  no

**HTTP Password**

• Enable password protection:  yes  no

• 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:

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

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

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

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



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

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

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

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



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



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

## 3.2 Protocols

### 3.2.1 Console

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

#### Telnet Console

- Enable Telnet:  yes  no
- Telnet TCP port:
- Raw mode:  yes  no
- Activate echo:  yes  no
- Active negotiation:  yes  no
  
- Require user login:  yes  no
  - Delay after 3 failed logins:  yes  no
  - use radius server passwords:  yes  no
  - use locally stored passwords:  yes  no
    - Username:
    - Set new password:  (32 characters max)
    - Repeat password:

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.

### 3.2.2 Syslog

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

**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.

### 3.2.3 SNMP

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

**SNMP**

- Enable SNMP options:  SNMP get  SNMP set
- SNMP UDP port:

**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.

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 reentered.



The calculation of the password hashes varies with the selected algorithms. If the Authentication or Privacy algorithms are changed, the passwords must be reentered 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.

### 3.2.4 Radius

Console · Syslog · SNMP · Radius · Modbus

**Radius**

- Enable Radius Client:  yes  no
- Use CHAP:  yes  no
- 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.

### 3.2.5 Modbus TCP

Console · Syslog · SNMP · Radius · Modbus

**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.

## 3.3 Clock

### 3.3.1 NTP

NTP · Timer

**NTP**

- Enable Time Synchronisation:  yes  no
- Primary NTP server:
- reply 21s ago · 11ms signal delay  
· Tue Feb 19 2019 16:50:33 GMT+0100 (Central European Standard Time)
- Backup NTP server:

**Timezone:**

- Timezone: (GMT+01:00) Berlin, Paris, Central I ▾
- Daylight Saving Time (DST):  yes  no

**Clock**

- Current Systemtime (UTC): 15:50:54 19.02.2019 (1550591454)
- Current Localtime: 16:50:54 19.02.2019
- Browsertime: 16:50:54 19.02.2019

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 Browsertime: Sets the time corresponding to web browser.



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

### 3.3.2 Timer

NTP · Timer

**Timer - Basic Settings**

Enable Timer:  yes  no

Syslog verbosity level:

**Timer - Rules**

New Rule: simple Timer

New Rule: advanced Timer

Apply

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

### 3.3.3 Timer Configuration

There are three possibilities in the timer configuration: Create a simple timer, add an advanced timer, or change an existing configuration.



Timer rules are only executed if the device has a valid time. See Configuration NTP.





This chapter of the manual applies to all Digitus devices. Devices without switchable ports can only have an advanced timer. For an action only the "Action CLI" tab is available there, and not the "Action PortSwitch" tab.

**Timer - Basic Settings**

Enable Timer:  yes  no

Syslog verbosity level:

---

**Timer - Rules**

### Create a simple timer

When "New Rule: simple Timer" is activated, the following dialog is displayed:

**Timer Rule** ✕

Switch

From : To :

On weekdays:  Mon  Tue  Wed  Thu  Fri  Sat  Sun

Here you set which port is to be switched for which period and on which weekdays 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. This rule is also not applied to Saturdays and Sundays. The now existing rule says that on every day, except Saturday and Sunday, port 1 is switched on at 9:30 a.m. and switched off after 1.5 hours. A click on "Save" saves this rule.



For example, using only one timer rule to turn on a port at 9:00, and turn it off at 20:00. If at 9:00 the timer is triggered, a batch mode is created to switch off after 11 hours. If the batch mode is running, the port is locked against manual operation on the web page. Also nothing happens on a day at 20:00, if this rule is entered at 10:00, because the rule is triggered at 9:00, and the batch mode then switches off at 20:00. If you don't want this behavior, please use a second rule to explicitly switch off the port at 20:00.

### Creating an advanced timer

If you create an advanced timer or change an already existing timer, an extended dialog is always shown:

Here you can see the extended representation 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 subsequent rules also changes by one. This also applies to the index in the console commands.

A simple timer is directly "enabled", on a new complex timer the "enable trigger" option must be switched on manually. You can set a probability and a scatter for the timer rules. Here the rule is executed with 100% probability. A jitter of 0 means that the action takes place exactly at the programmed time. As an action mode a ports can be switched, alternatively a console command (CLI Cmd) can be executed.

On the "Action PortSwitch" tab the switching function can be set in more detail. Port 1 is switched on and switched off again after 1.5 hours.

**Timer Rule** [X]

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

Switch Power Ports Action1:

On	On	On	On	On	On	On	On	On
Off	Off	Off	Off	Off	Off	Off	Off	Off

Switch Power Ports Action2:

On	-	-	-	-	-	-	-
Off	-	-	-	-	-	-	-

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

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

### Extending a rule

For demonstration purposes, the simple timer from the previous example is extended here:

**Timer Rule** [X]

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 will now not only start at 9:30, but also at 17:30. There are more 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 taken into account, 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 hours 9 and 17, as well as minutes 10 and 30, then the four times 9:10, 9:30, 17:10 and 17:30 would be programmed.

 In order 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.

**Timer Rule** [x]

Trigger: Date/Time Pattern   Options   Action PortSwitch   Action Cli

Rule Name:

Rule Valid from:  to  dd.mm.yyyy

Random Trigger Probability:  [▲ ▼]

Random Trigger Jitter:  secs

enable trigger:  yes  no

Action mode:  Switch Power Ports  Perform CLI Cmd

With this rule, the time period in the "Options" tab is limited to the period between December 5, 2018 and July 4, 2019. In this example, the timer rule is executed with a random trigger probability of 90%.

**Timer Rule** [x]

Trigger: Date/Time Pattern   Options   Action PortSwitch   Action Cli

Switch Power Ports Action1:

On	On	On	On	On	On	On	On
Off	Off	Off	Off	Off	Off	Off	Off

Switch Power Ports Action2:

On	-	-	-	On	-	-	-
Off	-	-	-	Off	-	-	-

Between Action1 and Action 2 : wait  minute(s) ▼

In addition to port 1, port 5 is activated here and deactivated again after 90 minutes.



A popup at the mouse pointer shows the port number of the corresponding field.

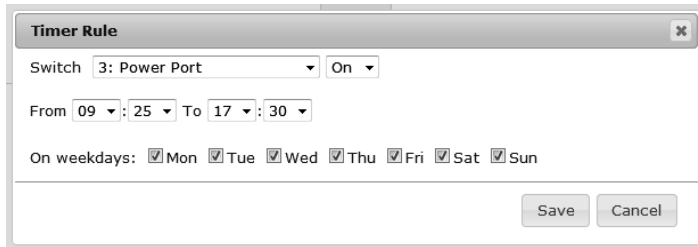
## Console Commands



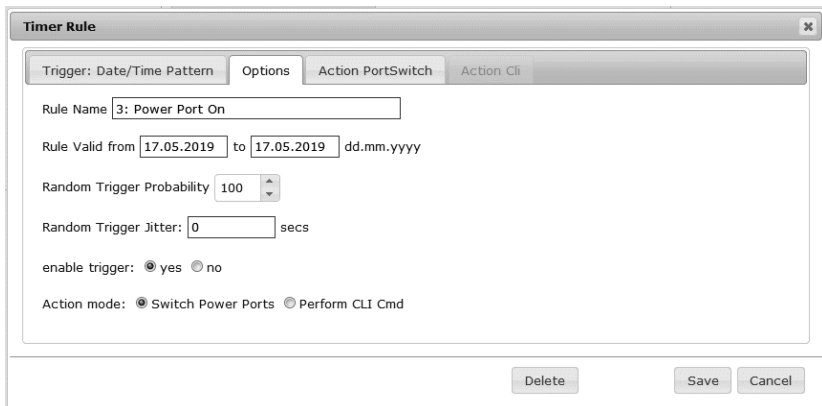
Instead of switching a port, you can run one or more console commands. These commands are entered in the "Action CLI" tab. The "Action Cli" tab can only be selected if the option "Perform CLI Cmd" is activated under "Options".

### Example Switching a Port on a Date

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



Switches port 3 on every day at 9:25, and off again at 17:30. Save the simple rule.



Then you call up the created timer and enter in the "Options" tab the date on which the switching process should take place.

### Example rolling shutter

**Timer Rule**

Trigger: Date/Time Pattern   Options   Action PortSwitch   Action Cli

Rule Name: 1: Power Port On

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

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

### 3.4 Sensors

Control Panel   Configuration   Maintenance   Logout

Ethernet · Protocols · **Sensors** · E-Mail · Front Panel

**Sensors Config**

- Sensor: 1: 7106 - 7106
- Sensor Name: 7106
- Select Sensor Field: Temperature (°C)
- Enable 'Temperature' Messages:  yes  no
- Maximum value: 65.0 °C
- Minimum value: 25.0 °C
- Hysteresis: 3.0 °C
- Message channels:  Syslog  SNMP  Email  Beeper

**Misc sensor options**

- Min/Max measurement period: 24 Hours
- Enable beeper for AC alarms:  yes  no
- Enable beeper for sensor alarms:  yes  no

Apply

Sensor: Selects a type of sensor to configure it. The first digit "1" indicates the number of the sensor port (only important for devices with more than one sensor port). This is followed by the sensor name, and the changeable sensor name.

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

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

Enable ... Messages: Enables the generation of sensor messages.

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

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

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

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

Enable beeper for AC alarms: Activates the beeper for all AC limit messages.

Enable beeper for sensor alarms: Activates the beeper for all sensor limit messages.

### **Hysteresis Example**

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

Example:

49.9 °C - is below the upper limit

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

50.1 °C - is above the upper limit

...

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

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

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

...

### 3.5 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.



### 3.6 Front Panel

**Front Panel**

- Button Lock:  yes  no
- Dark Display:  yes  no
- Default Display:

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

**Dark Display:** The 7-segment display remains dark. Front button activity temporarily switches the display on.

**Default Display:** Selects what sensor is displayed in the display.

## 4. Specifications

### 4.1 IP ACL

#### IP Access Control List

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

Examples:

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



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

## 4.2 IPv6

### IPv6 Addresses

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

### Address Notation

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

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

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

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

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

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

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

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

## 4.3 Radius

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

### RADIUS attributes

The following RADIUS attributes are evaluated by the client:

**Session-Timeout:** This attribute specifies (in seconds) how long an accepted RADIUS request is valid. After this time has elapsed, the RADIUS server must be prompted again. If this attribute is not returned, the default timeout entry from the configuration is used instead.

**Filter-Id:** If the value "admin" is set for this attribute, then an admin rights are assigned for the login, otherwise only user access.

**Service-Type:** This is an alternative to Filter-Id. A service type of "6" or "7" means admin rights for the HTTP login, otherwise only limited user access.

## HTTP Login

The HTTP login takes place via Basic Authentication. This means that it is the responsibility of the web server, how long the login credentials are temporarily stored there.

The RADIUS parameter "Session-Timeout" therefore does not determine when the user has to login again, but at what intervals the RADIUS servers are asked again.

## 4.4 Automated Access

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

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

Interface	Scope of Access
HTTP	Read / write all configuration data Read / write all status information
Console	Read / write all configuration data Read / write all status information
SNMP	Read / write status of Power Ports (relays) Read / write names of Power Ports (relays) Read / write status of Port start configuration Read / write status Buzzer Read measurement values of external sensors Read measurement values of all energy sensors Resetting the energy meters Read the status of Overvoltage Protection
Modbus TCP	Read / write status of Power Ports (relays) Read status of inputs Read measurement values of external sensors Read measurement values of all energy sensors

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

## 4.5 SNMP

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

- GET
- GETNEXT
- GETBULK
- SET

To query via SNMP you need a Network Management System, such as HP OpenView, OpenNMS, Nagios etc., or the simple command line tools of NET-SNMP software. The device

supports SNMP protocols v1, v2c and v3. If traps are enabled in the configuration, the device messages are sent as notifications (traps). SNMP Informs are not supported. SNMP Requests are answered with the same version with which they were sent. The version of the sent traps can be set in the configuration.

### **MIB Tables**

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

### **SNMP v1 and v2c**

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

### **SNMP v3**

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

### **Authentication**

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



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

### **Encryption**

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



While in the settings "AES-192" and "AES256" the key calculation is based on "draft-blumenthalphoto-aes-usm-04", the methods "AES 192-3DESKey" and "AES

256-3DESKey" utilize a key generation, which is also used in the "3DES" configuration ("draft-reeder-snmppv3-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 reentered in the configuration dialog.

## Security

The following aspects should be considered:

- If encryption or authentication is used, then SNMP v1 and v2c should be turned off. Otherwise the device could be accessed with it.
- If only authentication is used, then the new "HMAC-SHA-2" methods are superior to the MD5 or SHA-1 hashing algorithms. Since only SHA-256 is accelerated in hardware, and SHA-384 and SHA-512 are calculated purely in software, one should normally select SHA-256. From a cryptographic point of view, the security of SHA-256 is sufficient for today's usage.
- For SHA-1, there are a little less attack scenarios than MD5. If in doubt, SHA-1 is preferable.
- Encryption "DES" is considered very unsafe, use only in an emergency for reasons of compatibility!
- For cryptologists it's a debatable point whether "HMAC-MD5-96" and "HMAC-SHA-96" can muster enough entropy for key lengths of "AES-192" or "AES-256".
- From the foregoing considerations, we would recommended at present "HMAC- SHA-96" with "AES-128" as authentication and encryption method.

## Change in Trap Design



In older MIB tables, a separate trap was defined for each combination of an event and a port number. This results in longer lists of trap definitions for the devices. For example, from **epc8221SwitchEvtPort1** to **epc8221SwitchEvtPort12**. Since new firm- ware 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 (snmp-pget, snmpset, snmpwalk etc.) NET-SNMP is among others available for Linux and Windows. After installing NET-SNMP you should create the device-specific MIB of the device in NET-SMP share directory, e.g. after

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

or

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

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

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

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

## NET-SNMP Examples

Query Power Port 1 switching state:

```
snmpget -v2c -mALL -c public 192.168.1.232 epc822XPortState.1
```

Switch on Power Port 1:

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

### 4.5.1 Device MIB 8341 (DN-95637)

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 " was omitted at each entry in the table to preserve space. The example for a complete OID would be "1.3.6.1.4.1.28507.65.1.1.1.1". 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.
pdu8341TrapCtrl	0 = off 1 = Ver. 1 2 = Ver. 2c 3 = Ver. 3	.65.1.1.1.1.0	Integer32	RW
pdu8341TrapIIndex	A unique value, greater than zero, for each receiver slot.	.65.1.1.1.2.1.1.x	Integer32	RO
pdu8341TrapAddr	DNS name or IP address specifying one Trap receiver slot. A port can optionally be specified: 'name:port' An empty string disables this slot.	.65.1.1.1.2.1.2.x	OCTETS	RW
pdu8341Buzzer	Turn buzzer on and off	.65.1.3.10.0	Integer32	RW
pdu8341ActivePowerChan	Number of supported Power Channels	.65.1.5.1.1.0	Unsigned32	RO
pdu8341PowerIndex	Index of Power Channel entries	.65.1.5.1.2.1.1.x	Integer32	RO

pdu8341ChanStatus	0 = data not active, 1 = data valid	.65.1.5.1.2.1.2.x	Integer32	RO
pdu8341AbsEnergyActive	Absolute active energy counter	.65.1.5.1.2.1.3.x	Gauge32	RO
pdu8341PowerActive	Active Power	.65.1.5.1.2.1.4.x	Integer32	RO
pdu8341Current	Actual Current on Power Channel	.65.1.5.1.2.1.5.x	Gauge32	RO
pdu8341Voltage	Actual Voltage on Power Channel	.65.1.5.1.2.1.6.x	Gauge 32	RO
pdu8341Frequency	Frequency of Power Channel	.65.1.5.1.2.1.7.x	Gauge32	RO
pdu8341PowerFactor	Power Factor of Channel between -1.0 and 1.00	.65.1.5.1.2.1.8.x	Integer32	RO
pdu8341Pangle	Phase Angle between Voltage and L Line Current between -180.0 and 180.0	.65.1.5.1.2.1.9.x	Integer32	RO
pdu8341PowerApparent	L Line Mean Apparent Power	.65.1.5.1.2.1.10.x	Integer32	RO
pdu8341PowerReactive	L Line Mean Reactive Power	.65.1.5.1.2.1.11.x	Integer32	RO
pdu8341AbsEnergyReactive	Absolute reactive energy counter	.65.1.5.1.2.1.12.x	Gauge32	RO
pdu8341AbsEnergyActiveResettable	Resettable absolute active energy counter. Writing '0' resets all resettable counter.	.65.1.5.1.2.1.13.x	Gauge32	RW
pdu8341AbsEnergyReactiveResettable	Resettable absolute reactive energy counter	.65.1.5.1.2.1.14.x	Gauge32	RO
pdu8341ResetTime	Time in seconds since last energy counter reset	.65.1.5.1.2.1.15.x	Gauge32	RO
pdu8341ForwEnergyActive	Forward active energy counter	.65.1.5.1.2.1.16.x	Gauge32	RO
pdu8341ForwEnergyReactive	Forward reactive energy counter	.65.1.5.1.2.1.17.x	Gauge32	RO
pdu8341ForwEnergyActiveResettable	Resettable forward active energy counter	.65.1.5.1.2.1.18.x	Gauge32	RO
pdu8341ForwEnergyReactiveResettable	Resettable forward reactive energy counter	.65.1.5.1.2.1.19.x	Gauge32	RO
pdu8341RevEnergyActive	Reverse active energy counter	.65.1.5.1.2.1.20.x	Gauge32	RO
pdu8341RevEnergyReactive	Reverse reactive energy counter	.65.1.5.1.2.1.21.x	Gauge32	RO
pdu8341RevEnergyActiveResettable	Resettable reverse active energy counter	.65.1.5.1.2.1.22.x	Gauge32	RO
pdu8341RevEnergyReactiveResettable	Resettable reverse reactive energy counter	.65.1.5.1.2.1.23.x	Gauge32	RO
pdu8341ResidualCurrent	Actual residual current on power channel. According type A IEC 60755. Only visible on models that support this feature.	.65.1.5.1.2.1.24.x	Unsigned32	RO
pdu8341LineSensorName	A textual string containing name of a Line sensor.	.65.1.5.1.2.1.100.x	OCTETS	RW
pdu8341SensorIndex	None	.65.1.6.1.1.1.x	Integer32	RO
pdu8341TempSensor	Actual temperature	.65.1.6.1.1.2.x	Integer32	RO
pdu8341HygroSensor	Actual humidity	.65.1.6.1.1.3.x	Integer32	RO
pdu8341InputSensor	Logical state of input sensor	.65.1.6.1.1.4.x	INTEGER	RO
pdu8341AirPressure	Actual air pressure	.65.1.6.1.1.5.x	Integer32	RO
pdu8341DewPoint	Dew point for actual temperature and humidity	.65.1.6.1.1.6.x	Integer32	RO

pdu8341DewPointDiff	Difference between dew point and actual temperature (Temp-DewPoint)	.65.1.6.1.1.7.x	Integer32	RO
pdu8341ExtSensorName	A textual string containing name of an external sensor	.65.1.6.1.1.32.x	OCTETS	RW

## 4.6 SSL

### TLS Standard

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

The following TLS Ciphersuites are supported:

- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_PSK\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256



- TLS\_RSA\_WITH\_AES\_128\_CCM
- TLS\_RSA\_WITH\_AES\_256\_CCM
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CCM
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CCM
- TLS\_RSA\_WITH\_AES\_128\_CCM\_8
- TLS\_RSA\_WITH\_AES\_256\_CCM\_8
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CCM\_8
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CCM\_8
- TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256
- TLS\_DHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

### Creating your own certificates

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

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

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

Here are some examples for the generation with OpenSSL:

#### Creation of a self-signed RSA 2048-bit certificate:

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

#### RSA 2048-bit certificate with Sign Request:

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



The server keys should be 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.

### **Performance Considerations**

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

### **4.7 Console**

For the configuration and control of the device, there is a set of commands with parameters that can be entered through a console. The console is available via Telnet, or for devices with RS232 port through using a serial terminal. It is not necessary to use Telnet, in Raw Mode a simple TCP/IP connection is sufficient to send commands. The communication can also be performed automated (e.g. via scripting languages). The console features are configured through the web interface.

### **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_BEEP=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

### Bundled Information

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

#### a) External Sensors

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

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

#### b) Line Sensors

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

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



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

```
>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).

### 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.

#### 4.7.1 Console Cmd 8341 (DN-95637)

Command	Description	Note
Logout	Go to login prompt enabled	2
Quit	Quit 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
Clock	Enters cmd group "clock"	
Clock enabled set {OFF=0 ON=1}	Enables ntp	
Clock enabled show	Shows if ntp enabled	
Clock timezone set {minutes}	Sets timezone	
Clock timezone show	Shows timezone	
Clock dst enabled set {OFF=0 ON=1}	Enables dst	
Clock dst enabled show	Shows if dst is enabled	
Clock manual set "{hh:mm:ss yyyy-mm-dd}"	Sets time and date manually	
Clock show	Shows 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	Shows ntp server name	
Console	Enters cmd group "console"	

Console version	Shows unique console version number	
Console telnet enabled set {OFF=0 ON=1}	Enables telnet on/off	
Console telnet enabled show	Shows if telnet enabled	
Console telnet port set {ip_port}	Sets telnet port	
Console telnet port show	Shows telnet port	
Console telnet raw set {OFF=0 ON=1}	Sets raw mode (disables editing) on/off	
Console telnet raw show	Shows if raw mode enabled	
Console telnet echo set {OFF=0 ON=1}	Enables echo on/off	
Console telnet echo show	Shows if echo enabled	
Console telnet activeneg set {OFF=0 ON=1}	Enables telnet active negotiation (IAC) on/off	
Console telnet activeneg show	Shows if active negotiation enabled	
Console telnet login set {OFF=0 ON=1}	Enables login on/off	
Console telnet login show	Shows if login enabled	
Console telnet login local set {OFF=0 ON=1}	Enables local login on/off	
Console telnet login local show	Shows if local login enabled	
Console telnet login radius set {OFF=0 ON=1}	Enables login für RADIUS on/off	
Console telnet login radius show	Shows if RADIUS login enabled	
Console telnet login delay set {OFF=0 ON=1}	Enables delay (after 3 login fails) on/off	
Console telnet login delay show	Shows if login delay enabled	
Console telnet user set "{username}"	Sets login user name	
Console telnet user show	Shows login user name	
Console telnet passwd set "{passwd}"	Sets login password	
Console telnet passwd hash set "{passwd}"	Sets login hashed password	
Email	Enters cmd group "email"	
Email enabled set {OFF=0 ON=1}	Enables email on/off	
Email enabled show	Shows if email is enabled	
Email sender set "{email_addr}"	Sets email sender address	
Email sender show	Shows email sender address	
Email recipient set "{email_addr}"	Sets email recipient address	
Email recipient show	Shows email recipient address	
Email server set "{dns_name}"	Sets email SMTP server address	
Email server show	Shows email SMTP server address	
Email port set "{ip_port}"	Sets email SMTP port	
Email port show	Shows email SMTP port	
Email security set "{NONE=0 STARTTLS=1 SSL=2}"	Sets SMTP connection security	
Email security show	Shows SMTP connection security	
Email auth set "{NONE=0 PLAIN=1 LOGIN=2}"	Sets email authentication	
Email auth show	Show email authentication	
Email user set "{username}"	Sets SMTP username	
Email user show	Shows SMTP username	
Email passwd set "{passwd}"	Sets SMTP password	
Email passwd hash set "{passwd}"	Sets crypted SMTP password	
Email testmail	Send test mail	
Ethernet	Enters cmd group "ethernet"	
Ethernet mac show	Shows MAC address	
Ethernet link show	Shows ethernet link state	
Ethernet phyprefer set "{10MBIT_HD=0 10MBIT_FD=1 100MBIT_HD=2 100MBIT_FD=3}"	Sets preferred speed for PHY Auto Negotiation	
Ethernet phyprefer show	Shows preferred speed for PHY Auto Negotiation	
Extsensor	Enters cmd group "extsensor"	

Extsensor 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 values	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 label	6
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 enables different event types 6,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	Enables different event types	6
Extsensor {port_num} {sen_type} {sen_field} events type show	Shows what event types are enabled	6
Extsensor {port_num} {sen_type} {sen_field} maxval set {num}	Sets maximum value for sensor	6
Extsensor {port_num} {sen_type} {sen_field} maxval show	Shows maximum value for sensor	6
Extsensor {port_num} {sen_type} {sen_field} min- val set {num}	Sets minimum value for sensor	6
Extsensor {port_num} {sen_type} {sen_field} min- val show	Shows minimum value for sensor	6
Extsensor {port_num} {sen_type} {sen_field} hyst set {num}	Sets hysteresis value for sensor	6
Extsensor {port_num} {sen_type} {sen_field} hyst show	Shows hysteresis value for sensor	6
Extensor {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
Extensor {port_num} {sen_type} {sen_field} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2  BELOWMAX=3} port show	Shows port for power port switching actions	6
Extensor {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
Extensor {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	
Extensor beeper set {OFF=0 ON=1}	Enables beeper sensor alarms	
Extensor beeper show	Shows if beeper sensor alarms are enabled	
http	Enters cmd group "http"	
http server set {HTTP_BOTH=0 HTTPS_ONLY=1 HTTP_ONLY=2}	Sets connection typed the webserver accepts	
http server show	Shows webserver accepting connection types	
http port set {ip_port}	Sets http port	
http port show	Shows http port	
http portssl set {ip_port}	Sets https port	
http portssl show	Shows https port	
http ajax enabled set {OFF=0 ON=1}	Enables ajax autorefresh on/off	
http ajax enabled show	Shows if ajax autorefresh enabled	
http passwd enabled set {OFF=0 ON=1}	Enables http password on/off	
http passwd enabled show	Shows if http password enabled	
http passwd user set "{passwd}"	Sets http user password	
http passwd admin set "{passwd}"	Sets http admin password	
http passwd hash user set "{passwd}"	Sets hashed http user password	
http passwd hash admin set "{passwd}"	Sets hashed http admin password	



ip4	Enters cmd group "ip4"	
ip4 hostname set "{name}"	Sets device hostname	
ip4 hostname show	Shows device hostname	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 routeradv 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	3
ip6 manual address {1_4} show	Shows manual IPv6 address	3
ip6 manual gateway set "{ip_address}"	Sets manual IPv6 gateway address	3
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 ping enabled set {OFF=0 ON=1}	Enables ICMP ping on/off	
ipacl ping enabled show	Shows if ICMP ping enabled	
ipacl enabled set {OFF=0 ON=1}	Enables IP filter on/off	
ipacl enabled show	Shows if IP filter enabled	
ipacl filter {ipacl_num} set "{dns_name}"	Sets IP filter {ipacl_num}	
ipacl filter {ipacl_num} show	Shows IP filter {ipacl_num}	
linesensor all {field_list} show	Shows energy sensors according field list of all line sensors	5
linesensor {line_num} {energy_sensor} value show	Shows energy sensor of given line	5
linesensor {line_num} ovp show	Show state of overvoltage protection	
linesensor {line_num} counter reset	Resets energy metering counter	
linesensor {line_num} label set „{name}“	Sets line meter to label	
linesensor {line_num} label show	Shows label of line meter	
linesensor {line_num} {energy_sensor} events set {OFF=0 ON=1}	Enables events on/off	
linesensor {line_num} {energy_sensor} events show	Shows if events are enabled	
linesensor {line_num} {energy_sensor} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	Enables different event types	
linesensor {line_num} {energy_sensor} events type show	Shows what event types are enabled	
linesensor {line_num} {energy_sensor} maxval set {float}	Sets maximum value for line meter	
linesensor {line_num} {energy_sensor} maxval show	Shows maximum value for line meter	

Linesensor {line_num} {energy_sensor} minval set {float}	Sets minimum value for line meter	
Linesensor {line_num} {energy_sensor} minval show	Shows minimum value for line meter	
Linesensor {line_num} {energy_sensor} hyst set {float}	Sets hysteresis value for line meter	
Linesensor {line_num} {energy_sensor} hyst show	Shows hysteresis value for line meter	
Linesensor {line_num} {energy_sensor} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port set {port_num}	Sets port for power port switching actions	
Linesensor {line_num} {energy_sensor} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port show	Shows port for power port switching actions	
Linesensor {line_num} {energy_sensor} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} state set {OFF=0 ON=1 DISABLED=2}	Sets port state for power port switching actions	
Linesensor {line_num} {energy_sensor} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} state show	Shows port state for power port switching actions	
Linesensor {line_num} events set {OFF=0 ON=1}	LEGACY – enables event on/off	L
Linesensor {line_num} events show	LEGACY – shows if events are enabled	L
Linesensor {line_num} events type set {EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	LEGACY – enables different event types	L
Linesensor {line_num} events type show	LEGACY – shows what event types are enabled	L
Linesensor {line_num} maxval set {float}	LEGACY – sets maximum value for line meter	L
Linesensor {line_num} maxval show	LEGACY – shows maximum value for line meter	L
Linesensor {line_num} minval {float}	LEGACY – sets minimum value for line meter	L
Linesensor {line_num} minval show	LEGACY – shows minimum value for line meter	L
Linesensor {line_num} hyst set {float}	LEGACY – sets hysteresis value for line meter	L
Linesensor {line_num} hyst show	LEGACY – shows hysteresis value for line meter	L
Linesensor beeper set {OFF=0 ON=1}	Enables beeper for line meter alarms	
Linesensor beeper show	Shows if beeper for line meter alarms are enabled	
Modbus	Enters cmd group "modbus"	
Modbus enabled set <on=0 off=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	
Radius	Enters cmd group "radius"	
Radius {PRIMARY=0 SECONDARY=1} enabled set <off=0/on=1>	Enables radius client	
Radius {PRIMARY=0 SECONDARY=1} enabled show	Shows if radius client is enabled	
Radius {PRIMARY=0 SECONDARY=1} server set "<dns_name>"	Sets radius server address	
Radius {PRIMARY=0 SECONDARY=1} server show	Shows radius server address	
Radius {PRIMARY=0 SECONDARY=1} password	Sets radius server shared secret	
Radius {PRIMARY=0 SECONDARY=1} password hash set "{passwd}"	Sets radius server crypted shared secret	
Radius {PRIMARY=0 SECONDARY=1} auth timeout set {num_secs}	Sets server request timeout	
Radius {PRIMARY=0 SECONDARY=1} auth timeout show	Shows server request timeout	
Radius {PRIMARY=0 SECONDARY=1} retries set {num}	Sets server number of retries	
Radius {PRIMARY=0 SECONDARY=1} retries show	Shows server number of retries	

Radius chap enabled set <off=0/on=1>	Enables CHAP	
Radius chap enabled show	Shows if CHAP is enabled	
Radius message auth set <off=0/on=1>	Enables request message authentication	
Radius message auth show	Shows if request message authentication is enabled	
Radius default timeout set {num_secs}	Sets default session timeout (when not returned as session-timeout attribute)	
Radius default timeout show	Shows default session timeout	
Snmp	Enters cmd group "snmp"	
Snmp port set {ip_port}	Sets SNMP UDP port	
Snmp port show	Shows SNMP UDP port	
Snmp snmpget enabled set {OFF=0 ON=1}	Enables SNMP GET cmds on/off	
Snmp snmpget enabled show	Shows if SNMP GET cmds are enabled	
Snmp snmpset enabled set {OFF=0 ON=1}	Enables SNMP SET cmds on/off	
Snmp snmpset enabled show	Shows if SNMP SET cmds are enabled	
Snmp snmpv2 enabled set {OFF=0 ON=1}	Enables SNMP v2 on/off	
Snmp snmpv2 enabled show	Shows if SNMP v2 is enabled	
Snmp snmpv2 public set "{text}"	Enables SNMP v3 on/off	
Snmp snmpv2 public show	Shows if SNMP v3 is enabled	
Snmp snmpv2 private set "{text}"	Sets SNMP v2 public community	
Snmp snmpv2 private show	Shows SNMP v2 public community	
Snmp snmpv3 enabled set {OFF=0 ON=1}	Sets SNMP v2 private community	
Snmp snmpv3 enabled show	Shows SNMP v2 private community	
Snmp snmpv3 username set "{text}"	Sets SNMP v3 username	
Snmp snmpv3 username show	Shows SNMP v3 username	
Snmp snmpv3 authalg set {NONE=0 MD5=1 SHA1=2 SHA256=3 SHA384=4 SHA512=5}	Sets SNMP v3 authentication	
Snmp snmpv3 authalg show	Shows 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	Shows SNMP v3 privacy algorithm	
Snmp snmpv3 authpasswd set "{passwd}"	Sets SNMP v3 authentication password	
Snmp snmpv3 privpasswd set "{passwd}"	Sets SNMP v3 privacy password	
Snmp snmpv3 authpasswd hash set "{passwd}"	Sets SNMP v3 authentication hashed password	
Snmp snmpv3 privpasswd hash set "{passwd}"	Sets SNMP v3 privacy hashed password	
Snmp trap type set {NONE=0 V1=1 V2=2 V3=3}	Sets type of SNMP traps	
Snmp trap type show	Show SNMP trap type	
Snmp trap receiver {trap_num} set "{dns_name}"	Sets address and port of SNMP trap receiver [trap_num]	
Snmp trap receiver {trap_num} show	Show address and port of SNMP trap receiver {trap_num}	
Syslog	Enters cmd group "syslog"	
Syslog enabled set {OFF=0 ON=1}	Enables syslog msgs on/off	
Syslog enabled show	Shows if syslog enabled	
Syslog server set "{dns_name}"	Sets address of syslog server	
Syslog server show	Shows address of syslog server	

System	Enters cmd group "system"	
System restart	Restarts device	
System fabsettings	Restore fab settings and restart device	
System bootloader	Enters bootloader mode	
System flushdns	Flush DNS cache	
System uptime	Number of secons the device is running	
System panel enabled set {OFF=0 ON=1}	Blocks panel buttons when not enabled	
System panel enabled show	Shows if panel buttons are enabled	
System display enabled set {OFF=0 ON=1}	Dark display when not enabled	
System display enabled show	Show if display enabled	
System display default extsensor {port_num} {7x01=0 7x02=1 7x03=2} set {sen_field}	Sets default display to external sensor	
System display default linesensor {line_num} set {sen_field}	Sets default display to linesensor	
System display default show	Shows default display	
System display brightness set {brightness_num}	Sets display brightness	
System display brightness show	Shows display brightness	
Timer	Enters cmd group "timer"	
Timer enabled {OFF=0 ON=1}	Enables timer functions	
Timer enabled show	Shows if timer is enabled	
Timer syslog facility set {0..23}	Sets facility level for timer syslog	
Timer syslog facility show	Shows facility level for timer syslog	
Timer syslog verbose set {0..7}	Sets verbose level for timer syslog	
Timer syslog verbose show	Shows verbose level for timer syslog	
Timer {rule_num} enabled set {OFF=0 ON=1}	Enables rule	
Timer {rule_num} enabled show	Shows if rule is enabled	
Timer {rule_num} name set "{name}"	Sets name of rule	
Timer {rule_num} name show	Shows name of rule	
Timer {rule_num} {FROM=0 UNTIL=1} set "{yyyy-mm-dd}"	Sets data range of rule	
Timer {rule_num} {FROM=0 UNTIL=1} show	Shows data range of rule	
Timer {rule_num} trigger jitter set {0..65535}	Sets jitter for rule	
Timer {rule_num} trigger jitter show	Show jitter for rule	
Timer {rule_num} trigger random set {0..100}	Sets probability for rule	
Timer {rule_num} trigger random show	Shows 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	Shows time date list	
Timer {rule_num} action mode set {SWITCH=1 CLI=2}	Sets switch or cli cmd	
Timer {rule_num} action mode show	Shows if switch or cli cmd	
Timer {rule_num} action {SWITCH1=0 SWITCH2=1} {OFF=0 ON=1} set "{port_list}"	Sets port list for switch cmd	
Timer {rule_num} action {SWITCH1=0 SWITCH2=1} {OFF=0 ON=1} show	Shows port list for switch cmd	
Timer {rule_num} action delay set {0..65535}	Delay between cmds	
Timer {rule_num} action delay show	Shows delay between cmds	
Timer {rule_num} action console set "{cmd}"	Sets cmd string	
Timer {rule_num} action console show	Shows cmd string	
Timer {rule_num} action hash set "{data}"	Sets action binary form	
Timer {rule_num} action hash show	Shows 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	Shows console echo state	
Vt100 numeric set {OFF=0 ON=1}	Sets numeric mode	
Vt100 numeric show	Shows numeric mode state	
Vt100 reset	Resets terminal	

### Notes

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

### Energy Sensor Table "{energy\_sensor}"

Index	Description	Unit
0	Forward Active Energy	Wh
1	Power Active	W
2	Voltage	V
3	Current	A
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	Forward Active Energy Resettable	Wh
10	Forward Reactive Energy	VARh
11	Forward Reactive Energy Resettable	VARh
12	Reset Time – sec. Since last Energy Counter Rest	s
13	Reverse Active Energy	Wh
14	Reverse Reactive Energy	VARh
15	Reverse Active Energy Resettable	Wh
16	Reverse Reactive Energy Resettable	VARh
17	Absolute Active Energy	Wh
18	Absolute Reactive Energy	VARh
19	Absolute Active Energy Resettable	Wh
20	Absolute Reactive Energy Resettable	VARh
21	Residual Current	A



Whether the measured values "Residual Current" and "Neutral Current" are supported depends on the respective device model.

## External Sensor Type Table "{sen\_type}"

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

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

## External Sensor Field Table "{sen\_field}"

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

### 4.8 Modbus TCP

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

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



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



All calculations in this chapter are based on addresses starting at "0". 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!

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

## Address Range:

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

These functions are supported:

- Read Coils (0x01)

Reads the state of the ports (relay):

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

Response Code	1 Byte	0x01
Byte count	1 Byte	n
Coil Status	n Byte	each Bit represents a state

- Read Discrete Inputs (0x02)

Reads state informations:

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

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

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

- Write Single Coil (0x05)

Sets the state of a port (relay):

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

Response Code	1 Byte	0x05
Output Address	2 Bytes	n

- Write Multiple Coils (0x0F)

Sets the state of several ports (relays):

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

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

- Read Input Registers (0x04)

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

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

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



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

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

### External Sensors:

The measured value of the external sensors is 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):

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

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

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

### Energy Sensors:

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

Line:  $0x0400 + \text{Line} * 0x120 + \text{Phase} * 0x60 + \text{Offset} * 2$   
 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
12	Reset Time - sec. since last Energy Counter Reset	s
13	Forward Active Energy	Wh
14	Forward Reactive Energy	VARh
15	Forward Active Energy Resettable	Wh
16	Forward Reactive Energy Resettable	VARh
17	Reverse Active Energy	Wh
18	Reverse Reactive Energy	VARh
19	Reverse Active Energy Resettable	Wh
20	Reverse Reactive Energy Resettable	VARh
21	Residual Current Type A	mA
22	Neutral Current	mA
23	Residual Current Type B RMS	0.1 mA
24	Residual Current Type B DC	0.1 mA



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

- Read Device Identification (0x2B / 0x0E)

Returns manufacturer name and device identification:

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

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

#### 4.9 Messages

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

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

#### E-mail messages

E-mail messages are triggered by the following events:

- Turning on the device
- Exceeding of the max / min values of attached sensors
- State change of digital sensor input ports
- Exceeding of max / min values of the measured power consumption
- Exceeding max / min values of residual current type A

## 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:

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

## 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
- Exceeding of the max / min values of attached sensors
- State change of digital sensor input ports
- Exceeding of max / min values of the measured power consumption
- Exceeding max / min values of residual current type A

## 5. Support

You will find the latest product software on our website at [www.Digitus.info](http://www.Digitus.info) available for download.

### 5.1 Data Security

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

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

## **When accessed from the Internet**

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

## **5.2 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 cannot access the web server, bring the device into bootloader mode and search for it with GBL\_Conf.exe. Then check the TCP-IP parameters and change them if necessary.
- If the device is not found by GBL\_Conf.exe in bootloader mode, you can reset the settings to factory defaults as the last option.

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

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

### **3. Can you enter multiple e-mail recipients?**

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

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

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

### **5. 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).

This is a Class A product. In home environment, this product may cause radio interference. In this case, the user may be required to take appropriate measures.

Hereby Assmann Electronic GmbH declares that the Declaration of Conformity is part of the shipping content. If the Declaration of Conformity is missing, you can request it by post under the below mentioned manufacturer address.

**www.assmann.com**

Assmann Electronic GmbH  
Auf dem Schüffel 3  
58513 Lüdenscheid  
Germany





# Inline Metered PDU, 1U, 1-phasig, 16A, 4 x C20, 4 x C19



**Benutzerhandbuch**

DN-95637

# Inhaltsverzeichnis

<b>1. Gerätebeschreibung</b> .....	<b>4</b>
1.1. Sicherheitserklärung .....	4
1.2. Lieferumfang .....	4
1.3. Beschreibung .....	4
1.4. Anschluss und Inbetriebnahme .....	5
1.5. Hot-Swap Drawer .....	6
1.6. Technische Daten .....	6
1.6.1. Elektrische Messgrößen .....	7
<b>2. Bedienung</b> .....	<b>7</b>
2.1. Bedienung am Gerät .....	7
2.2. Control Panel .....	8
2.3. Maintenance .....	8
2.3.1. Maintenance Seite .....	11
2.3.2. Konfigurationsmanagement ..	12
2.3.3. Bootloader-Aktivierung .....	13
<b>3. Konfiguration</b> .....	<b>15</b>
3.1. Ethernet .....	15
3.1.1. IP Address .....	15
3.1.2. IP ACL .....	17
3.1.3. HTTP .....	18
3.2. Protokolle .....	19
3.2.1. Konsole .....	19
3.2.2. Syslog .....	20
3.2.3. SNMP .....	20
3.2.4. Radius .....	22
3.2.5. Modbus TCP .....	23
3.3. Uhr .....	23
3.3.1. NTP .....	23
3.3.2. Timer .....	24
3.3.3. Timer Konfiguration .....	24
3.4. Sensoren .....	30
3.5. E-Mail .....	32
3.6. Front Panel .....	33
<b>4. Spezifikationen</b> .....	<b>33</b>
4.1. IP ACL .....	33
4.2. IPv6 .....	34
4.3. Radius .....	34
4.4. Automatisierte Zugriffe .....	35
4.5. SNMP .....	36
4.5.1. Device MIB 8341 (DN-95637) .....	38
4.6. SSL .....	40
4.7. Konsole .....	43
4.7.1. Console Cmd 8341 (DN-95637) .....	47
4.8. Modbus TCP .....	55
4.9. Nachrichten .....	60
<b>5. Support</b> .....	<b>60</b>



5.1. Datensicherheit.....	61
5.2. FAQ .....	62
5.3. Konformitätserklärungen .....	63
5.4. Kontakt .....	63

# 1. Gerätebeschreibung

## 1.1 Sicherheitserklärung

- Das Gerät darf nur von qualifiziertem Personal installiert und verwendet werden. Der Hersteller übernimmt keine Haftung für durch die unsachgemäße Verwendung des Geräts entstandene Schäden oder Verletzungen.
- Eine Reparatur des Geräts durch den Kunden ist nicht möglich. Reparaturen dürfen nur durch den Hersteller durchgeführt werden.
- Dieses Betriebsmittel enthält stromführende Teile mit gefährlichen Spannungen und darf nicht geöffnet oder zerlegt werden.
- Das Gerät darf nur an ein 230 Volt Wechselstromnetz (50 Hz oder 60 Hz) angeschlossen werden.
- Die verwendeten Stromkabel, Stecker und Steckdosen müssen sich in einwandfreien Zustand befinden. Für den Anschluss des Geräts an das Stromnetz darf nur eine Steckdose mit ordnungsgemäßer Erdung des Schutzkontaktes eingesetzt werden.
- Dieses Betriebsmittel ist nur für den Innenraumgebrauch konstruiert. Es darf nicht in feuchten oder übermäßig heißen Umgebungen eingesetzt werden.
- Bitte beachten Sie ebenso die Sicherheitshinweise und Bedienungsanleitungen der übrigen Geräte, die an das Gerät angeschlossen werden.
- Das Gerät ist kein Spielzeug. Es darf nicht im Zugriffsbereich von Kindern aufbewahrt oder betrieben werden.
- Verpackungsmaterial nicht achtlos liegen lassen. Plastikfolien/-tüten, Styroportteile etc. könnten für Kinder zu einem gefährlichen Spielzeug werden. Bitte recyceln Sie das Verpackungsmaterial.
- Sollten Sie sich über den korrekten Anschluss nicht im Klaren sein oder sollten sich Fragen ergeben, die nicht durch die Bedienungsanleitung abgeklärt werden, so setzen Sie sich bitte mit unserem Support in Verbindung.
- Schließen Sie nur Elektrogeräte an, die keine eingeschränkte Einschaltdauer haben. D.h. alle angeschlossenen Elektrogeräte müssen im Fehlerfall eine Dauereinschaltung verkraften, ohne Schäden anzurichten.

## 1.2 Lieferumfang

Im Lieferumfang enthalten sind:

- Inline Metered PDU, 1U, 1-phasig, 16A, 4 x C20, 4 x C19
- 1 x Netz-Anschlusskabel (IEC C13, max. 10 A)
- CD-ROM mit Anleitung und Softwaretools

## 1.3 Beschreibung

Der PDU kann auf 4 verschiedenen Phasen (IEC C20 auf IEC C19, max. 16A) die Energiewerte messen. Das Gerät hat folgende Features:

- Energiemessung auf 4 Phasen, so-wie Messung der Größen Spannung, Strom, Wirkleistung, Blindleistung, Scheinleistung, Frequenz, Phasenwinkel und Powerfaktor.
- Energiezähler für alle Phasen jeweils total und rücksetzbar.
- Differenzstrommessung auf allen Phasen.

- Hot-Swap Drawer - Die Geräteelektronik, inklusive Netzteil, kann auf einer Schublade getauscht werden, ohne dass die angeschlossenen Verbraucher abgeschaltet werden müssen.
- Anschluss zweier optionaler externer Sensoren zur Ermittlung der Temperatur und Luftfeuchtigkeit, oder eines Schalteingangs.
- Eine dreistellige 7-Segment LED-Anzeige (für Stromanzeige, externe Sensorwerte, IP-Adresse, Gerätestatus).
- Dual TCP/IP Stack mit IPv4 und IPv6 Unterstützung.
- Steuerung und Überwachung des Geräts über Ethernet mit einem integrierten Webserver mit SSL Verschlüsselung und SNMP (v1, v2c und v3).
- Modbus TCP Support.
- Erzeugung von Nachrichten (E-Mail, Syslog und SNMP Traps) in Abhängigkeit von Grenzwerten der Energiemessung oder der externen Sensoren.
- Konsolensteuerung über Telnet.
- Verschlüsselte E-Mails

## 1.4 Anschluss und Inbetriebnahme

### Anschluss und Bedienelemente auf der Gerätevorderseite



- 1) Aktuelle Stromaufnahme der Phase (7-Segment Anzeige)
- 2) 8 Klartextanzeigen L1 bis L4 als Indikator für Spannung (grüne Anzeige) und welche Phase im Display angezeigt wird (rote Anzeige)
- 3) Status LED
- 4) Taster "Select" und "OK"
- 5) Netzwerkanschluss (RJ45)
- 6) Sensoranschlüsse (RJ45)



- 1) – 4) Lastausgänge für Phasen L1 bis L4 (IEC C19, max. 16 A)

## Anschlüsse auf Geräterückseite



- 1) – 4) Lasteingänge für Phasen L1 bis L4 (IEC C20, max. 16 A)
- 5) Netzanschluss (IEC C14, max. 10 A)

### Inbetriebnahme

- Verbinden Sie das Netz-Anschlusskabel (IEC C14, max. 10A) mit dem Stromnetz.
- Stecken Sie das Netzwerkkabel in die Ethernetbuchse (RJ45).
- Stecken Sie die optionalen externen Sensoren in die Sensoranschlüsse.
- Verbinden Sie die Stromversorgung mit den Lasteingängen (IEC C20, max. 16 A), und die Verbraucher mit den Lastausgängen (IEC C19, max. 16A). Die Zuleitungsstecker sind von der Bauart her gegen unbeabsichtigtes Lösen gesichert. Sie müssen bis zum Anschlag eingesteckt werden, sonst besteht keine sichere Verbindung. Der Stecker darf nicht in der Buchse wackeln, ansonsten ist der Stecker noch nicht bis zum Anschlag eingesteckt.

### 1.5 Hot-Swap Drawer

Diese PDU ist "Hot-Swap" fähig. Das Gerät verfügt über eine herausnehmbare Schublade, auf der sich die gesamte aktive Elektronik, inklusive des Netzteils, befindet. Im Falle eines Defekts können Sie beim Hersteller eine Ersatzelektronik bestellen. Die an den Messports angeschlossenen Geräte werden beim Austausch nicht gestört. Eine genaue Anleitung zum Tausch der Elektronikschublade erhalten Sie mit der Austauschelektronik. Öffnen Sie die Schublade nicht ohne zwingenden Grund, dies kann zum Garantieverlust führen.

### 1.6 Technische Daten

<b>Anschlüsse</b>	1 x Ethernetanschluss (RJ45) 1 x Netzanschluss (IEC C14, max. 10 A) 4 x Lasteingänge (IEC C20, max. 16 A) 4 x Lastausgänge (IEC C19, max. 16 A) 2 x RJ45 für externen Sensor
<b>Netzwerkanbindung</b>	10/100 Mbit/s 10baseT Ethernet
<b>Protokolle</b>	TCP/IP, HTTP/HTTPS, SNMP v1/v2c/v3, SNMP traps, Syslog, E-Mails (SMTP)
<b>Spannungsversorgung</b>	Internes Netzteil (90 - 265 V AC / -15%/+10%)

<b>Umgebung</b>	
· <b>Betriebstemperatur</b>	0 °C – 50 °C
· <b>Lagertemperatur</b>	-20 °C – 70 °C
· <b>Luftfeuchtigkeit</b>	0% - 95 % (nicht kondensierend)
<b>Gehäuse</b>	Pulverbeschichtetes, verzinktes Stahlblech
<b>Maße</b>	19 Zoll, 1 HE (Tiefe 195 mm)
<b>Gewicht</b>	ca. 3.3 kg

### 1.6.1 Elektrische Messgrößen

Elektrische Messgrößen				
Messwert	Bereich	Einheit	Auflösung	Ungenauigkeit (typisch)
Spannung (voltage)	90 – 265	V	0.01	< 1 %
Strom (current)	0 – 16	A	0.001	< 1.5 %
Frequenz (frequency)	45 – 65	Hz	0.01	< 0.03 %
Phasenwinkel (phase)	-180 – +180	°	0.1	< 1 %
Wirkleistung (active power)	0 – 4000	W	1	< 1.5 %
Blindleistung (reactive power)	0 – 4000	Var	1	< 1.5 %
Scheinleistung (apparent power)	0 – 4000	VA	1	< 1.5 %
Powerfaktor (PF)	0 – 1	-	0.01	< 3 %
Energiezähler				
Wirkenergie (total)	9.999.999,999	kWh	0.001	< 1.5 %
Wirkenergie (temporary)	9.999.999,999	kWh	0.001	< 1.5 %

## 2. Bedienung

### 2.1 Bedienung am Gerät

#### Stromanzeige

Ist die Stromanzeige im Display (7-Segment Anzeige) aktiviert (siehe Konfiguration - Sensoren), dann werden nacheinander die Strommesswerte aller Phasen wiedergegeben. Wird keine Spannung gemessen (kleiner 70 V), werden drei Striche angezeigt, und die grünen

Klartextanzeigen L1 bis L4 leuchten nicht. Die roten Klartextanzeigen L1 bis L4 symbolisieren, welche Phase im Display gerade gezeigt wird

### Phase selektieren

Durch wiederholtes Betätigen des "Select" Tasters kann die Phase manuell angewählt werden, die im Display erscheinen soll. Nach ca. 60 Sekunden wird der Durchlauf aller Phasen wieder fortgesetzt.

### Anzeigeinformationen

Ist keine Phase selektiert, werden durch wiederholtes Drücken des "OK" Tasters nach-einander die IP-Adresse und die Werte der externen Sensoren im Display (7-Segment Anzeige) dargestellt.

### Status-LED

Die Status-LED zeigt verschiedene Zustände direkt am Gerät an:

- rot: Das Gerät ist nicht mit dem Ethernet verbunden.
- orange: Das Gerät ist mit dem Ethernet verbunden und wartet auf die Antwort vom DHCP-Server.
- grün: Das Gerät ist mit dem Ethernet verbunden, und die TCP/IP Einstellungen wurden vorgenommen.
- regelmäßig blinkend: Das Gerät befindet sich im Bootloader-Modus.

## 2.2 Control Panel

Rufen Sie das Webinterface unter <http://IP-Adresse> auf und loggen Sie sich ein.

Control Panel														
Configuration Maintenance Logout														
Id	Line Name	Voltage AC rms V	Current AC rms A	Freq Hz	Phase *	active W	reactive VAR	apparent VA	PF	Residual Current AC rms mA	total Energy active kWh	resettable Energy active kWh	time h:m:s	Reset
I1	Meter1	229,3	3,326	50,00	0,0	763	-2	763	1,00	2,7	0,142	0,142	00:15:57	Reset
I2	Meter2	229,3	0,000	50,00	-94,5	0	0	0	1,00	0,0	0,005	0,005	00:15:57	Reset
I3	Meter3	227,6	0,000	50,00	137,9	0	0	0	1,00	0,0	0,005	0,005	00:15:57	Reset
I4	Meter4	8,8	0,000	50,00	-57,3	0	0	0	1,00	0,0	0,006	0,006	00:15:57	Reset
sum		3,326				763				0,0				

auto logout in 219s

Die Webseite bietet einen Überblick über die Messwerte aller Phasen, sowie der angeschlossenen Sensoren.



Die Spalte "Residual Current" wird nur bei Modellen mit Differenzstrommessung angezeigt.

## 2.3 Maintenance

Die aktuelle Gerätegeneration mit IPv6 und SSL erlaubt es alle Wartungsfunktionen im Webinterface auf der Maintenance Seite durchzuführen.

### Maintenance im Webinterface

Folgende Funktionen sind aus der Maintenance Webseite abrufbar:

- Firmware Update
- Ändern des SSL-Zertifikats
- Laden und Speichern der Konfiguration
- Neustart des Geräts
- Wiederherstellung des Werkzustand
- Sprung in den Bootloader
- Löschen des DNS-Cache

### **Aktualisierung von Firmware, Zertifikat oder Konfiguration**

Auf der Maintenance Webseite in den Sektionen "Firmware Update", "SSL Certificate Upload" oder "Config Import File Upload" mit "Browse.." die gewünschte Datei auswählen und "Upload" drücken. Die Datei wird nun auf den Updatebereich des Geräts übertragen und der Inhalt überprüft. Erst jetzt führt ein Druck auf "Apply" mit einem Gerätereustart endgültig die Aktualisierung der Daten durch, oder wird mit "Cancel" abgebrochen.



Es kann mit einem Neustart jeweils nur eine Upload-Funktion initiiert werden, man kann z.B. nicht gleichzeitig Firmware und Konfiguration übertragen.



Wenn nach einem Firmware-Update die Webseite nicht mehr korrekt dargestellt wird, kann das am Zusammenspiel von Javascript und einem veralteten Browser-Cache liegen. Sollte die Tastenkombination Strg mit F5 nicht helfen, empfiehlt es sich, in den Browser Optionen den Cache manuell zu löschen. Eine weitere Möglichkeit besteht darin, den Browser im "Privaten Modus" zu starten.



Bei einem Firmware-Update werden manchmal auch alte Datenformate zu neuen Strukturen konvertiert. Wird eine ältere Firmware neu eingespielt kann es zu Verlust der Konfigurationsdaten und der Energiezähler kommen! Sollte das Gerät dann nicht einwandfrei laufen, bitte den Werkzustand (Fab-Settings) wiederherstellen (z.B. von der Maintenance Seite).

### **Aktionen im Bootloader-Modus**

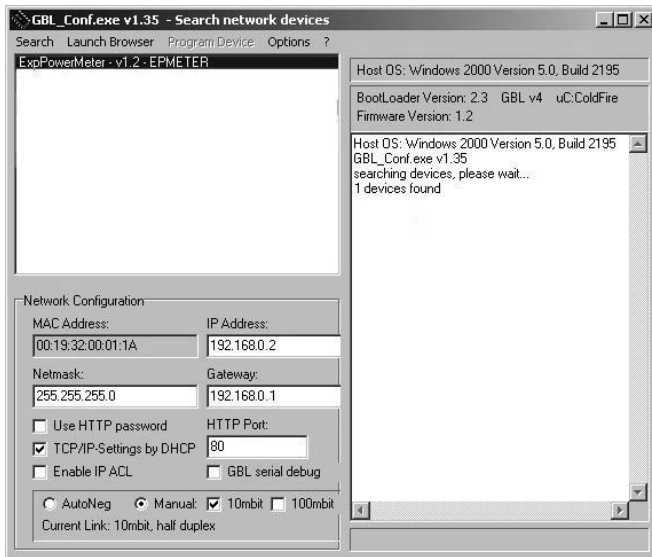
Falls das Webinterface des Geräts nicht mehr erreichbar ist, so kann das Gerät in den Bootloader-Modus gebracht werden (siehe Kapitel Bootloader-Aktivierung). Dort lassen sich mit Hilfe der Applikation "GBL\_Conf.exe" folgende Funktionen ausführen:

- Setzen von IPv4-Adresse, Netzmaske, Gateway
- Ein- und Ausschalten des HTTP-Passworts
- Ein- und Ausschalten der IP-ACL
- Wiederherstellung des Werkzustands
- Neustart des Geräts



Bei Geräten mit Relais, verändert ein Betreten oder Verlassen des Bootloader Modus nicht den Zustand der Relais, solange die Betriebsspannung erhalten bleibt.

Das Programm "GBL\_Conf.exe" ist kostenlos auf unserer Webseite [www.Digitus.info](http://www.Digitus.info) erhältlich und befindet sich auch auf der beiliegenden CD-ROM.



Oberfläche GBL\_Conf


Starten Sie das Programm und gehen Sie nun im Programm im Menü "Search" auf "All Devices". Aus der angezeigten Liste können Sie das entsprechende Gerät auswählen. Im unteren Teil der linken Hälfte des Programmfensters werden nun die aktuellen Netzwerkeinstellungen des Geräts angezeigt. Handelt es sich bei der angezeigten IP-Adresse um die Werkseinstellung (192.168.0.2), ist entweder kein DHCP-Server im Netzwerk vorhanden oder es konnte keine freie IP-Adresse vergeben werden.

- Aktivieren Sie den Bootloader-Modus (siehe Kapitel Bootloader Modus) und wählen Sie in "Search" den Punkt "Bootloader-Mode Devices" auf.
- Geben Sie im Eingabefenster die gewünschten Einstellungen ein und speichern Sie die Änderungen bei "Program Device" im Menüpunkt "Save Config".
- Deaktivieren Sie den Bootloader-Modus, damit die Änderungen wirksam werden. Rufen Sie nun im Programm unter "Search" die Funktion "All Devices" auf.

Die neue Netzwerkkonfiguration wird jetzt angezeigt.

### Werkzustand

Das Gerät lässt sich per Webinterface von der Maintenance Seite oder aus dem Bootloader-Modus (siehe Kapitel Bootloader-Aktivierung) in den Werkzustand zurückversetzen. Dabei werden sämtliche TCP/IP Einstellungen zurückgesetzt.

 Ein Firmware-Update oder ein hochgeladenes Zertifikat bleiben erhalten, wenn man das Gerät in den Werkzustand versetzt.



### 2.3.1 Maintenance Seite

Diese Sektion ermöglicht den Zugriff auf wichtige Funktionen wie Firmware-Update oder den Neustart des Geräts. Es empfiehlt sich aus diesem Grunde ein HTTP-Passwort zu setzen.

The screenshot shows the 'Maintenance' page of a control panel. At the top, there are four tabs: 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. The 'Maintenance' tab is active. Below the tabs, there are four main sections, each with a title and a set of buttons:

- Firmware Update:** Contains a 'Browse...' button and an 'Upload' button. The text 'No file selected.' is displayed between the buttons.
- SSL Certificate Upload:** Contains a 'Browse...' button and an 'Upload' button. The text 'No file selected.' is displayed between the buttons.
- Config Import File Upload:** Contains a 'Browse...' button and an 'Upload' button. Below these buttons is a link for 'Config File Export'.
- Restart / Fab-Settings:** Contains four buttons: 'Restart Device', 'Restore Fab Settings and Restart Device', 'Enter Bootloader Mode', and 'Flush DNS Cache'.

Firmware Update: Führt ein Firmware-Update durch.

SSL Certificate Upload: Speichert ein eigenes SSL Zertifikat ab. Siehe das Kapitel „SSL“ für die Generierung eines Zertifikats im richtigen Format.

Config Import File Upload: Lädt eine neue Konfiguration aus einer Textdatei. Für das Setzen der neuen Konfiguration muss nach dem „Upload“ ein Neustart durch „Restart Device“ durchgeführt werden.

Config File Export: Speichert die aktuelle Konfiguration in einer Textdatei.



Das Speichern der Konfiguration sollte nur in einer SSL Verbindung durchgeführt werden, da dort auch Passwortinformationen (wenn auch nur verschlüsselt oder als Hash) enthalten sind.

Restart Device: Startet das Gerät neu, ohne den Zustand der Relais zu verändern.



Manche Funktionen wie z.B. ein Firmware-Update oder das Ändern der IP- bzw. HTTP-Einstellungen erfordern einen Neustart des Gerätes. Ein Sprung in den Bootloader, oder ein Neustart des Geräts führen in keinem Fall zu einer Änderung der Relaiszustände.

Restore Fab Settings and Restart Device: Führt einen Neustart aus und setzt das Gerät in den Werkzustand.

Enter Bootloader Mode: Springt in den Bootloader-Modus, in welchem mit "Gbl\_Conf.exe" Einstellungen vorgenommen werden können.

Flush DNS Cache: Alle Einträge im DNS-Cache werden verworfen und Adressauflösungen werden neu angefordert.


### 2.3.2 Konfigurationsmanagement

Die Gerätekonfiguration lässt sich im Maintenance Bereich speichern und wiederherstellen.



The screenshot shows a web interface for configuration management. At the top, it says "Config Import File Upload". Below this, there is a "Browse..." button, the text "No file selected.", and an "Upload" button. Below this section, there is a section for "Config File Export".

Durch die Funktion "Config File Export" kann die aktuelle Konfiguration als Textdatei gespeichert werden. Die verwendete Syntax in der Konfigurationsdatei entspricht den Befehlen der Telnet Konsole. Soll die Konfiguration eines Gerätes aus einer Textdatei wiederhergestellt werden, so muss erst die Datei mit "Upload" hochgeladen und dann das Gerät mittels "Restart Device" neu gestartet werden.

 Das Speichern der Konfiguration sollte nur in einer SSL Verbindung durchgeführt werden, da dort auch Passwortinformationen (wenn auch nur verschlüsselt oder als Hash) enthalten sind. Aus den gleichen Gründen ist bei einer Archivierung zu einem sorgfältigen Umgang mit den erzeugten Konfigurationsdateien zu raten.

### Anpassung der Konfigurationsdatei

Es ist möglich, eine gespeicherte Konfigurationsdatei mit einem Texteditor den eigenen Bedürfnissen anpassen. Ein Szenario wäre z.B., mit Hilfe einer Skriptsprache automatisiert viele angepasste Versionen einer Konfiguration zu erzeugen, um dann eine hohe Anzahl von Geräten mit einer individualisierten Konfiguration auszustatten. Auch lassen sich Upload und Neustart mit Hilfe von CGI Kommandos in Skriptsprachen durchführen. Mit dem Kommentarzeichen "#" lassen sich schnell einzelne Befehle ausblenden, oder persönliche Anmerkungen hinzufügen.

Modifiziert man eine Konfigurationsdatei per Hand, ist es nicht immer klar, welche Grenzen für Parameter erlaubt sind. Nach einem Upload und Neustart werden Befehle mit unzulässigen Parametern ignoriert. Daher beinhaltet die erzeugte Konfiguration Kommentare, die die Grenzen der Parameter beschreiben. Dabei bezieht sich "range:" auf eine numerische Werte, und "len:" auf Textparameter. Z.B:

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

Der Befehl "system fabsettings" am Anfang einer generierten Konfigurationsdatei bringt das Gerät in den Werkzustand und führt dann die einzelnen Befehle aus, die den Konfigurationszustand verändern. Es kann wünschenswert sein, die Änderungen relativ zur aktuellen Konfiguration und nicht aus dem Werkzustand heraus vorzunehmen. Dann sollten die "system fabsettings" entfernt werden.

### **Kein Ausgabe der Default-Werte**

Die Konfigurationsdatei enthält (mit Ausnahmen) nur Werte die vom Default abweichen. Der Befehl "system fabsettings" (gehe zu Werkzustand) vom Anfang einer erzeugten Konfigurationsdatei darf deshalb nicht entfernt werden, ansonsten wird das Gerät unter Umständen nur unvollständig konfiguriert.

### **Konfiguration über Telnet**

Die Konfigurationsdateien lassen sich im Prinzip auch in einer Telnet-Session übertragen, allerdings findet dann die Änderung der Einstellungen im laufenden Betrieb statt, und nicht vollständig beim Neustart, wie es beim Upload der Fall gewesen wäre. Es kann dann passieren, dass gleichzeitig Ereignisse ausgelöst werden, während das Gerät konfiguriert wird. Man sollte daher folgendes Vorgehen wählen:

- a) Funktion deaktivieren
- b) Vollständig parametrisieren
- c) Funktion wieder aktivieren

Ein Beispiel:

```
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-Aktivierung**

Die Konfiguration des Gerätes mit der Anwendung "GBL\_Conf.exe" ist nur möglich, wenn sich das Gerät im Bootloader-Modus befindet.

#### **Aktivierung des Bootloader-Modus**

- 1) Per Taster:
  - Halten Sie beide Taster für 3 Sekunden gedrückt.
- 2) oder
  - Entfernen Sie die Betriebsspannung
  - Halten Sie den "Select" Taster gedrückt
  - Verbinden Sie die Betriebsspannung

- 3) Per Software: (nur wenn vorher "Enable FW to BL" in der Anwendung "GBL\_Conf.exe" aktiviert wurde)
  - Starten Sie die Applikation "GBL\_Conf.exe"
  - Führen Sie mit "Search" eine Netzwerksuche aus
  - Aktivieren Sie unter "Program Device" den Menüpunkt "Enter Bootloader"
- 4) Per Webinterface:
  - Drücken Sie "Enter Bootloader Mode" auf der Maintenance Webseite.

Ob sich das Gerät im Bootloader-Modus befindet, erkennen Sie am Blinken der Status LED, oder im Programm "GBL\_Conf.exe" bei einer erneuten Gerätesuche an dem Zusatz „BOOT-LDR“ hinter dem Gerätenamen. Im Bootloader-Modus lassen sich mit Hilfe von "GBL\_Conf.exe" das Passwort und die IP ACL deaktivieren, ein Firmware-Update durchführen sowie der Werkzustand wiederherstellen.



Bei Geräten mit Relais, verändert ein Betreten oder Verlassen des Bootloader Modus nicht den Zustand der Relais, solange die Betriebsspannung erhalten bleibt.

### **Verlassen des Bootloader Modus**

1. Per Taster:
  - Halten Sie beide Taster für 3 Sekunden gedrückt
2. oder
  - Entfernen und verbinden Sie die Betriebsspannung ohne einen Taster zu betätigen
3. Per Software:
  - Starten Sie die Applikation "GBL\_Conf.exe"
  - Führen Sie mit "Search" eine Netzwerksuche aus
  - Aktivieren Sie unter "Program Device" den Menüpunkt "Enter Firmware"

### **Werkzustand**

Wenn sich das Gerät im Bootloader-Modus befindet, lässt es sich jederzeit in den Werkzustand zurückversetzen. Dabei werden sämtliche TCP/IP Einstellungen zurückgesetzt.



Ein Firmware-Update oder ein hochgeladenes Zertifikat bleiben erhalten, wenn man das Gerät in den Werkzustand versetzt.

- 1) Per Taster:
  - Aktivieren Sie dazu den Bootloader-Modus des Geräts
  - Halten Sie den "Select" Taster für 6 Sekunden gedrückt.
  - Die Status LED blinkt nun in schnellem Rhythmus, bitte warten Sie, bis die LED wieder langsam blinkt (ca. 5 Sekunden)

2) Per Taster:

- Aktivieren Sie dazu den Bootloader-Modus des Geräts
- Starten Sie das Programm "GBL\_Conf.exe"
- Wählen Sie nun unter "Program Device" den Menüpunkt "Reset to Fab Settings"
- Die Status LED blinkt nun in schnellem Rhythmus, warten Sie, bis die LED wieder langsam blinkt (ca. 5 Sekunden)

### 3. Konfiguration

#### Automatische Konfiguration per DHCP

Nach dem Einschalten sucht das Gerät im Ethernet einen DHCP-Server und fordert bei diesem eine freie IP-Adresse an. Prüfen Sie in den Einstellungen des DHCP-Servers, welche IP-Adresse zugewiesen wurde und stellen Sie gegebenenfalls ein, dass dieselbe IP-Adresse bei jedem Neustart verwendet wird. Zum Abschalten von DHCP verwenden Sie die Software GBL\_Conf.exe oder nutzen Sie die Konfiguration über das Webinterface.

Starten Sie das Programm und gehen Sie auf "Search -> All Devices". Aus der angezeigten Liste können Sie das entsprechende Gerät auswählen. Im unteren Teil der linken Hälfte des Programmfensters werden nun die aktuellen Netzwerkeinstellungen des Geräts angezeigt. Handelt es sich bei der angezeigten IP-Adresse um die Werkseinstellung (192.168.0.2), ist entweder kein DHCP-Server im Netzwerk vorhanden oder es konnte keine freie IP-Adresse vergeben werden.

#### 3.1 Ethernet

##### 3.1.1 IP Adresse

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

---

**Hostname**

• Hostname:

---

**IPv4**

• Use IPv4 DHCP:  yes  no

• IPv4 Address:

• IPv4 Netmask:

• IPv4 Gateway address:

• IPv4 DNS address:

---

**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: Hier kann ein Name mit maximal 63 Zeichen vergeben werden. Mit diesem Namen erfolgt die Anmeldung beim DHCP-Server.



Sonderzeichen oder Umlaute im Hostnamen können zu Problemen im Netzwerk führen.

IPv4 Address: Die IP-Adresse des Gerätes.

IPv4 Netmask: Die Netzmaske im verwendeten Netz.

IPv4 Gateway address: Die IP-Adresse des Gateway.

IPv4 DNS address: Die IP-Adresse des DNS-Servers.

Use IPv4 DHCP: Wählen Sie "yes", wenn die TCP/IP-Einstellungen direkt vom DHCP-Server bezogen werden sollen. Bei aktivierter Funktion wird nach jedem Einschalten geprüft, ob ein DHCP-Server im Netz vorhanden ist. Wenn nicht, wird die zuletzt genutzte Einstellung weiterverwendet.

Use IPv6 Protocol: Aktiviert das IPv6 Protokoll.

Use IPv6 Router Advertisement: Das Router Advertisement kommuniziert mit dem Router, um globale IPv6-Adressen zugänglich zu machen.

Use DHCP v6: Fordert von einem vorhandenen DHCP-v6-Server die Adressen der konfigurierten DNS-Server an.

Use manual IPv6 address settings: Aktiviert die manuelle Eingabe von IPv6-Adressen.

IPv6 status: Zeigt die IPv6-Adressen, über die das Gerät erreichbar ist, sowie DNS Server und Router.

```
IPv6 status
• Current IPv6 status:
IPv6 Addr:
fe80::219:32ff:fe00:996d
2007:7dd0:ffc1:1:219:32ff:fe00:996d
IPv6 DNS Server:
2007:7dd0:ffc1:1:20c:29ff:feaf:93c
IPv6 Router:
fe80::20c:29ff:feaf:93c
```



Für IP-Änderungen ist ein Neustart der Firmware notwendig. Dies kann im Maintenance Bereich vorgenommen werden. Ein Neustart des Geräts führt in keinem Fall zu einer Änderung der Relaiszustände.

## Manuelle IPv6 Konfiguration

**IPv6 (manual)**

- IPv6 Addresses:  / 64  
 / 64  
 / 64  
 / 64
- IPv6 DNS addresses:
- IPv6 Gateway address:

Die Eingabefelder für das manuelle Setzen von IPv6-Adressen erlauben das Konfigurieren des Prefix von vier zusätzlichen IPv6 Geräteadressen, sowie die Angabe von zwei DNS-Adressen und einem Gateway.

### 3.1.2 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:f12"/>	<input type="button" value="Delete"/>	<input type="button" value="Add"/>
2. Grant IP access to host/net:	<input type="text" value="192.168.1.84"/>	<input type="button" value="Delete"/>	<input type="button" value="Add"/>
3. Grant IP access to host/net:	<input type="text" value="mypc.loddom"/>	<input type="button" value="Delete"/>	<input type="button" value="Add"/>
4. Grant IP access to host/net:	<input type="text" value="192.168.1.0/24"/>	<input type="button" value="Delete"/>	<input type="button" value="Add"/>
5. Grant IP access to host/net:	<input type="text" value="1234:4ef0:eec1:0::/64"/>	<input type="button" value="Delete"/>	<input type="button" value="Add"/>

Reply ICMP ping requests: Wenn Sie diese Funktion aktivieren, antwortet das Gerät auf ICMP-Pings aus dem Netzwerk.

Enable IP filter: Aktivieren oder deaktivieren Sie hier den IP-Filter. Der IP-Filter stellt eine Zugriffskontrolle für eingehende IP-Pakete dar.



Bitte beachten Sie, dass bei aktivierter IP-Zugriffskontrolle HTTP und SNMP nur dann funktionieren, wenn die entsprechenden Server und Clients in der IP Access Control List eingetragen sind.



Sollten Sie sich hier aus Versehen „ausgesperrt“ haben, aktivieren Sie den Bootloader-Modus und deaktivieren Sie mit Hilfe des Programms "GBL\_Conf.exe" die IP ACL. Als Alternative können Sie das Gerät in den Werkzustand zurücksetzen.

### 3.1.1.3 HTTP

IP Address · IP ACL · HTTP Server

**HTTP**

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

**HTTP Password**

- Enable password protection:  yes  no
- 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:

HTTP Server option: Selektiert ob Zugriff nur mit HTTP, HTTPS oder beidem möglich ist.

Server port HTTP: Hier kann die Portnummer des internen HTTP-Servers eingestellt werden. Möglich sind Werte von 1 bis 65534 (Standard: 80). Um auf das Gerät zugreifen zu können müssen Sie die Portnummer an die Adresse mit einem Doppelpunkt anhängen, wie z.B.: "http://192.168.0.2:800"

Server port HTTPS: Die Portnummer für die Verbindung des Webservers über das SSL (TLS) Protokoll.

Enable Ajax autorefresh: Ist dies aktiviert, so werden in der Statusseite die Informationen automatisch per HTTP-Request aktualisiert.



Für manche HTTP-Änderungen ist ein Neustart der Firmware notwendig. Dies kann im Maintenance Bereich vorgenommen werden. Ein Neustart des Geräts führt in keinem Fall zu einer Änderung der Relaiszustände.


Enable password protection: Auf Wunsch kann der Passwort-Zugangsschutz aktiviert werden. Wenn das Admin-Passwort vergeben ist, können Sie sich nur unter Eingabe dieses Passworts einloggen um Einstellungen zu ändern. User können sich unter Eingabe des User-Passworts einloggen um die Status-Informationen abzufragen und Schaltvorgänge auszulösen.


Use radius server passwords: Username und Passwort werden von einem Radius Server validiert.

Use locally stored passwords: Username und Passwort werden lokal gespeichert. In diesem Fall müssen ein Admin-Passwort und ein User-Passwort vergeben werden. Das Passwort darf



maximal 31 Zeichen besitzen. In der Passwordeingabemaske des Browsers sind für den Usernamen "admin" und "user" vorgesehen. Im Werkzustand ist als Default das Passwort für den Admin auf "admin" gesetzt bzw. "user" für das User Passwort.

 Wird die Passwort-Eingabemaske neu angezeigt, so gelten die vier "Kreise" nur als symbolischer Platzhalter, da aus Sicherheitsgründen auf dem Gerät nie das Passwort selber, sondern nur der SHA2-256 Hash abgespeichert wird. Möchte man das Passwort ändern, so muss immer das vollständige Passwort neu eingegeben werden.

 Sollten Sie das Passwort vergessen haben, aktivieren Sie den Bootloader-Modus und deaktivieren Sie dann die Passwortabfrage mit der SoftwareGBL\_Conf.exe.

## 3.2 Protokolle

### 3.2.1 Konsole

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

**Telnet Console**

- Enable Telnet:  yes  no
- Telnet TCP port:
- Raw mode:  yes  no
- Activate echo:  yes  no
- Active negotiation:  yes  no
  
- Require user login:  yes  no
  - Delay after 3 failed logins:  yes  no
  - use radius server passwords:  yes  no
  - use locally stored passwords:  yes  no
- Username:
- Set new password:  (32 characters max)
- Repeat password:

Enable Telnet: Aktiviert die Telnet Konsole.

Telnet TCP port: Port auf dem Telnet Sitzungen angenommen werden.

Raw mode: Die VT100 Editierfunktionen und das IAC Protokoll sind deaktiviert.

Activate echo: Die Echo-Einstellung, wenn nicht durch IAC geändert.

Active negotiation: Die IAC Aushandlung wird vom Server initiiert.

Require user login: Es werden Username und Passwort verlangt.

Delay after 3 failed logins: Nach 3 Fehleingaben von Username oder Passwort, muss auf den nächsten Loginversuch gewartet werden.

Use radius server passwords: Username und Passwort werden von einem Radius Server validiert.

Use locally stored passwords: Username und Passwort werden lokal gespeichert.

### 3.2.2 Syslog

Console · Syslog · SNMP · Radius · Modbus

**Syslog**

- Enable Syslog:  yes  no
- Syslog server:

Apply

Enable Syslog: Hier können Sie einstellen, ob die Syslog-Informationen über das Netzwerk weitergegeben werden sollen.

Syslog Server: Wenn Sie den Punkt Enable Syslog aktiviert haben, tragen Sie hier die IP-Adresse des Servers ein, an den die Syslog-Informationen übertragen werden sollen.

### 3.2.3 SNMP

Console · Syslog · SNMP · Radius · Modbus

**SNMP**

- Enable SNMP options:  SNMP get  SNMP set
- SNMP UDP port:

**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: Aktiviert die Annahme von SNMP-get Kommandos.

SNMP-set: Erlaubt die Ausführung von SNMP-set Befehlen.

SNMP UDP Port: Setzt den UDP Port auf dem SNMP Nachrichten empfangen werden.

Enable SNMP v2: Aktiviert SNMP v2.



Aufgrund von Sicherheitsaspekten empfiehlt es sich nur SNMP v3 zu nutzen, und SNMP v2 abzuschalten, da auf SNMP v2 nur unsicher zugegriffen werden kann.

Community public: Das Passwort für die SNMP-get Arbeitsgruppe.

Community private: Das Passwort für die SNMP-set Arbeitsgruppe.

Enable SNMP v3: Aktiviert SNMP v3.

SNMP v3 Username: Der SNMP v3 Benutzername.

SNMP v3 Authorization Algorithm: Der ausgewählte Authentifizierungs Algorithmus.

SNMP v3 Privacy Algorithm: Die SNMP v3 Verschlüsselung.



Wird die Passwort Eingabemaske neu angezeigt, so gelten die vier "Kreise" nur als symbolischer Platzhalter, da aus Sicherheitsgründen auf dem Gerät nie das Passwort selber, sondern nur der mit Hilfe des Authorization Algorithm gebildete Schlüssel gespeichert wird. Möchte man das Passwort ändern, so muss immer das vollständige Passwort neu eingegeben werden.



Die Berechnung der Passwort Hashes ändert sich mit den eingestellten Algorithmen. Werden die Authentication oder Privacy Algorithmen geändert, müssen im Konfigurationsdialog die Passwörter wieder neu eingegeben werden. "SHA-384" und "SHA-512" werden rein in Software berechnet. Wird auf der Konfigurationsseite "SHA-512" eingestellt, können einmalig bis zu ca. 45 Sekunden für die Schlüsselerzeugung vergehen. Send SNMP traps: Here you can specify whether, and in what format the device should send SNMP traps.

Send SNMP traps: Hier können Sie festlegen ob, und in welchem Format das Gerät SNMP-traps versenden soll.

SNMP trap receiver: Man kann hier bis zu acht SNMP Trap Empfänger einfügen.

MIB table: Der Download Link zur Textdatei mit der MIB-Table für das Gerät.

### 3.2.4 Radius

Console · Syslog · SNMP · Radius · Modbus

**Radius**

- Enable Radius Client:  yes  no
- Use CHAP:  yes  no
- 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: Aktiviert die Validierung über Radius.

Use CHAP: Benutze CHAP Passwort Kodierung.

Use Message Authentication: Fügt das "Message Authentication" Attribut zum Authentication Request hinzu.

Primary Server: Name oder IP-Adresse des Primary Radius server.

Shared secret: Radius Shared Secret. Aus Kompatibilitätsgründen nur ASCII Zeichen verwenden.

Timeout: Wie lange (in Sekunden) auf eine Antwort von einem Authentication Request gewartet wird.

Retries: Wie oft ein Authentication Request nach einem Timeout wiederholt wird.

Use Backup Server: Aktiviert einen Radius Backup Server.

Backup Server: Name oder IP-Adresse des Radius Backup server.

Shared secret: Radius Shared Secret. Aus Kompatibilitätsgründen nur ASCII Zeichen verwenden.

Timeout: Wie lange (in Sekunden) auf eine Antwort von einem Authentication Request gewartet wird.

Retries: Wie oft ein Authentication Request nach einem Timeout wiederholt wird.

**Test Radius Server**

• Test Username:

• Test Password:

Test Username: Username Eingabefeld für Radius Test.

Test Password: Passwort Eingabefeld für Radius Test.

Die "Test Radius Server" Funktion ermöglicht die Überprüfung, ob eine Kombination von Username und Passwort von den konfigurierten Radius Servern akzeptiert würde.

### 3.2.5 Modbus TCP

Console · Syslog · SNMP · Radius · Modbus

**Modbus TCP**

• Enable Modbus TCP:  yes  no

• Modbus TCP port:

Enable Modbus TCP: Aktiviert Modbus TCP Unterstützung

Modus TCP port: Die TCP/IP Portnummer für Modbus TCP.

## 3.3 Uhr

### 3.3.1 NTP

NTP · Timer

**NTP**

Enable Time Synchronisation:  yes  no

Primary NTP server:

· reply 21s ago, 11ms signal delay  
· Tue Feb 19 2019 16:50:33 GMT+0100 (Central European Standard Time)

Backup NTP server:

**Timezone:**

Timezone:  ▾

Daylight Saving Time (DST):  yes  no

**Clock**

Current Systemtime (UTC): 15:50:54 19.02.2019 (1550591454)

Current Localtime: 16:50:54 19.02.2019

Browsertime: 16:50:54 19.02.2019

Set clock:

Enable Time Synchronization: Schaltet das NTP Protokoll ein.

Primary NTP server: IP-Adresse des ersten NTP Servers.

Backup NTP server: IP-Adresse des zweiten NTP Servers. Wird genutzt, wenn der erste NTP Server sich nicht meldet.

Timezone: Die eingestellte Zeitzone für die lokale Zeit.

Daylight Saving Time: Falls aktiviert, wird die lokale Zeit in die Mitteleuropäische Sommerzeit umgerechnet.

Set manually: Der Benutzer kann manuell eine Uhrzeit setzen.

Set to Browsertime: Setzt die Uhrzeit des Webbrowsers.



Wenn Time Synchronisation eingeschaltet ist, wird eine manuelle Uhrzeit bei der nächsten NTP Synchronisation überschrieben.

### 3.3.2 Timer

NTP · [Timer](#)

**Timer - Basic Settings**

Enable Timer:  yes  no

Syslog verbosity level:

**Timer - Rules**

New Rule: simple Timer

New Rule: advanced Timer

Apply

Enable Timer: Schaltet alle Timer global ein oder aus.

Syslog verbosity level: Setzt die “verbosity” Stufe für Timer Syslog Ausgaben.

New Rule simple Timer: Zeigt ein Dialogfenster für eine einfache Timer Regel.

New Rule advanced Timer: Bringt den Dialog für komplexe Timer Einstellungen.

### 3.3.3 Timer Konfiguration

In der Timer-Konfiguration hat man drei Möglichkeiten: Einen einfachen Timer anlegen, einen komplexen Timer hinzufügen, oder eine bestehende Konfiguration ändern.



Timer Regeln werden nur dann ausgeführt, wenn das Gerät eine valide Uhrzeit hat. Siehe Konfiguration NTP.



Dieses Anleitungskapitel bezieht sich auf alle Digitus Geräte. Bei Geräten ohne schaltbare Ports kann man nur einen komplexen Timer anlegen. Für eine Aktion ist dort nur das Register "Action CLI" verfügbar, und nicht das Register "Action PortSwitch".

The image shows two configuration panels. The top panel, titled "Timer - Basic Settings", contains the following options: "Enable Timer:" with radio buttons for "yes" (selected) and "no"; and "Syslog verbosity level:" with a dropdown menu set to "normal". The bottom panel, titled "Timer - Rules", contains a lock icon followed by "Rule 1: 1: Power Port On", and two buttons: "New Rule: simple Timer" and "New Rule: advanced Timer".

### Einen einfachen Timer anlegen

Aktiviert man "New Rule: simple Timer" wird folgender Dialog angezeigt:

The image shows a dialog box titled "Timer Rule" with a close button (X) in the top right corner. It contains the following fields: "Switch" with a dropdown menu showing "1: Power Port" and "On" with a dropdown arrow; "From" with a time selector set to "09:30" and "To" with a time selector set to "11:00"; and "On weekdays:" with checkboxes for "Mon", "Tue", "Wed", "Thu", "Fri", "Sat", and "Sun", where "Mon" through "Fri" are checked. At the bottom right, there are "Save" and "Cancel" buttons.

Man stellt hier ein, welcher Port für welchen Zeitraum geschaltet werden soll, und an welchen Wochentagen die Regel aktiv ist. In diesem Beispiel ist im Vergleich zur Default-Eingabemaske der Zeitraum 9:00 bis 17:00 zu 9:30 bis 11:00 geändert. Auch soll diese Regel nicht an Samstag und Sonntag angewendet werden. Die nun vorliegende Regel besagt, dass jeden Tag, außer Samstag und Sonntag, der Port 1 um 9:30 Uhr eingeschaltet und nach 1,5 Stunden ausgeschaltet wird. Ein Klick auf "Save" speichert diese Regel.



Benutzt man z.B. nur eine Timer-Regel um einen Port um 9:00 einzuschalten, und um 20:00 auszuschalten. Wird um 9:00 der Timer getriggert, und ein Batchmode angelegt, um nach 11 Stunden auszuschalten. Wenn der Batchmode läuft, ist der Port gegen manuelle Bedienung auf der Webseite gesperrt. Auch passiert an einem Tag um 20:00 nichts, wenn diese Regel erst um 10:00 eingegeben wird, da ja die Regel erst gegen 9:00 getriggert wird, und der Batchmode dann um 20:00 ausschaltet. Möchte man dieses Verhalten nicht, bitte eine zweite Regel nutzen, um explizit um 20:00 den Port abzuschalten.

## Einen komplexen Timer anlegen

Legt man einen komplexen Timer an, oder verändert man einen schon bestehenden Timer, wird immer ein erweiterter Dialog gezeigt:

The 'Timer Rule' dialog box is shown with the following configuration:

- Trigger: Date/Time Pattern
- Options: Selected
- 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

Buttons: Delete, Save, Cancel

Man sieht hier die erweiterte Darstellung des einfachen Timers aus dem vorherigen Beispiel. Die Aktion wird jeden Tag jedes Monats um 9:30 gestartet. Die Wochentage Samstag und Sonntag sind ausgeschlossen. Eine bestehende Regel kann mit dem "Delete" Schalter entfernt werden.



Wenn eine Regel gelöscht wird, dann rücken die nachfolgenden Regeln nach. Auch die Nummerierung der nachfolgenden Regeln ändert sich dann um eins. Dies gilt auch für den Index in den Konsolen Kommandos.

The 'Timer Rule' dialog box is shown with the following configuration:

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

Rule Name: 1: Power 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

Ein einfacher Timer wird direkt "enabled", bei einem neuen komplexen Timer muss "enable trigger" manuell eingeschaltet werden. Man kann für die Timer-Regeln eine Wahrscheinlichkeit und eine Streuung einstellen. Hier wird die Regel mit 100% Wahrscheinlichkeit ausgeführt. Ein Jitter von 0 besagt, dass die Aktion exakt am



programmierten Zeitpunkt stattfindet. Als Aktionsmodus werden Ports geschaltet, alternativ kann auch ein Konsolen Kommando (CLI Cmd) ausgeführt werden.

Auf dem "Action PortSwitch" Register ist die Schaltfunktion detaillierter einstellbar. Der Port 1 wird eingeschaltet und nach 1,5h wieder ausgeschaltet.

Timer Rule

Trigger: Date/Time Pattern   Options   Action PortSwitch   Action Cli

Switch Power Ports Action1:

On	On	On	On	On	On	On	On
Off	Off	Off	Off	Off	Off	Off	Off

Switch Power Ports Action2:

On	-	-	-	-	-	-	-
Off	-	-	-	-	-	-	-

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

Test Action

"Action PortSwitch" steht nur bei Geräten mit schaltbaren Ports zur Verfügung.

## Eine Regel erweitern

Zur Demonstration wird hier der einfache Timer aus dem vorherigen Beispiel erweitert:

Timer Rule

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

Die Aktion wird jetzt nicht nur um 9:30 gestartet, sondern zusätzlich um 17:30. Es gibt weitere Veränderungen: Der Timer ist nur zwischen Oktober und Dezember aktiv, auch findet die Aktion nicht am ersten Tag eines Monats statt.



Da immer alle Felder in der Maske berücksichtigt werden, ist es in einer einzigen Timer-Regel nicht möglich, die Zeitpunkte 9:30 und 17:10 zu definieren. Man benötigt dafür eine

zweite Regel. Setzt man die Stunden 9 und 17, sowie die Minuten 10 und 30, dann wären die vier Zeitpunkte 9:10, 9:30, 17:10 und 17:30 programmiert.



Um in dieser Eingabemaske ein Feld zu wechseln ohne den Zustand der anderen Felder zu ändern, muss während des Mausclicks die Strg-Taste gedrückt werden.

**Timer Rule**

Trigger: Date/Time Pattern   Options   Action PortSwitch   Action Cli

Rule Name: 1: Power Port On

Rule Valid from: 05.12.2018 to 04.07.2019 dd.mm.yyyy

Random Trigger Probability: 90

Random Trigger Jitter: 0 secs

enable trigger:  yes  no

Action mode:  Switch Power Ports  Perform CLI Cmd

Bei dieser Regel ist auf dem "Options" Register der Zeitraum auf den Bereich zwischen dem 5.12.2018 und dem 4.7.2019 eingeschränkt. Die Timer-Regel wird in diesem Beispiel nur mit einer Wahrscheinlichkeit (Random Trigger Probability) von 90% ausgeführt.

**Timer Rule**

Trigger: Date/Time Pattern   Options   Action PortSwitch   Action Cli

Switch Power Ports Action1:

On	On	On	On	On	On	On	On
Off	Off	Off	Off	Off	Off	Off	Off

5: Power Port

Switch Power Ports Action2:

On	-	-	-	On	-	-	-
Off	-	-	-	Off	-	-	-

Between Action1 and Action 2 : wait 90 minute(s)

Test Action

Zusätzlich zu Port 1 ist hier Port 5 aktiviert und nach 90 Minuten wieder deaktiviert.



Ein Popup beim Mauszeiger zeigt die Portnummer des Feldes.

## Konsolen Kommandos

The screenshot shows the 'Timer Rule' dialog box with the 'Action CLI' tab selected. The 'Trigger' is set to 'Date/Time Pattern'. The 'Action CLI' field contains the following text:

```
Perform CLI Command:  
port 1 reset  
port 3 stat set 1
```

Below the text field, there is a 'Test Action' button.

Anstatt einen Port zu schalten, kann man einen oder mehrere Konsolen Kommandos ausführen lassen. Diese Befehle werden im "Action CLI" Register eingetragen. Der "Action Cli" Register ist nur dann anwählbar, wenn bei "Options" die Option "Perform CLI Cmd" aktiviert ist.

### Beispiel Port an einem Datum schalten

Wenn man einen Timer an einem bestimmten Datum zu einer Uhrzeit einschalten und zu einem späteren Zeitpunkt ausschalten möchte, kann man es nicht direkt mit einem einfachen Timer durchführen. Daher kann es sinnvoll sein, den Timer erst als einen einfachen Timer anzulegen, und dann in im erweiterten Dialog anzupassen.

The screenshot shows the 'Timer Rule' dialog box with the 'Options' tab selected. The 'Switch' is set to '3: Power Port' and the state is 'On'. The 'From' time is '09:25' and the 'To' time is '17:30'. The 'On weekdays' section has checkboxes for Mon, Tue, Wed, Thu, Fri, Sat, and Sun, all of which are checked. There are 'Save' and 'Cancel' buttons at the bottom right.

Schaltet jeden Tag Port 3 um 9:25 ein, und um 17:30 wieder aus. Man speichert den die einfache Regel.

The screenshot shows the 'Timer Rule' dialog box with the 'Action PortSwitch' tab selected. The 'Rule Name' is '3: Power Port On'. The 'Rule Valid from' is '17.05.2019' and the 'Rule Valid to' is '17.05.2019'. The 'Random Trigger Probability' is '100' and the 'Random Trigger Jitter' is '0' secs. The 'enable trigger' section has radio buttons for 'yes' (selected) and 'no'. The 'Action mode' section has radio buttons for 'Switch Power Ports' (selected) and 'Perform CLI Cmd'. There are 'Delete', 'Save', and 'Cancel' buttons at the bottom.

Danach ruft man den angelegten Timer auf und trägt im "Options" Register das Datum ein, an dem der Schaltvorgang stattfinden soll.

### Beispiel rolling shutter

**Timer Rule**

Trigger: Date/Time Pattern   Options   Action PortSwitch   Action Cli

Rule Name: 1: Power Port On

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

Man kann den Jitter z.B. für eine Rollladensteuerung einsetzen. Bei dem klassischen Beispiel einer Rollladensteuerung möchte man, um potentielle Einbrecher zu verwirren, die Jalousien nicht immer zu den gleichen Zeitpunkten herauf- und herunterfahren. Der Jitter von 1800 Sekunden bedeutet, dass die Aktion zufällig in einem Zeitraum von zwischen 30 Minuten vor und 30 Minuten nach dem programmierten Zeitpunkt ausgeführt wird. Die Wahrscheinlichkeit (Random Trigger Probability) der Ausführung beträgt hier 100%.

### 3.4 Sensoren

Control Panel   Configuration   Maintenance   Logout

Ethernet · Protocols · **Sensors** · E-Mail · Front Panel

**Sensors Config**

- Sensor: 1: 7106 - 7106
- Sensor Name: 7106
- Select Sensor Field: Temperature (°C)
- Enable "Temperature" Messages:  yes  no
- Maximum value: 65.0 °C
- Minimum value: 25.0 °C
- Hysteresis: 3.0 °C
- Message channels:  Syslog  SNMP  Email  Beeper

**Misc sensor options**

- Min/Max measurement period: 24 Hours
- Enable beeper for AC alarms:  yes  no
- Enable beeper for sensor alarms:  yes  no

Apply

Sensor: Wählt einen Sensortyp aus um ihn zu konfigurieren. Die erste Ziffer "1:" gibt die Nummer des Sensorports an (nur wichtig bei Geräten mit mehr als einem Sensor Anschluss). Danach folgt die Sensor Bezeichnung, und der einstellbare Sensorname.

Sensor Name: Änderbarer Name für diesen Sensor. Dabei kann man z.B. der Temperatur und der Luftfeuchtigkeit einen anderen Namen geben, auch wenn sie dem gleichen Sensor angehören.

Select Sensor Field: Wählt einen Datenkanal aus einem Sensor aus.

Enable ... Messages: Schaltet die Überwachung von Sensor-Grenzwerten ein.

Maximum/Minimum value: Einstellbare Grenzwerte für Stromstärken (Min. und Max.), bei denen Warnmeldungen per SNMP-Traps, Syslog oder E-Mail versendet werden sollen.

Hysteresis: Konfiguriert den Abstand, der nach einem Überschreiten eines Stromgrenzwertes überquert werden muss, um das Unterschreiten des Grenzwertes zu signalisieren.

Message channels: Aktiviert die Erzeugung von Nachrichten auf verschiedenen Kanälen.

Min/Max measurement period: Selektiert den Zeitraum für den Sensor Min./Max. Werte auf der "Control Panel" Webseite angezeigt werden.

Enable beeper for AC alarms: Schaltet den Summer für alle Nachrichten bei Unter-/Überschreiten der Strom-Grenzwerte ein.

Enable beeper for sensor alarms: Schaltet den Summer für alle Nachrichten bei Unter-/Überschreiten der Sensor Grenzwerte ein.

### **Hysterese Beispiel**

Ein Hysteresewert verhindert, dass zuviele Nachrichten erzeugt werden, wenn ein Sensor-Wert um eine Sensor-Grenze "jittert". Das folgende Beispiel zeigt das Verhalten für einen Temperatursensor bei einem Hysteresewert von "1". Die obere Grenze ist auf 50 °C gesetzt.

#### **Beispiel:**

49.9 °C – unterhalb der Obergrenze

50.0 °C – eine Nachricht für das Erreichen der oberen Grenze wird erzeugt

50.1 °C – ist oberhalb der Obergrenze

...

49.1 °C – unterhalb der oberen Grenze, aber im Hysteresebereich

49.0 °C – unterhalb der oberen Grenze, aber im Hysteresebereich

48.9 °C – eine Meldung für das Überschreiten der oberen Grenze inklusive Hysteresebereich wird erzeugt

...

### 3.5 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: Hier können Sie einstellen ob E-Mails versendet werden sollen.

Sender address: Tragen Sie hier ein, unter welcher E-Mailadresse die E-mails versendet werden sollen.

Recipient address: Geben Sie hier die E-Mailadresse des Empfängers ein. Es können weitere E-Mail Adressen, durch Komma getrennt, angegeben werden. Die Eingabegrenze liegt bei 100 Zeichen.

SMTP Server: Tragen Sie hier die SMTP Adresse des E-Mailservers ein. Entweder als FQDN, z.B: "mail.gmx.net", oder als IP-Adresse, z.B: "213.165.64.20".

SMTP server port: Die Port-Adresse des E-Mailservers. Dies sollte im Normalfall die gleiche wie der Default sein, der durch die "SMTP Connection Security" vorgegeben wird.

SMTP Connection Security: Übertragung per SSL oder ohne Verschlüsselung.

SMTP Authentification (password): Authentifizierungsmethode des E-Mailservers.

Username: Der Benutzernamen, mit dem sich beim E-Mailserver angemeldet wird.

Set new password: Tragen Sie hier das Passwort, für die Anmeldung beim E-Mailserver, ein.

Repeat password: Wiederholen Sie das Passwort, um es zu bestätigen.



Wird die Passwort Eingabemaske neu angezeigt, so gelten die vier "Kreise" nur als symbolischer Platzhalter, da aus Sicherheitsgründen auf dem Gerät nie das Passwort selber angezeigt wird. Möchte man das Passwort ändern, so muss immer das vollständige Passwort neu eingegeben werden.

E-Mail Logs: Ausgabe von E-Mail Diagnose Nachrichten.

### 3.6 Front Panel

**Front Panel**

- Button Lock:  yes  no
- Dark Display:  yes  no
- Default Display:

Button Lock: Deaktiviert die Front-Taster (bzw. aktiviert die Tastensperre) mit Ausnahme der Bootloader-Aktivierung.

Dark Display: Das Display bleibt dunkel. Tastenbedienung schaltet die Anzeige temporär ein.

Default Display: Wählt aus, welcher Sensor im Display angezeigt wird.

## 4. Spezifikationen

### 4.1 IP ACL

#### IP Access Control List

Die IP Access Control List (IP-ACL) ist ein Filter für eingehende IP-Verbindungen. Ist der Filter aktiv, können nur die Hosts und Subnetze, deren IP-Adressen in der Liste eingetragen sind, Kontakt über HTTP oder SNMP aufnehmen, und Einstellungen ändern. Für eingehende Verbindungen von nicht autorisierten PCs verhält sich das Gerät nicht komplett transparent. Aufgrund technischer Eigenschaften wird eine TCP/IP-Verbindung zwar zuerst angenommen, aber dann direkt abgelehnt.

Beispiele:

Eintrag in der IP ACL	Bedeutung
192.168.0.123	der PC mit der IP Adresse "192.168.0.123" kann auf das Gerät zugreifen
192.168.0.1/24	alle Geräte des Subnetzes "192.168.0.1/24" können auf das Gerät zugreifen
1234:4ef0:eec1:0::/64	alle Geräte des Subnetzes "234:4ef0:eec1:0::/64" können auf das Gerät zugreifen



Sollten Sie sich hier aus Versehen „ausgesperrt“ haben, aktivieren Sie den Bootloader-Modus und deaktivieren Sie mit Hilfe der GBL\_Conf.exe die IP ACL. Alternativ können Sie das Gerät in den Werkzustand zurücksetzen.

## 4.2 IPv6

### IPv6 Adressen

IPv6-Adressen sind 128 Bit lang und damit viermal so lang wie IPv4 Adressen. Die ersten 64 Bit bilden den sogenannten Präfix, die letzten 64 Bit bezeichnen den eindeutigen Interface-Identifizierer. Der Präfix setzt sich aus Routing-Präfix und der Subnetz-ID zusammen. Ein IPv6 Netzwerk Interface kann unter mehreren IP-Adressen erreichbar sein. Normalerweise ist dies durch eine globale Adresse und der link local Adresse.

### Adressnotation

IPv6 Adressen werden hexadezimal in 8 Blöcken zu 16-Bit notiert, wo hingegen IPv4 normalerweise dezimal angegeben wird. Das Trennzeichen ist ein Doppelpunkt und nicht der Punkt.

z.B.: 1234:4ef0:0:0:0019:32ff:fe00:0124

Innerhalb eines Blockes dürfen führende Nullen weggelassen werden. Das vorhergehende Beispiel kann auch so geschrieben werden:

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

Man darf einen oder mehrere aufeinanderfolgende Blöcke auslassen, wenn Sie aus Nullen bestehen. Dies darf in einer IPv6-Adresse aber nur einmal durchgeführt werden!

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

Man darf für die letzten 4 Bytes die von IPv4 gewohnte Dezimalnotation verwenden:

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

## 4.3 RADIUS

Die Passwörter für HTTP, telnet und serielle Konsole (abhängig vom Modell) können lokal gespeichert werden, und / oder über RADIUS authentifiziert werden. Die RADIUS Konfiguration unterstützt einen Primary Server und einen Backup Server. Sollte der Primary Server sich nicht melden, wird die RADIUS Anfrage an den Backup Server gestellt. Sind das lokale Passwort und RADIUS gleichzeitig aktiviert, wird erst lokal geprüft, und dann bei Misserfolg die RADIUS Server kontaktiert.

### RADIUS Attribute

Folgende RADIUS Attribute werden vom Client ausgewertet:

**Session-Timeout:** Dieses Attribut gibt an (in Sekunden), wie lange eine akzeptierte RADIUS Anfrage gültig ist. Nach Ablauf dieser Zeitspanne muss der RADIUS Server erneut gefragt werden. Wird dieses Attribut nicht zurückgegeben, wird stattdessen der Default-Timeout Eintrag aus der Konfiguration genutzt.

**Filter-Id:** Ist für dieses Attribut der Wert "admin" gesetzt, dann werden bei einem HTTP Login Admin Rechte vergeben, sonst nur User Zugang.



**Service-Type:** Dies ist eine Alternative zu Filter-Id. Ein Service-Type von "6" oder "7" bedeuten bei einem HTTP Login Admin Rechte, andernfalls nur beschränkter User Zugriff.

### HTTP Login

Der HTTP Login findet über Basic Authentication statt. Dies bedeutet, dass es in der Verantwortung des Webservers liegt, wie lange die Login-Credentials dort zwischengespeichert werden. Der RADIUS Parameter "Session Timeout" bestimmt also nicht, wann der Nutzer sich über einen Login erneut anmelden muss, sondern in welchen Abständen die RADIUS Server erneut gefragt werden.

### 4.4 Automatisierte Zugriffe

Das Gerät kann automatisiert über vier verschiedene Schnittstellen angesprochen werden, die unterschiedliche Möglichkeiten bieten auf die Konfigurationsdaten und Statusinformationen zuzugreifen. Nur http und die Konsole (telnet und serielle) bieten den kompletten Zugriff auf das Gerät.

Liste der unterschiedlichen Zugriffsmöglichkeiten (falls vom Modell unterstützt):

Schnittstelle	Umfang des Zugriffs
HTTP	Lesen/Schreiben aller Konfigurationsdaten Lesen/Schreiben aller Statusinformationen
Console	Lesen/Schreiben aller Konfigurationsdaten Lesen/Schreiben aller Statusinformationen
SNMP	Lesen/Schreiben Zustand der Powerports (Relais) Lesen/Schreiben Namen der Powerports (Relais) Lesen/Schreiben Zustand der Port Startkonfiguration Lesen/Schreiben Zustand Buzzer Lesen Messwerte externer Sensoren Lesen Messwerte aller Energiesensoren Rücksetzen der Energiezähler Lesen Zustand Overvoltage Protection
Modbus TCP	Lesen/Schreiben Zustand der Powerports (Relais) Lesen Zustand der Eingänge Lesen Messwerte externer Sensoren Lesen Messwerte aller Energiesensoren

Über die http Schnittstelle kann das Gerät mit CGI Befehlen gesteuert werden, und gibt die interne Konfiguration und Status im JSON Format zurück.

## 4.5 SNMP

SNMP kann dazu verwendet werden, Statusinformationen per UDP (Port 161) zu erhalten. Unterstützte SNMP Befehle:

- GET
- GETNEXT
- GETBULK
- SET

Um per SNMP abzufragen benötigen Sie ein Network Management System, wie z.B. HP-OpenView, OpenNMS, Nagios, etc., oder die einfachen Kommandozeilen-Tools der NET-SNMP Software. Das Gerät unterstützt die SNMP Protokolle v1, v2c und v3. Sind in der Konfiguration Traps aktiviert, werden die auf dem Gerät erzeugten Messages als Notifications (Traps) versendet. SNMP Informs werden nicht unterstützt. SNMP Requests werden mit der gleichen Version beantwortet, mit der sie verschickt wurden. Die Version der versendeten Traps lässt sich in der Konfigurationseinstellen.

### MIB Tabellen

Die Werte, die vom Gerät ausgelesen bzw. verändert werden können, die so genannten "Managed Objects", werden in Management Information Bases (kurz MIBs) beschrieben. Diesen Teilstrukturen sind sogenannte OIDs (Object Identifiers) untergeordnet. Eine OID-Stelle steht für den Ort eines Wertes innerhalb der MIB-Struktur. Jeder OID kann alternativ mit seinem Symbolnamen (subtree name) bezeichnet werden. Die MIB Tabelle dieses Gerätes kann aus der SNMP Konfigurationsseite mit einem Klick auf den Link "MIB table" im Browser als Textdatei angezeigt werden.

### SNMP v1 and v2c

SNMP v1 und v2c authentifiziert die Netzwerkanfragen anhand sogenannter "Communities". Der SNMP-Request muss bei Abfragen (Lesezugriff) die sogenannte "public Community", und bei Zustandsänderungen (Schreibzugriff) die "private Community" mitsenden. Die SNMP-Communities sind Lese- bzw. Schreibpasswörter. Bei den SNMP Versionen v1 und v2c werden die Communities unverschlüsselt im Netzwerk übertragen und können innerhalb dieser Kollisionsdomäne also leicht mit IP-Sniffern abgehört werden. Zur Begrenzung des Zugriffs empfehlen wir den Einsatz innerhalb einer DMZ bzw. die Verwendung der IP-ACL.

### SNMP v3

Da das Gerät keine Mehrbenutzerverwaltung kennt, wird auch in SNMP v3 nur ein Benutzer (default name "standard") erkannt. Aus den User-based Security Model (USM) MIB Variablen gibt es eine Unterstützung der "usmStats..." Zähler. Die "usmUser..." Variablen werden mit der Erweiterung für weitere Nutzer in späteren Firmwareversionen hinzugefügt. Das System kennt nur einen Kontext. Das System akzeptiert den Kontext "normal" oder einen leeren Kontext.

### Authentication

Zur Authentifizierung werden die Algorithmen "HMAC-MD5-96" und "HMAC-SHA-96" angeboten. Zusätzlich sind die "HMAC-SHA-2" Varianten (RFC7630) "SHA-256", "SHA-384" und "SHA-512" implementiert.



"SHA-384" und "SHA-512" werden rein in Software berechnet. Werden auf der Konfigurationsseite "SHA-384" oder "SHA-512" eingestellt, können einmalig bis zu ca. 45 Sekunden für die Schlüsselerzeugung vergehen.

### **Verschlüsselung**

Die Verfahren "DES", "3DES", "AES-128", "AES-192" und "AES-256" werden in Kombination mit "HMAC-MD5-96" und "HMAC-SHA-96" unterstützt. Für die "HMAC-SHA-2" Protokolle gibt es zur Zeit weder ein RFC noch ein Draft, das eine Zusammenarbeit mit einer Verschlüsselung ermöglicht.



Während bei der Einstellung "AES-192" und "AES-256" die Schlüssel nach "draft-blumenthal-aes-usm-04" berechnet werden, benutzen die Verfahren "AES-192-3DESKey" und "AES-256-3DESKey" eine Art der Schlüsselerzeugung, die auch beim "3DES" ("draft-reeder-snmvp3-usm-3desede-00") eingesetzt wird. Ist man kein SNMP Experte, empfiehlt es sich, jeweils die Einstellungen mit und ohne "...-3DESKey" auszuprobieren.

### **Passwörter**

Die Passwörter für Authentifizierung und Verschlüsselung sind aus Sicherheitsgründen nur als berechnete Hashes abgespeichert. So kann, wenn überhaupt, nur sehr schwer auf das Ausgangspasswort geschlossen werden. Die Berechnung des Hashes ändert sich aber mit den eingestellten Algorithmen. Werden die Authentication oder Privacy Algorithmen geändert, müssen im Konfigurationsdialog die Passwörter wieder neu eingegeben werden.

### **Sicherheit**

Folgende Aspekte gibt es zu beachten:

- Sollen Verschlüsselung oder Authentifizierung zum Einsatz kommen, dann SNMP v1 und v2c ausschalten, da sonst darüber auf das Gerät zugegriffen werden kann.
- Wird nur authentifiziert, dann sind die neuen "HMAC-SHA-2" Verfahren den MD5 oder SHA-1 Hashing Algorithmen überlegen. Da nur SHA-256 in Hardware beschleunigt wird, und SHA-384 sowie SHA-512 rein in Software berechnet werden, sollte man im Normalfall SHA-256 auswählen. Vom kryptographischen Standpunkt reicht die Sicherheit eines SHA-256 zur Zeit vollkommen aus.
- Für SHA-1 gibt es derzeit etwas weniger Angriffsszenarien als für MD5. Im Zweifelsfall ist SHA-1 vorzuziehen.
- Die Verschlüsselung "DES" gilt als sehr unsicher, nur im Notfall aus Kompatibilitätsgründen einsetzen!
- Es gilt bei Kryptologen als umstritten, ob "HMAC-MD5-96" und "HMAC-SHA-96" genügend Entropie für die Schlüssellängen von "AES-192" oder "AES-256" aufbringen können.
- Ausgehend von den vorhergehenden Betrachtungen empfehlen wir zur Zeit "HMAC-SHA-96" mit "AES-128" als Authentifizierung und Verschlüsselung.

## Änderungen im Trap Design



In älteren MIB-Tabellen wurde für jede Kombination aus einem Event und einer Portnummer ein eigener Trap definiert. Dies führt bei den Geräten zu längeren Listen von Trap-Definitionen. Z.B. von **epc8221SwitchEvtPort1** bis **epc8221SwitchEvtPort12**. Da neue Firmwareversionen viel mehr verschiedene Events generieren können, produziert dieses Verhalten schnell mehrere hundert Trap-Definitionen. Um diese Überfülle an Trap-Definitionen einzuschränken, wurde das Trap-Design so verändert, das für jeden Event-Typ nur ein bestimmter Trap erzeugt wird. Die Port- oder Sensornummer wird jetzt im Trap als Index OID innerhalb der "variable bindings" zur Verfügung gestellt.

Damit diese Änderung direkt erkannt wird, wurde der "Notification" Bereich in der MIB Tabelle von sysObjectID.0 nach sysObjectID.3 verschoben. So werden erstmal nicht identifizierte events generiert, bis die neue MIB Tabelle eingespielt wird. Aus Kompatibilitätsgründen werden SNMP v1 Traps genauso erzeugt wie früher.

### NET-SNMP

NET-SNMP bietet eine sehr weit verbreitete Sammlung von SNMP Kommandozeilen Tools (snmpget, snmpset, snmpwalk, etc.) NET-SNMP ist u.a. für Linux und Windows verfügbar. Nach der Installation von NET-SNMP sollten Sie die Gerätespezifische MIB des Geräts in das "share" Verzeichnis von NET-SNMP legen, z.B. nach

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

oder

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

So können Sie später anstatt der OIDs die 'subtree names' verwenden:

```
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 Beispiele

Power Port 1 Schaltzustand abfragen:

```
snmpget -v2c -mALL -c public 192.168.1.232 epc822XPortState.1
```

Power Port 1 einschalten:

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

#### 4.5.1 Device MIB 8341 (DN-95637)

Es folgt eine Tabelle aller gerätespezifischen OID's die über SNMP angesprochen werden können. Bei der numerischen OID Darstellung wurde das Präfix "1.3.6.1.4.1.28507" aus Platzgründen bei jedem Eintrag in der Tabelle weggelassen. Die komplette OID würde daher z.B.

"1.3.6.1.4.1.28507.65.1.1.1.1" lauten. Man unterscheidet in SNMP bei OID's zwischen Tabellen und Skalaren. OID Skalare haben die Endung ".0" und spezifizieren nur einen Wert. Bei SNMP Tabellen wird das "x" durch einen Index (1 oder größer) ersetzt, um einen Wert aus der Tabelle zu adressieren.

Name	Description	OID	Type	Acc.
pdu8341TrapCtrl	0 = off 1 = Ver. 1 2 = Ver. 2c 3 = Ver. 3	.65.1.1.1.1.0	Integer32	RW
pdu8341TrapPIIndex	A unique value, greater than zero, for each receiver slot.	.65.1.1.1.2.1.1.x	Integer32	RO
pdu8341TrapAddr	DNS name or IP address specifying one Trap receiver slot. A port can optionally be specified: 'name:port' An empty string disables this slot.	.65.1.1.1.2.1.2.x	OCTETS	RW
pdu8341Buzzer	Turn buzzer on and off	.65.1.3.10.0	Integer32	RW
pdu8341ActivePowerChan	Number of supported Power Channels	.65.1.5.1.1.0	Unsigned32	RO
pdu8341PowerIndex	Index of Power Channel entries	.65.1.5.1.2.1.1.x	Integer32	RO
pdu8341ChanStatus	0 = data not active, 1 = data valid	.65.1.5.1.2.1.2.x	Integer32	RO
pdu8341AbsEnergyActive	Absolute active energy counter	.65.1.5.1.2.1.3.x	Gauge32	RO
pdu8341PowerActive	Active Power	.65.1.5.1.2.1.4.x	Integer32	RO
pdu8341Current	Actual Current on Power Channel	.65.1.5.1.2.1.5.x	Gauge32	RO
pdu8341Voltage	Actual Voltage on Power Channel	.65.1.5.1.2.1.6.x	Gauge 32	RO
pdu8341Frequency	Frequency of Power Channel	.65.1.5.1.2.1.7.x	Gauge32	RO
pdu8341PowerFactor	Power Factor of Channel between -1.0 and 1.00	.65.1.5.1.2.1.8.x	Integer32	RO
pdu8341Pangle	Phase Angle between Voltage and L Line Current between -180.0 and 180.0	.65.1.5.1.2.1.9.x	Integer32	RO
pdu8341PowerApparent	L Line Mean Apparent Power	.65.1.5.1.2.1.10.x	Integer32	RO
pdu8341PowerReactive	L Line Mean Reactive Power	.65.1.5.1.2.1.11.x	Integer32	RO
pdu8341AbsEnergyReactive	Absolute reactive energy counter	.65.1.5.1.2.1.12.x	Gauge32	RO
pdu8341AbsEnergyActiveResettable	Resettable absolute active energy counter. Writing '0' resets all resettable counter.	.65.1.5.1.2.1.13.x	Gauge32	RW
pdu8341AbsEnergyReactiveResettable	Resettable absolute reactive energy counter	.65.1.5.1.2.1.14.x	Gauge32	RO
pdu8341ResetTime	Time in seconds since last energy counter reset	.65.1.5.1.2.1.15.x	Gauge32	RO
pdu8341ForwEnergyActive	Forward active energy counter	.65.1.5.1.2.1.16.x	Gauge32	RO
pdu8341ForwEnergyReactive	Forward reactive energy counter	.65.1.5.1.2.1.17.x	Gauge32	RO
pdu8341ForwEnergyActiveResettable	Resettable forward active energy counter	.65.1.5.1.2.1.18.x	Gauge32	RO

pdu8341ForwEnergyReactiveResettable	Resettable forward reactive energy counter	.65.1.5.1.2.1.19.x	Gauge32	RO
pdu8341RevEnergyActive	Reverse active energy counter	.65.1.5.1.2.1.20.x	Gauge32	RO
pdu8341RevEnergyReactive	Reverse reactive energy counter	.65.1.5.1.2.1.21.x	Gauge32	RO
pdu8341RevEnergyActiveResettable	Resettable reverse active energy counter	.65.1.5.1.2.1.22.x	Gauge32	RO
pdu8341RevEnergyReactiveResettable	Resettable reverse reactive energy counter	.65.1.5.1.2.1.23.x	Gauge32	RO
pdu8341ResidualCurrent	Actual residual current on power channel. According type A IEC 60755. Only visible on models that support this feature.	.65.1.5.1.2.1.24.x	Unsigned32	RO
pdu8341LineSensorName	A textual string containing name of a Line sensor.	.65.1.5.1.2.1.100.x	OCTETS	RW
pdu8341SensorIndex	None	.65.1.6.1.1.1.x	Integer32	RO
pdu8341TempSensor	Actual temperature	.65.1.6.1.1.2.x	Integer32	RO
pdu8341HygroSensor	Actual humidity	.65.1.6.1.1.3.x	Integer32	RO
pdu8341InputSensor	Logical state of input sensor	.65.1.6.1.1.4.x	INTEGER	RO
pdu8341AirPressure	Actual air pressure	.65.1.6.1.1.5.x	Integer32	RO
pdu8341DewPoint	Dew point for actual temperature and humidity	.65.1.6.1.1.6.x	Integer32	RO
pdu8341DewPointDiff	Difference between dew point and actual temperature (Temp-DewPoint)	.65.1.6.1.1.7.x	Integer32	RO
pdu8341ExtSensorName	A textual string containing name of an external sensor	.65.1.6.1.1.32.x	OCTETS	RW

## 4.6 SSL

### TLS Standard

Das Gerät ist kompatibel zu den Standards TLS v1.0 bis TLS v1.2. Wegen fehlender Sicherheit sind SSL v3.0, sowie die Verschlüsselungen RC4 und DES deaktiviert.

Die folgenden TLS Ciphersuites werden unterstützt:

- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_PSK\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA256

- TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_CCM
- TLS\_RSA\_WITH\_AES\_256\_CCM
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CCM
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CCM
- TLS\_RSA\_WITH\_AES\_128\_CCM\_8
- TLS\_RSA\_WITH\_AES\_256\_CCM\_8
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CCM\_8
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CCM\_8
- TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256
- TLS\_DHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

### Erstellen eigener Zertifikate

Der SSL Stack wird mit einem eigens neu generierten Zertifikat ausgeliefert. Es gibt keine Funktion, um das lokale Zertifikat auf Knopfdruck neu zu erzeugen, da die benötigten Zufallszahlen in einem Embedded Device meist nicht unabhängig genug sind. Man kann jedoch selbst neue Zertifikate erzeugen und auf das Gerät importieren. Der Server akzeptiert RSA (1024/2048/4096) und ECC (Elliptic Curve Cryptography) Zertifikate.

Zum Erstellen eines SSL-Zertifikats wird meist OpenSSL verwendet. Für Windows gibt es z.B. die Light-Version von Shining Light Productions. Dort eine Eingabeaufforderung öffnen, in das Verzeichnis "C:\OpenSSL-Win32\bin" wechseln und diese Environment Variablen setzen:

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

Hier einige Beispiele zur Generierung mit OpenSSL:

### Erstellung eines RSA 2048-Bit self-signed Zertifikats:

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

### RSA 2048-Bit Zertifikat mit 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
```



Die Server Keys sollten mit "openssl genrsa" erzeugt werden. Das Gude Gerät verarbeitet Keys im traditionellen PKCS#1 Format. Dies erkennt man, in dem in der erzeugten Schlüsseldatei am Anfang "-----BEGIN RSA PRIVATE KEY" steht. Beginnt die Datei mit "-----BEGIN PRIVATE KEY", ist die Datei im PKCS#8 Format, und der Schlüssel wird nicht erkannt. Hat man nur einen Schlüssel im PKCS#8 Format, kann dieser z.B. mit openssl nach PKCS#1 konvertiert werden: "**openssl rsa -in pkcs8.key -out pkcs1.key**".

### ECC Zertifikat mit 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
```

Hat man Schlüssel und Zertifikat erstellt, werden beide Dateien zu einer Datei aneinandergehängt:

Linux:

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

Windows:

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

Die erstellte "server.pem" kann nun im Maintenance Bereich im Gerät hochgeladen werden.



Sollen mehrere Zertifikate (Intermediate CRT's) zusätzlich auf das Gerät geladen werden, so sollte man darauf achten, in der Reihenfolge als erstes das Server-Zertifikat, und dann die Intermediates zusammenzufügen. z.B.:

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



Nach einem Zurücksetzen in den Werkszustand bleibt ein hochgeladenes Zertifikat erhalten.



## Performance Betrachtung

Werden RSA 4096 Zertifikate eingesetzt, so kann der erste Zugriff auf den Webserver 8-10 Sekunden dauern, da die Mathematikeinheit der Embedded CPU stark gefordert ist. Danach sind die Parameter im SSL Session Cache, und alle weiteren Zugriffe sind genauso schnell wie bei anderen Zertifikatslängen. Für eine schnelle Antwort auch beim ersten Zugriff, empfehlen wir daher RSA 2048-Bit Zertifikate, die auch ausreichend Sicherheit bieten.

## 4.7 Konsole

Für die Konfiguration und Steuerung des Gerätes existiert ein Befehlssatz von Kommandos mit Parametern, die über eine Konsole eingegeben werden können. Die Konsole steht über Telnet, oder bei Geräten mit RS232 Anschluss über ein serielles Terminal zur Verfügung. Es muss nicht unbedingt Telnet genutzt werden, im Raw Mode reicht eine einfache TCP/IP Verbindung, um Befehle schicken zu können. Die Kommunikation lässt sich auch automatisiert durchführen (z.B. über Skriptsprachen). Die Konsoleneigenschaften werden über das Webinterface konfiguriert.

### Befehlssatz

Es existieren mehrere Kommando-Ebenen. Folgende Kommandos sind von jeder Ebene benutzbar:

Back	Eine Befehlsebene zurück gehen
Help	Die Befehle der aktuellen Ebene
Help all	Alle Befehle anzeigen
Logout	Ausloggen (nur wenn Login erforderlich)
Quit	Konsole beenden

Der Befehl "help" gibt alle Kommandos der aktuellen Ebene zurück. Wird "help" von der obersten Ebene aufgerufen, wird z.B. auch die Zeile "http [subtopics]" angezeigt. Dies bedeutet, dass es für "http" eine weitere Ebene gibt. Mit dem Kommando "http help" lassen sich nun alle Befehle unterhalb von "http" anzeigen. Alternativ kann man mit dem Aufruf "http" diese Ebene auswählen, und "help" zeigt alle Befehle der gewählten Ebene. Das Kommando "back" selektiert wieder die oberste Ebene. Es ist möglich "help" an einer beliebigen Position zu benutzen: "http passwd help" stellt z.B. alle Kommandos dar, die den Präfix "http passwd" besitzen.

Eine komplette Liste aller möglichen Geräte-Befehle finden Sie im Kapitel "Console Cmd".

### Parameter

Werden für die Kommandos Parameter erwartet, lässt sich der Parameter numerisch oder als Konstante übergeben. Bekommt man als Hilfe z.B. die folgende Zeile:

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

so sind die folgenden Anweisungspaare jeweils äquivalent:

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

oder

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

Numerische Parameter können mit verschiedenen Basen eingegeben werden. Hier ein Beispiel für den dezimalen Wert 11:

Basis	Eingabe
Dezimal (10)	11
Hexadezimal (16)	0xb
Oktal (8)	013
Binär (2)	0b1011

### Bitfield-Parameter

Manche Parameter können mehrere Werte gleichzeitig annehmen. Im folgenden Beispiel können alle Werte zwischen 0 und 5 gesetzt werden. In der Hilfe ist dies daran erkennbar, dass die Werte nicht durch das "|" Zeichen, sondern durch Kommata getrennt sind.

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

Um in einem Befehl EVT\_SYSLOG und EVT\_EMAIL zu setzen, kann man z.B. folgende Syntax benutzen:

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

oder numerisch

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

Zusätzlich kann man mit "ALLSET" alle Werte setzen, oder mit der Syntax "#7f1a" eine beliebiges Bitmuster als Hexzahl kodieren.

### Rückgabewerte

Ist ein Befehl unbekannt oder ein Parameter fehlerhaft, so erfolgt am Anfang der Zeile die Ausgabe "ERR." mit einer nachfolgenden Fehlerbeschreibung. Erfolgreiche Anweisungen ohne speziellen Rückgabewert werden mit "OK." quittiert. Alle anderen Rückgabewerte werden innerhalb einer einzelnen Zeile ausgegeben. Es gibt davon zwei Ausnahmen:

1. Manche Konfigurationsänderungen, die TCP/IP und UDP betreffen, werden erst nach einem Neustart übernommen. Diese Parameter werden zweizeilig ausgegeben. In der ersten Zeile ist der aktuelle Wert, in der zweiten Zeile der Wert nach dem Neustart. In der "Cmd Overview" Tabelle ist dies mit "Note 2" gekennzeichnet.
2. Einige Konfigurationen (wie z.B. die vergebenen IPv6-Adressen) haben mehrere Werte, die sich dynamisch ändern können. Dies ist mit "Note 3" in der "Cmd Overview" Tabelle markiert.

## Numerische Rückgaben

Bei Parametern, die Konstanten unterstützen, werden diese Konstanten auch als Rückgabewerte ausgegeben. Um besser mit Skriptsprachen arbeiten zu können, kann es einfacher sein, nur mit numerischen Rückgaben zu arbeiten. Mit dem Befehl "`vt100 numeric set ON`" werden nur noch numerische Werte angezeigt.

## Kommentare

Möchten Sie mit einem Tool eine ganze Datei von Kommandos über Telnet schicken, so ist es hilfreich, dort Kommentare verfassen zu können. Ab dem Kommentarzeichen "#" wird deshalb der restliche Inhalt einer Zeile ignoriert.

## Telnet

Ist die Konfiguration nicht im "Raw Mode", so wird mit Hilfe der IAC Befehle versucht, die Telnet Konfiguration zwischen Client und Server auszutauschen. Gelingt dies nicht, so sind die Editierfunktionen nicht aktiv, und die "Activate echo" Option bestimmt, ob die zum Telnet Server gesendeten Zeichen zurückgeschickt werden. Normalerweise beginnt der Client die IAC Negotiation. Ist dies beim Client nicht der Fall, sollte in der Gerätekonfiguration "Active negotiation" eingeschaltet werden.

## Raw Mode

Möchte man die Konsole nur automatisiert nutzen, so kann es von Vorteil sein, die Konfiguration "Raw mode" auf "yes" und "Activate echo" auf "no" zu stellen. Es gibt dann keine störende Interaktion mit den Editor-Funktionen und es müssen die gesendeten Zeichen nicht gefiltert werden, um die Rückgabewerte zu verarbeiten.



Ist in der Konsole "Raw mode" aktiviert aber nicht im benutzten Telnet Client, dann können die am Anfang übermittelten IAC Befehle als störende Zeichen in Kommandozeile auftauchen (teilweise unsichtbar).

## Editierfunktion

Die folgenden Editierfunktionen sind verfügbar, wenn das Terminal VT100 unterstützt, und der RAW-Modus nicht eingeschaltet ist. Eingegebene Zeichen werden an der Cursorposition eingefügt.

Tasten	Funktion
Links, Rechts	Bewegt den Cursor nach links oder rechts
Pos1, End	Setzt den Cursor auf Anfang oder Ende der Zeile
Del	Löscht Zeichen unter dem Cursor
Backspace	Löscht Zeichen links vom Cursor
Up, Down	Zeigt ältere Eingabezeilen (History)
Tab, Strg-Tab	Vervollständigt das Wort am Cursor
Strg-C	Löscht die Zeile

## Gebündelte Informationen

Die Syntax der Konsolenbefehle macht es nicht einfach, gebündelte Informationen mit wenigen Befehlen auszugeben. Folgende Spezialbefehle erleichtern dies:

### a) Externe Sensoren

```
>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"
```

Der Befehl listet jeweils einen angeschlossenen externen Sensor pro Zeile, und nach dem Labelnamen kommen die einzelnen Messwerte durch Kommata getrennt. Die Ziffer vor dem Gleichheitszeichen entspricht dem Feld Index aus der Externer Sensor Tabelle.

### b) Line-Sensoren

```
>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"
```

Dieses Kommando gibt alle Line-Sensorwerte in jeweils einer Zeile aus. Als Parameter wird eine Liste aller Felder (entsprechend der Energie Sensor Tabelle) übergeben. In diesem Beispiel sind dies die Felder Absolute Active Energy (0), Power Active (1), Voltage (2), Current (3) und Reset Time (12).



Bei Geräten mit Overvoltage Protection wird bei dem "linesensor all" Kommando der Zustand der Protection mit ausgegeben ("OVP=x"). Eine "1" bedeutet Ok, eine "0" ein Ausfall der Protection.

### c) Port Sensoren

```
>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"
```

Dieses Kommando gibt alle Port-Sensorwerte in jeweils einer Zeile aus. Als Parameter wird eine Liste aller Felder (entsprechend der Energie Sensor Tabelle) übergeben. In diesem Beispiel sind dies die Felder Absolute Active Energy (0), Power Active (1), Vol- tage (2), Current (3) und Reset Time (12).

### d) Port-Relais anzeigen

```
>port all state 1 show
P1=ON,P2=OFF,P3=ON,P4=OFF,P5=OFF,P6=OFF,P7=OFF,P8=ON
```

Der Befehl "port all state {MODE0=0|MODE1=1|MODE2=2} show" gibt den Schaltzustand aller Relais zurück in 3 möglichen Formaten zurück.

## e) Port-Relais schalten

```
#port all state set "1,2,12" 1
OK.
```

Die Befehlssyntax "port all state set "{port\_list}" {OFF=0|ON=1}" setzt eine Liste von Ports auf den Zustand ON=1 oder OFF=0.

### 4.7.1 Console Cmd 8341 (DN-95637)

Kommando	Beschreibung	Hinweis
Logout	Go to login prompt enabled	2
Quit	Quit 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
Clock	Enters cmd group "clock"	
Clock enabled set {OFF=0 ON=1}	Enables ntp	
Clock enabled show	Shows if ntp enabled	
Clock timezone set {minutes}	Sets timezone	
Clock timezone show	Shows timezone	
Clock dst enabled set {OFF=0 ON=1}	Enables dst	
Clock dst enabled show	Shows if dst is enabled	
Clock manual set "{hh:mm:ss yyyy-mm-dd}"	Sets time and date manually	
Clock show	Shows 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	Shows ntp server name	
Console	Enters cmd group "console"	
Console version	Shows unique console version number	
Console telnet enabled set {OFF=0 ON=1}	Enables telnet on/off	
Console telnet enabled show	Shows if telnet enabled	
Console telnet port set {ip_port}	Sets telnet port	
Console telnet port show	Shows telnet port	
Console telnet raw set {OFF=0 ON=1}	Sets raw mode (disables editing) on/off	
Console telnet raw show	Shows if raw mode enabled	
Console telnet echo set {OFF=0 ON=1}	Enables echo on/off	
Console telnet echo show	Shows if echo enabled	
Console telnet activeneg set {OFF=0 ON=1}	Enables telnet active negotiation (IAC) on/off	
Console telnet activeneg show	Shows if active negotiation enabled	
Console telnet login set {OFF=0 ON=1}	Enables login on/off	
Console telnet login show	Shows if login enabled	
Console telnet login local set {OFF=0 ON=1}	Enables local login on/off	
Console telnet login local show	Shows if local login enabled	
Console telnet login radius set {OFF=0 ON=1}	Enables login für RADIUS on/off	
Console telnet login radius show	Shows if RADIUS login enabled	
Console telnet login delay set {OFF=0 ON=1}	Enables delay (after 3 login fails) on/off	
Console telnet login delay show	Shows if login delay enabled	
Console telnet user set "{username}"	Sets login user name	
Console telnet user show	Shows login user name	

Console telnet passwd set "{passwd}"	Sets login password	
Console telnet passwd hash set "{passwd}"	Sets login hashed password	
Email	Enters cmd group "email"	
Email enabled set {OFF=0 ON=1}	Enables email on/off	
Email enabled show	Shows if email is enabled	
Email sender set "{email_addr}"	Sets email sender address	
Email sender show	Shows email sender address	
Email recipient set "{email_addr}"	Sets email recipient address	
Email recipient show	Shows email recipient address	
Email server set "{dns_name}"	Sets email SMTP server address	
Email server show	Shows email SMTP server address	
Email port set "{ip_port}"	Sets email SMTP port	
Email port show	Shows email SMTP port	
Email security set "{NONE=0 STARTTLS=1 SSL=2}"	Sets SMTP connection security	
Email security show	Shows SMTP connection security	
Email auth set "{NONE=0 PLAIN=1 LOGIN=2}"	Sets email authentication	
Email auth show	Show email authentication	
Email user set "{username}"	Sets SMTP username	
Email user show	Shows SMTP username	
Email passwd set "{passwd}"	Sets SMTP password	
Email passwd hash set "{passwd}"	Sets crypted SMTP password	
Email testmail	Send test mail	
Ethernet	Enters cmd group "ethernet"	
Ethernet mac show	Shows MAC address	
Ethernet link show	Shows ethernet link state	
Ethernet phyprefer set "{10MBIT_HD=0 10MBIT_FD=1 100MBIT_HD=2 100MBIT_FD=3}"	Sets preferred speed for PHY Auto Negotiation	
Ethernet phyprefer show	Shows preferred speed for PHY Auto Negotiation	
Extsensor	Enters cmd group "extsensor"	
Extsensor 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 values	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 label	6
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 enables different event types 6,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	Enables different event types	6
Extsensor {port_num} {sen_type} {sen_field} events type show	Shows what event types are enabled	6
Extsensor {port_num} {sen_type} {sen_field} maxval set {num}	Sets maximum value for sensor	6
Extsensor {port_num} {sen_type} maxval show	Shows maximum value for sensor	6
Extsensor {port_num} {sen_type} {sen_field} min- val set {num}	Sets minimum value for sensor	6
Extsensor {port_num} {sen_type} {sen_field} min- val show	Shows minimum value for sensor	6
Extsensor {port_num} {sen_type} {sen_field} hyst set {num}	Sets hysteresis value for sensor	6
Extsensor {port_num} {sen_type} {sen_field} hyst show	Shows hysteresis value for sensor	6

Extensor {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
Extensor {port_num} {sen_type} {sen_field} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port show	Shows port for power port switching actions	6
Extensor {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
Extensor {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	
Extensor beeper set {OFF=0 ON=1}	Enables beeper sensor alarms	
Extensor beeper show	Shows if beeper sensor alarms are enabled	
http	Enters cmd group "http"	
http server set {HTTP_BOTH=0 HTTPS_ONLY=1 HTTP_ONLY=2}	Sets connection typed the webserver accepts	
http server show	Shows webserver accepting connection types	
http port set {ip_port}	Sets http port	
http port show	Shows http port	
http portssl set {ip_port}	Sets https port	
http portssl show	Shows https port	
http ajax enabled set {OFF=0 ON=1}	Enables ajax autorefresh on/off	
http ajax enabled show	Shows if ajax autorefresh enabled	
http passwd enabled set {OFF=0 ON=1}	Enables http password on/off	
http passwd enabled show	Shows if http password enabled	
http passwd user set "{passwd}"	Sets http user password	
http passwd admin set "{passwd}"	Sets http admin password	
http passwd hash user set "{passwd}"	Sets hashed http user password	
http passwd hash admin set "{passwd}"	Sets hashed http admin password	
ip4	Enters cmd group "ip4"	
ip4 hostname set "{name}"	Sets device hostname	
ip4 hostname show	Shows device hostname	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 routeradv 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	3
ip6 manual address {1_4} show	Shows manual IPv6 address	3
ip6 manual gateway set "{ip_address}"	Sets manual IPv6 gateway address	3
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 ping enabled set {OFF=0 ON=1}	Enables ICMP ping on/off	
ipacl ping enabled show	Shows if ICMP ping enabled	
ipacl enabled set {OFF=0 ON=1}	Enables IP filter on/off	
ipacl enabled show	Shows if IP filter enabled	
ipacl filter {ipacl_num} set "{dns_name}"	Sets IP filter {ipacl_num}	
ipacl filter {ipacl_num} show	Shows IP filter {ipacl_num}	
linesensor all {field_list} show	Shows energy sensors according field list of all line sensors	5
linesensor {line_num} {energy_sensor} value show	Shows energy sensor of given line	5
linesensor {line_num} ovp show	Show state of overvoltage protection	
linesensor {line_num} counter reset	Resets energy metering counter	
linesensor {line_num} label set „{name}“	Sets line meter to label	
linesensor {line_num} label show	Shows label of line meter	
linesensor {line_num} {energy_sensor} events set {OFF=0 ON=1}	Enables events on/off	
linesensor {line_num} {energy_sensor} events show	Shows if events are enabled	
linesensor {line_num} {energy_sensor} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER =5}"	Enables different event types	
linesensor {line_num} {energy_sensor} events type show	Shows what event types are enabled	
linesensor {line_num} {energy_sensor} maxval set {float}	Sets maximum value for line meter	
linesensor {line_num} {energy_sensor} maxval show	Shows maximum value for line meter	
linesensor {line_num} {energy_sensor} minval set {float}	Sets minimum value for line meter	
linesensor {line_num} {energy_sensor} minval show	Shows minimum value for line meter	
linesensor {line_num} {energy_sensor} hyst set {float}	Sets hysteresis value for line meter	
linesensor {line_num} {energy_sensor} hyst show	Shows hysteresis value for line meter	



Linesensor {line_num} {energy_sensor} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port set {port_num}	Sets port for power port switching actions	
Linesensor {line_num} {energy_sensor} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port show	Shows port for power port switching actions	
Linesensor {line_num} {energy_sensor} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} state set {OFF=0 ON=1 DISABLED=2}	Sets port state for power port switching actions	
Linesensor {line_num} {energy_sensor} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} state show	Shows port state for power port switching actions	
Linesensor {line_num} events set {OFF=0 ON=1}	LEGACY – enables event on/off	L
Linesensor {line_num} events show	LEGACY – shows if events are enabled	L
Linesensor {line_num} events type set {EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2, EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	LEGACY – enables different event types	L
Linesensor {line_num} events type show	LEGACY – shows what event types are enabled	L
Linesensor {line_num} maxval set {float}	LEGACY – sets maximum value for line meter	L
Linesensor {line_num} maxval show	LEGACY – shows maximum value for line meter	L
Linesensor {line_num} minval {float}	LEGACY – sets minimum value for line meter	L
Linesensor {line_num}minval show	LEGACY – shows minimum value for line meter	L
Linesensor {line_num} hyst set {float}	LEGACY – sets hysteresis value for line meter	L
Linesensor {line_num} hyst show	LEGACY – shows hysteresis value for line meter	L
Linesensor beeper set {OFF=0 ON=1}	Enables beeper for line meter alarms	
Linesensor beeper show	Shows if beeper for line meter alarms are enabled	
Modbus	Enters cmd group "modbus"	
Mobus enabled set <on=0 off=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	
Radius	Enters cmd group "radius"	
Radius {PRIMARY=0 SECONDARY=1} enabled set <off=0/on=1>	Enables radius client	
Radius {PRIMARY=0 SECONDARY=1} enabled show	Shows if radius client is enabled	
Radius {PRIMARY=0 SECONDARY=1} server set "<dns_name>"	Sets radius server address	
Radius {PRIMARY=0 SECONDARY=1} server show	Shows radius server address	
Radius {PRIMARY=0 SECONDARY=1} password	Sets radius server shared secret	
Radius {PRIMARY=0 SECONDARY=1} password hash set "{passwd}"	Sets radius server crypted shared secret	
Radius {PRIMARY=0 SECONDARY=1} auth timeout set {num_secs}	Sets server request timeout	
Radius {PRIMARY=0 SECONDARY=1} auth timeout show	Shows server request timeout	
Radius {PRIMARY=0 SECONDARY=1} retries set {num}	Sets server number of retries	
Radius {PRIMARY=0 SECONDARY=1} retries show	Shows server number of retries	
Radius chap enabled set <off=0/on=1>	Enables CHAP	
Radius chap enabled show	Shows if CHAP is enabled	
Radius message auth set <off=0/on=1>	Enables request message authentication	

Radius message auth show	Shows if request message authentication is enabled	
Radius default timeout set {num_secs}	Sets default session timeout (when not returned as session-timeout attribute)	
Radius default timeout show	Shows default session timeout	
Snmp	Enters cmd group "snmp"	
Snmp port set {ip_port}	Sets SNMP UDP port	
Snmp port show	Shows SNMP UDP port	
Snmp snmpget enabled set {OFF=0 ON=1}	Enables SNMP GET cmds on/off	
Snmp snmpget enabled show	Shows if SNMP GET cmds are enabled	
Snmp snmpset enabled set {OFF=0 ON=1}	Enables SNMP SET cmds on/off	
Snmp snmpset enabled show	Shows if SNMP SET cmds are enabled	
Snmp snmpv2 enabled set {OFF=0 ON=1}	Enables SNMP v2 on/off	
Snmp snmpv2 enabled show	Shows if SNMP v2 is enabled	
Snmp snmpv2 public set "{text}"	Enables SNMP v3 on/off	
Snmp snmpv2 public show	Shows if SNMP v3 is enabled	
Snmp snmpv2 private set "{text}"	Sets SNMP v2 public community	
Snmp snmpv2 private show	Shows SNMP v2 public community	
Snmp snmpv3 enabled set {OFF=0 ON=1}	Sets SNMP v2 private community	
Snmp snmpv3 enabled show	Shows SNMP v2 private community	
Snmp snmpv3 username set "{text}"	Sets SNMP v3 username	
Snmp snmpv3 username show	Shows SNMP v3 username	
Snmp snmpv3 authalg set {NONE=0 MD5=1 SHA1=2 SHA256=3 SHA384=4 SHA512=5}	Sets SNMP v3 authentication	
Snmp snmpv3 authalg show	Shows 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	Shows SNMP v3 privacy algorithm	
Snmp snmpv3 authpasswd set "{passwd}"	Sets SNMP v3 authentication password	
Snmp snmpv3 privpasswd set "{passwd}"	Sets SNMP v3 privacy password	
Snmp snmpv3 authpasswd hash set "{passwd}"	Sets SNMP v3 authentication hashed password	
Snmp snmpv3 privpasswd hash set "{passwd}"	Sets SNMP v3 privacy hashed password	
Snmp trap type set {NONE=0 V1=1 V2=2 V3=3}	Sets type of SNMP traps	
Snmp trap type show	Show SNMP trap type	
Snmp trap receiver {trap_num} set "{dns_name}"	Sets address and port of SNMP trap receiver {trap_num}	
Snmp trap receiver {trap_num} show	Show address and port of SNMP trap receiver {trap_num}	
Syslog	Enters cmd group "syslog"	
Syslog enabled set {OFF=0 ON=1}	Enables syslog msgs on/off	
Syslog enabled show	Shows if syslog enabled	
Syslog server set "{dns_name}"	Sets address of syslog server	
Syslog server show	Shows address of syslog server	
System	Enters cmd group "system"	

System restart	Restarts device	
System fabsettings	Restore fab settings and restart device	
System bootloader	Enters bootloader mode	
System flushdns	Flush DNS cache	
System uptime	Number of secons the device is running	
System panel enabled set {OFF=0 ON=1}	Blocks panel buttons when not enabled	
System panel enabled show	Shows if panel buttons are enabled	
System display enabled set {OFF=0 ON=1}	Dark display when not enabled	
System display enabled show	Show if display enabled	
System display default extsensor {port_num} {7x01=0 7x02=1 7x03=2} set {sen_field}	Sets default display to external sensor	
System display default linesensor {line_num} set {sen_field}	Sets default display to linesensor	
System display default show	Shows default display	
System display brightness set {brightness_num}	Sets display brightness	
System display brightness show	Shows display brightness	
Timer	Enters cmd group "timer"	
Timer enabled {OFF=0 ON=1}	Enables timer functions	
Timer enabled show	Shows if timer is enabled	
Timer syslog facility set {0..23}	Sets facility level for timer syslog	
Timer syslog facility show	Shows facility level for timer syslog	
Timer syslog verbose set {0..7}	Sets verbose level for timer syslog	
Timer syslog verbose show	Shows verbose level for timer syslog	
Timer {rule_num} enabled set {OFF=0 ON=1}	Enables rule	
Timer {rule_num} enabled show	Shows if rule is enabled	
Timer {rule_num} name set "{name}"	Sets name of rule	
Timer {rule_num} name show	Shows name of rule	
Timer {rule_num} {FROM=0 UNTIL=1} set "{yyyy-mm-dd}"	Sets data range of rule	
Timer {rule_num} {FROM=0 UNTIL=1} show	Shows data range of rule	
Timer {rule_num} trigger jitter set {0..65535}	Sets jitter for rule	
Timer {rule_num} trigger jitter show	Show jitter for rule	
Timer {rule_num} trigger random set {0..100}	Sets probability for rule	
Timer {rule_num} trigger random show	Shows 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	Shows time date list	
Timer {rule_num} action mode set {SWITCH=1 CLI=2}	Sets switch or cli cmd	
Timer {rule_num} action mode show	Shows if switch or cli cmd	
Timer {rule_num} action {SWITCH1=0 SWITCH2=1} {OFF=0 ON=1} set "{port_list}"	Sets port list for switch cmd	
Timer {rule_num} action {SWITCH1=0 SWITCH2=1} {OFF=0 ON=1} show	Shows port list for switch cmd	
Timer {rule_num} action delay set {0..65535}	Delay between cmds	
Timer {rule_num} action delay show	Shows delay between cmds	
Timer {rule_num} action console set "{cmd}"	Sets cmd string	
Timer {rule_num} action console show	Shows cmd string	
Timer {rule_num} action hash set "{data}"	Sets action binary form	
Timer {rule_num} action hash show	Shows 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	Shows console echo state	
Vt100 numeric set {OFF=0 ON=1}	Sets numeric mode	
Vt100 numeric show	Shows numeric mode state	
Vt100 reset	Resets terminal	

## Hinweise

1. Legacy - Der Befehl ist von einer neueren Version abgelöst worden
2. Befehl kann auf allen Ebenen ausgeführt werden
3. Die Ausgabe kann 2 Zeilen umfassen – die erste Zeile zeigt den aktuellen Zustand, die zweite Zeile den Status nach einem Neustart
4. Die Ausgabe kann mehrere Zeilen umfassen
5. Bitte die **Energie Sensor Tabelle** konsultieren, um den richtigen Index zu finden
6. Bitte die Tabellen **Externer Sensor Feld und Externer Sensor Typ** konsultieren, um den richtigen Index zu finden.

## Energie Sensor Tabelle "{energy\_sensor}"

Index	Beschreibung	Einheit
0	Forward Active Energy	Wh
1	Power Active	W
2	Voltage	V
3	Current	A
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	Forward Active Energy Resettable	Wh
10	Forward Reactive Energy	VARh
11	Forward Reactive Energy Resettable	VARh
12	Reset Time – sec. Since last Energy Counter Rest	s
13	Reverse Active Energy	Wh
14	Reverse Reactive Energy	VARh
15	Reverse Active Energy Resettable	Wh
16	Reverse Reactive Energy Resettable	VARh
17	Absolute Active Energy	Wh
18	Absolute Reactive Energy	VARh
19	Absolute Active Energy Resettable	Wh
20	Absolute Reactive Energy Resettable	VARh
21	Residual Current	A



Abhängig vom Gerätemodell wird die Messung des Fehlerstroms (Residual Current) nicht unterstützt.

### Externer Sensor Typ Tabelle "{sen\_type}"

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

Index	Description	Products
0	Temperatur	7001, 7101, 7201
0	Temperatur	7004, 7104, 7204
1	Temperatur, Luftfeuchtigkeit	7002, 7102, 7202
1	Temperatur, Luftfeuchtigkeit	7005, 7105, 7205
2	Temperatur, Luftfeuchtigkeit, Luftdruck	7006, 7106, 7206

### Externer Sensor Feld Tabelle "{sen\_field}"

Index	Description	Unit
0	Temperatur	°C
1	Luftfeuchtigkeit	%
2	Digitale Eingabe	bool
3	Luftdruck	hPa
4	Taupunkt	°C
5	Taupunkt Temperaturunterschied	°C

## 4.8 Modbus TCP

Wird Modbus TCP in der Konfiguration aktiviert, sind Ports (Relais) schaltbar und folgende Informationen abrufbar:

- Status der Ports (Relais)
- Status der DC-Eingänge
- Anzahl der Ports (Relais)
- Anzahl der Energiesensoren
- Messwerte der Energiesensoren
- Messwerte der externen Sensoren



Dieses Kapitel ist allgemein für alle Digitus Geräte gehalten. Je nach Gerätetyp sind Ports oder bestimmte Sensoren nicht verfügbar.



Alle Berechnungen in diesem Kapitel gehen von Adressen aus die bei "0" beginnen. Bei manchen Modbus TCP Utilities beginnen die Adressen aber bei 1. In diesem Fall muss zu den Adressen in diesem Kapitel eine 1 addiert werden. Bei Tests bitte beide Möglichkeiten probieren!

Die Unit-ID wird ignoriert, da das Gerät eindeutig über die IP-Adresse gekennzeichnet wird.

**Adressbereich:**

Geräte Resource	Start	Ende	Modbus Data Type
Power/Output Ports	0x000	0x3ff	Coils
DC Eingänge	0x400	0x7ff	Discrete Inputs
Infobereich	0x000	0x005	Input Registers
Externe Sensoren	0x100	0x1ff	Input Registers
Line Energie Sensoren	0x400	0x39ff	Input Registers
Port Energie Sensoren	0x3a00	0x6fff	Input Registers

Diese Funktionen werden unterstützt:

- Read Coils (0x01)

Liest den Status der Ports (Relais):

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

Response Code	1 Byte	0x01
Byte count	1 Byte	n
Coil Status	n Byte	each Bit represents a state

- Read Discrete Inputs (0x02)

Liest Status-Informationen:

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

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

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

- Write Single Coil (0x05)

Setzt den Status eines Ports (Relais):

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

Response Code	1 Byte	0x05
Output Address	2 Bytes	n

- Write Multiple Coils (0x0F)

Setzt den Status mehrerer Ports (Relais):

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

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

- Read Input Registers (0x04)

Liest 16-Bit Werte die je nach Adresse verschiedene Geräte Informationen beinhalten:

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

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

In den Input Registers sind verschiedene Status- und Messwerte des Gerätes angeordnet:

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

### Externe Sensoren:

Die Messwerte der externen Sensoren sind als Fixpunktarithmetik kodiert. Bei einem Faktor von z.B. 0,1 in der Einheit muss durch 10 geteilt werden, um zum realen Messwert zu gelangen. Ein Wert von 0x8000 bedeutet, das in dem entsprechenden Port kein Sensor eingesteckt ist, oder das entsprechende Feld im Sensor nicht verfügbar ist. Die Formel für die Adresse lautet (die Portnummern beginnen bei Null):

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

Offset	Sensor Feld	Einheit
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

Zum Beispiel hat die Luftfeuchtigkeit des zweiten Ports die Adresse:  $0x100 + 1 * 8 + 1 = 0x109$

### Energie Sensoren:

Wir unterscheiden bei den Energie-Sensoren zwischen den Line-Sensoren, die den Eingangsstromkreisen entsprechen, und den Port-Sensoren, die die Energie messen, die über den geschalteten Port geleitet wird. Die Messwerte der Energie-Sensoren werden als vorzeichenbehaftete 32-Bit Integer zurückgegeben. Auf der geraden Adresse sind erst die höherwertigen 16-Bit, dann folgen auf der ungeraden Adresse die niederwertigen 16-Bit. Für die Adresse gibt es folgende Formeln (die Werte für Line, Port und Phase beginnen bei Null):



Line:  $0x0400 + \text{Line} * 0x120 + \text{Phase} * 0x60 + \text{Offset} * 2$   
 Port:  $0x3a00 + \text{Port} * 0x120 + \text{Phase} * 0x60 + \text{Offset} * 2$



Bei Geräten mit nur einer Phase, wird in der Formel die Phase auf Null gesetzt.

### Beispiele:

"Power Active" bei 1. Line-Sensor und 3. Phase:  $0x400 + 0 * 0x120 + 2 * 0x60 + 1 * 2 = 0x4C2$

"Voltage" bei 2. Line-Sensor und einphasigem Gerät:  $0x400 + 1 * 0x120 + 2 * 2 = 0x524$

"Power Angle" bei 4. Port-Sensor und einphasigem Gerät:  $0x3a00 + 3 * 0x120 + 6 * 2 = 0x3d6c$

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



Ob die Messwerte "Residual Current" und "Neutral Current" unterstützt werden, hängt von dem jeweiligen Gerätemodell ab. Bei Messwerten wie "Neutral Current", die unabhängig von der Phase sind, werden für alle Phasen der gleiche Wert zurückgeliefert.

- Read Device Identification (0x2B / 0x0E)

Gibt Herstellernamen und Geräte Identifikation zurück:

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

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

#### 4.9 Nachrichten

In Abhängig von einstellbaren Ereignissen können vom Gerät verschiedene Nachrichtenarten verschickt werden. Folgende Nachrichtentypen werden unterstützt:

- Versendung von E-mails
- SNMP Traps
- Syslog Nachrichten

#### E-mail Benachrichtigungen

Bei folgenden Ereignissen werden E-Mail Benachrichtigungen ausgelöst:

- Einschalten des Geräts
- Überschreiten von Max/Min Werten der Sensoren
- Änderung des Sensor Digitaleingang
- Überschreiten von Max/Min Werten der gemessenen Stromaufnahme
- Überschreiten von Max/Min Werten der Differenzstrommessung Typ A

## **SNMP Traps**

SNMP-Traps können über das SNMP Protokoll an verschiedene Empfänger gesendet werden. Bei folgenden Ereignissen werden SNMP-Traps ausgelöst:

- Überschreiten von Max/Min Werten der Sensoren
- Änderung des Sensor Digitaleingangs
- Überschreiten von Max/Min Werten der gemessenen Stromaufnahmen
- Überschreiten von Max/Min Werten der Differenzstrommessung Typ A

## **Syslog Nachrichten**

Syslog-Nachrichten sind einfache Textnachrichten die per UDP an einen Syslog-Server verschickt werden. Unter Linux läuft normalerweise bereits ein Syslog-Daemon (z.B. syslog-ng), für Windows-Systeme (z.B. Windows 2000, XP, Vista, etc.) gibt es einige Freeware-Programme auf dem Markt. Die Syslog-Nachrichten werden bei folgenden Ereignissen gesendet:

- Einschalten des Geräts
- Ein- bzw. Ausschalten von Syslog in der Konfiguration
- Überschreiten von Max/Min Werten der Sensoren
- Änderung des Sensor Digitaleingangs
- Überschreiten von Max/Min Werten der gemessenen Stromaufnahme
- Überschreiten von Max/Min Werten der Differenzstrommessung Typ A
- Zustandsänderung des Überspannungsschutzes

## **5. Support**

Auf unseren Internetseiten unter [www.Digitus.info](http://www.Digitus.info) steht Ihnen die aktuelle Software zu unseren Produkten kostenlos zum Download zur Verfügung.

### **5.1 Datensicherheit**

Um das Gerät mit hoher Datensicherheit auszustatten, empfehlen wir folgende Maßnahmen:

- HTTP Passwort einschalten
- Ein eigenes HTTP Passwort einrichten
- Den Zugriff auf HTTP nur über SSL erlauben
- In SNMPv3 Authentifizierung und Verschlüsselung einschalten
- SNMP v2 abschalten
- In der E-Mail Konfiguration STARTTLS bzw. SSL einschalten
- Konfigurationsdateien sicher archivieren
- In der IP ACL nur die Geräte eintragen, die Zugriff auf das Gerät benötigen
- Login für Telnet oder serielle Konsolen setzen
- Da Telnet unverschlüsselt ist, nur in einer sicheren Umgebung einsetzen.
- Da Modbus TCP unverschlüsselt ist, nur in einer sicheren Umgebung aktivieren.
- In RADIUS "Message Authentication" einschalten.

### **Bei Zugriff aus dem Internet**

- Ein randomisiertes Passwort mit mindestens 32 Buchstaben benutzen
- Das Gerät möglichst hinter einer Firewall betreiben.

## 5.2 FAQ

### 1. Was kann ich machen, wenn das Gerät nicht mehr erreichbar ist?

- Ist die Status-LED rot, dann hat das Gerät keine Verbindung zum Switch. Stecken Sie das Ethernetkabel aus und ein. Wenn die Status-LED dann immer noch rot ist, versuchen Sie bitte andere Switches anzuschließen. Benutzen Sie keinen Switch, sondern verbinden z.B. ein Laptop direkt mit dem Gerät, ist darauf zu achten, dass ein gedrehtes Ethernetkabel angeschlossen ist.
- Bleibt die Status-LED nach dem Aus- und Einstecken des Ethernetkabels für eine längere Zeit orange, dann ist DHCP konfiguriert, aber es wurde kein DHCP-Server im Netz gefunden. Nach einem Timeout wird die letzte IP-Adresse manuell konfiguriert.
- Besteht eine physikalische Verbindung (Status-LED leuchtet grün) zum Gerät, aber der Webserver ist nicht zu erreichen, versuchen Sie das Gerät mit
- GBL\_Conf.exe zu finden. Sehen Sie ihr Gerät in der Liste, überprüfen Sie die dort eingestellten TCP/IP-Parameter und korrigieren Sie die Werte gegebenenfalls.
- Wird das Gerät im Bootloader-Modus nicht von GBL\_Conf.exe gefunden, haben Sie noch die Möglichkeit, die Einstellungen in den Werkszustand zurückzusetzen.

### 2. Warum dauert es auf der Webseite manchmal so lange, neue SNMPv3 Passwörter zu konfigurieren?

Die Authentifizierungsmethoden "SHA-384" und "SHA-512" werden rein in Software berechnet und können nicht die Crypto-Hardware nutzen. Wird auf der Konfigurationsseite z.B. "SHA-512" eingestellt, können einmalig bis zu ca. 45 Sekunden für die Schlüsselerzeugung vergehen.

### 3. Kann man mehrere E-Mail Empfänger eintragen?

Ja. In der E-Mail Konfiguration im Feld Recipient Address ist es möglich, mehrere E-Mail-Adressen, durch Kommata getrennt, einzugeben. Die Eingabegrenze liegt bei 100 Zeichen.

### 4. Warum haben sich nach dem Firmware-Update die MIB-Tabellen geändert?

Da die Anzahl der möglichen Event-Typen erhöht wurde, führte das bisherige Trap-Design zu einem Übermaß an Trap-Definitionen: Siehe Änderung im Trap-Design.

### 5. Ältere Firmware importieren

Bei einem Firmware-Update werden manchmal auch alte Datenformate zu neuen Strukturen konvertiert. Wird eine ältere Firmware neu eingespielt kann es zu Verlust der Konfigurationsdaten und der Energiezähler kommen! Sollte das Gerät dann nicht einwandfrei laufen, bitte den Werkszustand (Fab-Settings) wiederherstellen (z.B. von der Maintenance Seite).

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstörungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Maßnahmen zu ergreifen.

Hiermit erklärt die Assmann Electronic GmbH, dass die gedruckte Konformitätserklärung dem Produkt beiliegt. Sollte die Konformitätserklärung fehlen, kann diese postalisch unter der unten genannten Herstelleradresse angefordert werden.

**[www.assmann.com](http://www.assmann.com)**

Assmann Electronic GmbH  
Auf dem Schüffel 3  
58513 Lüdenscheid  
Germany

