

Anleitung



Expert Net Control 2302



© 2019 GUDE Systems GmbH
Handbuch Ver. 1.0.3
ab Firmware Ver. 1.0



1. Gerätebeschreibung	5
1.1 Sicherheitserklärung	6
1.2 Lieferumfang	6
1.3 Beschreibung	6
1.4 Anschluss und Inbetriebnahme	8
1.4.1 Anschlussbeispiel	9
1.5 Technische Daten	10
1.6 Sensoren	10
2. Bedienung	13
2.1 Bedienung am Gerät	14
2.2 Control Panel	14
2.3 Maintenance	16
2.3.1 Maintenance Seite	18
2.3.2 Konfigurationsmanagement	20
2.3.3 Bootloader-Aktivierung	21
3. Konfiguration	23
3.1 Output Ports	24
3.1.1 Watchdog	25
3.2 Input Ports	27
3.3 Ethernet	27
3.3.1 IP Address	28
3.3.2 IP ACL	29
3.3.3 HTTP	30
3.4 Protocols	31
3.4.1 Console	31
3.4.2 Syslog	32
3.4.3 SNMP	33
3.4.4 Radius	34
3.4.5 Modbus TCP	35
3.5 Sensors	36
3.5.1 Port Switching	37
3.6 E-Mail	38
3.7 Front Panel	39
4. Spezifikationen	40
4.1 IP ACL	41
4.2 IPv6	41
4.3 Radius	42

4.4	Automatisierte Zugriffe	42
4.5	SNMP	43
4.5.1	Geräte MIB 2302	46
4.6	SSL	46
4.7	Konsole	49
4.7.1	Console Cmd 2302	52
4.8	Modbus TCP	58
4.9	Nachrichten	62
5.	Support	63
5.1	Datensicherheit	64
5.2	Kontakt	64
5.3	Konformitätserklärungen	65
5.4	FAQ	65
	Stichwortverzeichnis	66

Gerätebeschreibung

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.
- Verbinden Sie das Gerät mit dem Stromnetz (230V AC) oder mit einem Steckernetzteil (10V bis 24V AC, 12V bis 28V DC, bei 4 Watt Leistungsaufnahme). Auf keinen Fall darf das Gerät gleichzeitig mit dem Stromnetz und Steckernetzteil gleichzeitig gespeist werden!
- Die verwendeten Stromkabel, Stecker und Steckdosen müssen sich in einwandfreiem 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.

1.2 Lieferumfang

Im Lieferumfang enthalten sind:

- Expert Net Control 2302
- CD-ROM mit Handbuch und Softwaretools

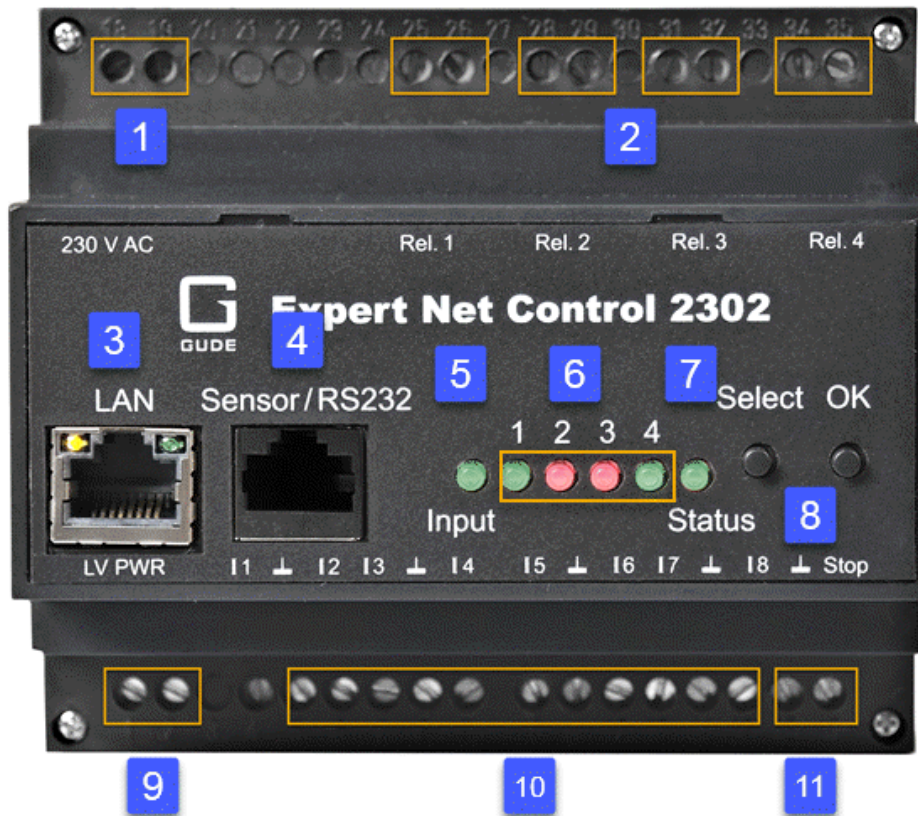
1.3 Beschreibung

Der **Expert Net Control 2302** kann 4 Relaisausgänge schalten und 8 passive Signaleingänge überwachen. Das Gerät hat folgende Features:

- Hutschienenmontage
- 4 schaltbare, potenzialfrei Relaisausgänge mit Schaltspannung (230V AC 16A, 24V DC 10A).
- Relais verfügen auch bei sehr kleinen Lasten über hohe Kontaktzuverlässigkeit
- 8 eigenständige, passive Signaleingänge für die Abfrage von NO/NC-Geräten (z.B. Türkontakt, Rauchmelder etc.)
- Stop-Eingang für Abschaltung aller Relais

- Schaltzustand und Einschaltverzögerung (0...9999 Sekunden) für jeden Relaisausgang nach Stromausfall einstellbar
- Programmierbare Ein-/Ausschaltsequenz 4-Kanal-Watchdog, jedem Output Port kann ein eigener Watchdog (ICMP/TCP) zugewiesen werden
- Anschluss für einen externen Sensor zur Umgebungsüberwachung (Temperatur, Luftfeuchtigkeit und Luftdruck)
- Betrieb mit 230 V Wechselspannung oder 24 V Gleichspannung
- möglich (Anschlussklemmen)
- Einfache und flexible Konfiguration über Webbrowser, Windows- oder Linux-Programm
- Erzeugung von Nachrichten (E-Mail, Syslog und SNMP Traps) und Schalten der Relais in Abhängigkeit von der Eingangsüberwachung oder der externen Sensoren
- Firmware-Update im laufenden Betrieb über Ethernet möglich
- IPv6-ready
- HTTP/HTTPS, E-Mail (SSL, STARTTLS), DHCP, Syslog
- SNMPv1, v2c, v3 (Traps)
- Modbus TCP Support
- Konsolensteuerung über Telnet
- TLS 1.0, 1.1, 1.2
- Zugriffsschutz durch IP-Zugriffskontrolle
- Geringer Eigenverbrauch
- Steuerbar über iOS- und Android-App Gude Control
- Geringer Eigenverbrauch, typ. 2 W
- Entwickelt und produziert in Deutschland

1.4 Anschluss und Inbetriebnahme



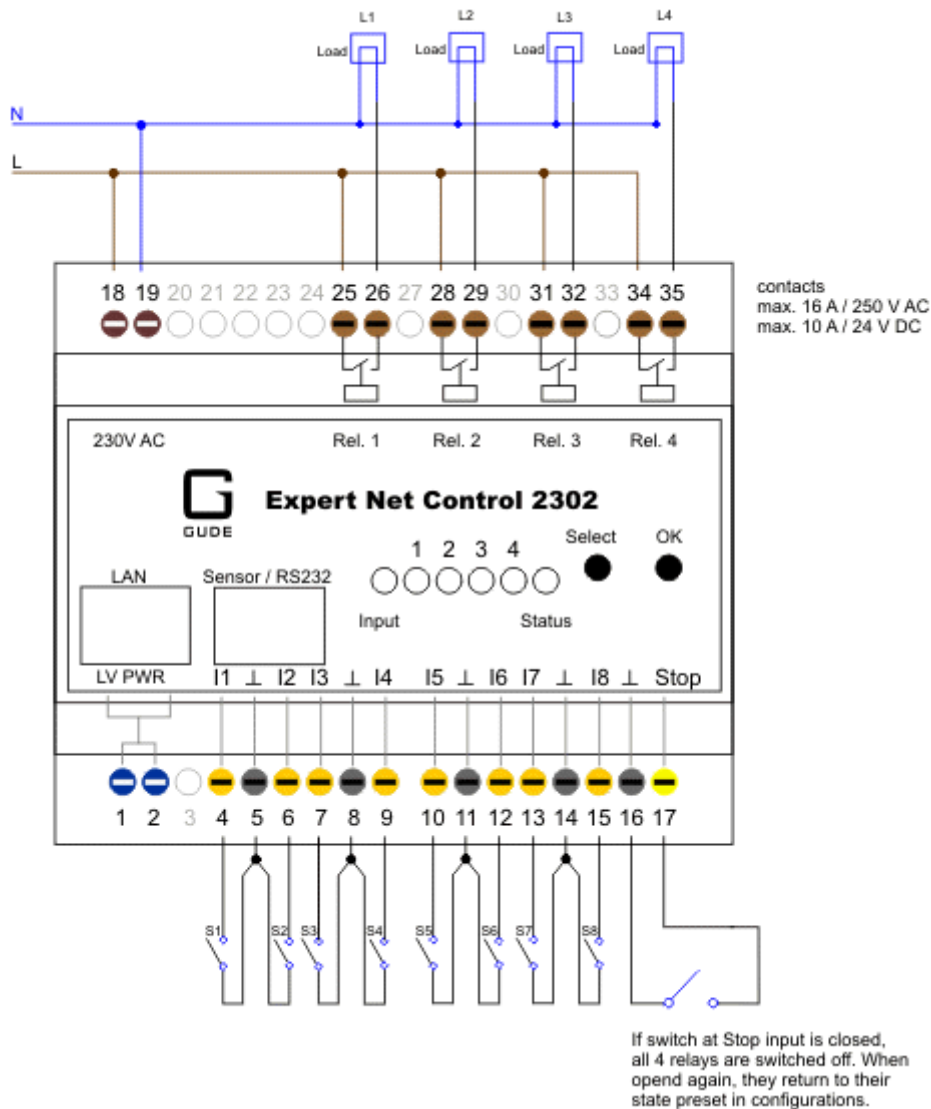
1. 230V AC Stromversorgung
2. Vier Relais Ausgänge (potenzialfrei)
3. Netzwerkanschluss (RJ45)
4. LAN Anschluss für Sensor (RJ45)
5. Aktivitäts-LED (Input) für digitale Eingänge
6. 4 Kontroll-LEDs für Relais Ausgänge
7. Status-LED
8. Taster für Select und OK
9. Alternative Niederspannung-Stromversorgung (Low Voltage PoWER)
10. Acht passive Eingänge (mit GND (⏚)) für jeweils 2 Eingänge)
11. Stop-Eingang (mit GND (⏚)) für Abschaltung aller Relais

Inbetriebnahme

- Verbinden Sie das Gerät mit dem Stromnetz (230V AC) oder mit einem Steckernetzteil (10V bis 24V AC, 12V bis 28V DC, bei 4 Watt Leistungsaufnahme). Auf keinen Fall darf das Gerät gleichzeitig mit dem Stromnetz und Steckernetzteil gleichzeitig gespeist werden!
- Stecken Sie das Netzkabel in die Ethernetbuchse (RJ45).
- Verbinden Sie die Relais mit den Lasten die betrieben werden sollen.
- Stellen Sie Kontakt zwischen den Leitungen die überwacht werden sollen und den digitalen Eingängen her. Um einen Eingangsstromkreis zu schließen, muss eine Verbindung zwischen einem Massepin (⏚) und dem jeweiligen Eingangspin hergestellt werden.
- Schließen Sie (falls vorhanden) einen Sensor an.

1.4.1 Anschlussbeispiel

An dieser Stelle ein Beispiel mit Blockschaltbild in dem das Gerät mit 230V AC versorgt wird, und in dem vier Wechselspannungslasten (L1 - L4) angeschlossen sind. Zusätzlich sind die Eingänge mit acht Schaltern (S1 - S8) belegt, sowie der Stop-Eingang mit dem Taster PB1 verbunden.



1.5 Technische Daten

Anschlüsse	1 x Ethernetanschluss (RJ45) 1 x Netzanschluss 230V AC 1 x Alternative Niederspannung-Stromversorgung 12 x Schraubklemme mit 8 x Eingang und 4 x GND 8 x Schraubklemme mit 4 x Relais Schliesserkontakt (230V AC 16A, 24V DC 10A) 2 x Schraubklemme mit 1 x Stop Eingang und 1 x GND 1 x RJ45 für externen Sensor
Netzwerkanbindung	10/100 MBit/s 10baseT Ethernet
Protokolle	TCP/IP, HTTP/HTTPS, SNMP v1/v2c/v3, SNMP traps, Syslog, E-Mail (SMTP)
Spannungsversorgung	internes Netzteil (230V AC) alternativ: 10V bis 24V AC, 12V bis 28V DC (bei 4 Watt Leistungsaufnahme)
Umgebung	<ul style="list-style-type: none"> • Betriebstemperatur 0°C bis 50°C • Lagertemperatur -20 °C - 70 °C • Luftfeuchtigkeit 0% - 95% (nicht kondensierend)
Gehäuse	Kunststoff schwarz
Maße	105mm x 70mm x 90mm (L x H x T)
Gewicht	ca. 300g

1.6 Sensoren

Am **Expert Net Control 2302** kann ein externer Sensor der Firma Gude angeschlossen werden. Aktuell sind folgende Sensoren verfügbar



Feuchte/Temperatursensor 7102 (End-of-Life)	
Kabellänge	≈ 2m
Anschluss	RJ45
Temperaturbereich	-20°C bis +80°C, ±0,5°C (maximal) und ±0,3°C (typisch)
Luftfeuchtebereich (nicht kondensierend)	0-100%, ±3% (maximal) und ±2% (typisch)

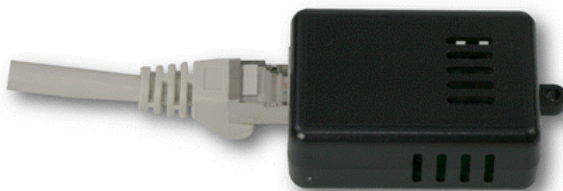


7101



7104 - 7106

Name	7101	7104	7105	7106
Kabellänge	≈ 2m	≈ 2m	≈ 2m	≈ 2m
Anschluss	RJ45	RJ45	RJ45	RJ45
Temperaturbereich	-20°C bis +80°C bei ±2°C (maximal) und ±1°C (typisch)	-20°C bis +80°C bei ±2°C (maximal) und ±1°C (typisch)	-20°C bis +80°C bei ±2°C (maximal) und ±1°C (typisch)	-20°C bis +80°C bei ±2°C (maximal) und ±1°C (typisch)
Luftfeuchtebereich (nicht kondensierend)	-	-	0-100%, ±3% (maximal) und ±2% (typisch)	0-100%, ±3% (maximal) und ±2% (typisch)
Luftdruckbereich (voll)	-	-	-	± 1 hPa (typisch) bei 300 ... 1100 hPa, 0 ... +40 °C
Luftdruckbereich (erw.)	-	-	-	± 1.7 hPa (typisch) bei 300 ... 1100 hPa, -20 ... 0 °C
Schutz	IP68	-	-	-



7201, 7202

Gerätebeschreibung

Name	7201	7202
Kabellänge	-	-
Anschluss	RJ45	RJ45
Temperaturbereich	-20°C bis +80°C bei ±2°C (maximal) und ±1°C (typisch)	-20°C bis +80°C bei ±2°C (maximal) und ±1°C (typisch)
Luftfeuchtebereich (nicht kondensierend)	-	0-100%, ±3% (maximal) und ±2% (typisch)

Die Sensoren werden nach dem Anschließen automatisch erkannt. Auf der "Control Panel" Webseite werden die Sensorwerte direkt angezeigt:

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

Ein Klick auf den Link in der "Name" Spalte klappt die Anzeige der Min und Max Werte auf. Die Werte in einer Spalte können über den "Reset" Knopf zurückgesetzt werden. Der "Reset" Knopf in der Namensspalte löscht alle gespeicherten Min und Max Werte.

Id	Name	Temperature °C	Humidity %	Dew Point °C	Dew Diff °C
1: 7102	7102	25.5	46.6	13.2	12.3
	24h min	25.4	46.0	13.1	12.2
	24h max	25.9	47.0	13.5	12.5
	<input type="button" value="Reset"/>	<input type="button" value="Reset"/>	<input type="button" value="Reset"/>	<input type="button" value="Reset"/>	<input type="button" value="Reset"/>

Bedienung

2 Bedienung

2.1 Bedienung am Gerät



Schalten

Den aktuellen Schaltzustand des Ausgangs erkennt man an den dazugehörigen Port-LEDs. Leuchtet die LED grün, ist der Port eingeschaltet, ist die LED rot, ist der Ausgangsport ausgeschaltet. Am Gerät befinden sich die Taster „Select“ und „Ok“. Wenn Sie „Select“ drücken, beginnt die LED für den ersten Ausgang an zu blinken, d.h. der Ausgang ist ausgewählt. Drücken Sie „Select“ erneut, um den nächsten Ausgang auszuwählen. Halten Sie den Taster „Ok“ für zwei Sekunden gedrückt, wird der Zustand des gewählten Ausgangs umgeschaltet.

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"](http://IP-Adresse) auf und loggen Sie sich ein.

Control Panel Configuration Maintenance Logout

ON 1: Output Port

ON 2: Output Port

OFF 3: Output Port

OFF 4: Output Port

Port	Name	logical state	time since transition	toggle count
Input 1	Input	● 0: off / open	00:43:05	1
Input 2	Input	● 0: off / open	00:43:05	1
Input 3	Input	● 0: off / open	00:43:05	1
Input 4	Input	● 0: off / open	00:43:05	1
Input 5	Input	● 0: off / open	00:43:05	1
Input 6	Input	● 0: off / open	00:43:05	1
Input 7	Input	● 0: off / open	00:43:05	1
Input 8	Input	● 0: off / open	00:43:05	1

auto logout in 298s

Die Webseite bietet einen Überblick über den Schaltzustand, sowie den Sensor, sofern er angeschlossen ist. Klickt man auf einen einzelnen Port, dann erscheinen die Schaltflächen, um den Port zu kontrollieren:

OFF 1: Output Port

On Off Reset Batch Close

Das Portsymbol ist grün, wenn das Relais geschlossen ist, oder rot bei offenem Zustand. Ein zusätzliches kleines Uhrensymbol signalisiert, dass ein Timer aktiv ist. Timer werden durch Einschaltverzögerung, Reset oder Batchmode aktiviert.



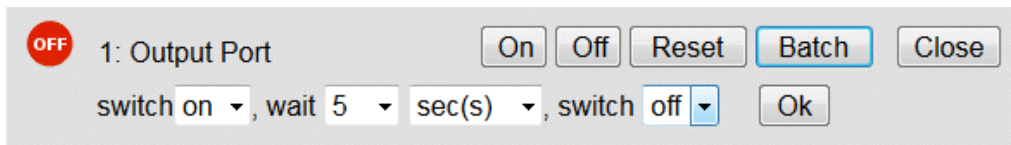
Ein aktivierter Watchdog wird durch ein Augensymbol dargestellt. Ein "X" bedeutet, dass die zu überwachende Adresse nicht aufgelöst werden konnte. Zwei kreisförmige Pfeile zeigen den Zustand Booting an.



Der Ausgang kann über die Buttons "On" und "Off" manuell geschaltet werden. Ist der Ausgang eingeschaltet, kann er durch Druck auf "Reset" ausgeschaltet werden, bis er sich dann nach einer Verzögerung wieder einschaltet. Diese Verzögerungszeit wird durch den Parameter Reset Duration bestimmt, der im Kapitel "Configuration - Output Ports" beschrieben wird. Der Button "Close" lässt die Schaltflächen wieder verschwinden.

Batchmode

Möchte man den Zustand des Ports für eine festgelegte Zeitspanne ändern, kann man mit Hilfe der Dropdown-Werte die Schaltvorgänge ("switch on" bzw. "switch off") sowie die Wartezeit dazwischen (in Sekunden, Minuten oder Stunden) auswählen.



Optional kann das Gerät auch über ein Perl-Skript oder externe Programme wie wget geschaltet werden. Mehr Informationen dazu erhalten Sie in unserem Support-Wiki unter www.gude.info/wiki.

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

Die Webseite enthält eine Status-Übersicht aller passiven Signaleingänge, die Zeit seit der letzten Änderung, und einen Zähler der Schaltwechsel. Der Name und Text für einen logischen Zustand eines jeden Eingangs wird im Kapitel Configuration-Input Ports ^[27] konfiguriert.

2.3 Maintenance

Die aktuelle Gerätegeneration mit IPv6 und SSL erlaubt es alle Wartungsfunktionen im Webinterface auf der Maintenance Seite ^[18] 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 Werkszustand
- Sprung in den Bootloader
- Löschen des DNS-Cache

Aktualisierung von Firmware, Zertifikat oder Konfiguration

Auf der Maintenance Webseite ^[18] 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 Geräteneustart 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.

Aktionen im Bootloader-Modus

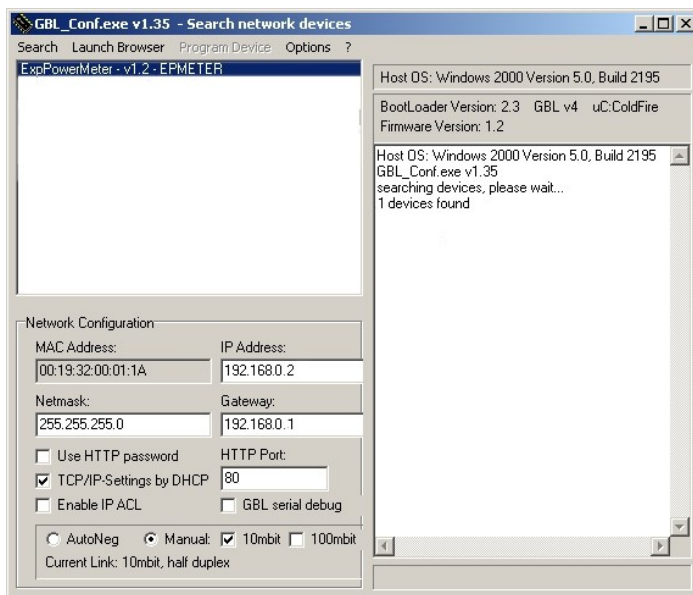
Falls das Webinterface des Geräts nicht mehr erreichbar ist, so kann das Gerät in den Bootloader-Modus gebracht werden (siehe Kapitel Bootloader-Aktivierung ^[21]). Dort lassen sich mit Hilfe der Applikation "GBL_Conf.exe" folgende Funktionen ausführen:

- Setzen von IPv4-Adresse, Netzmaske, Gateway
- Ein- und Ausschalten des HTTP-Passworts
- Ein- und Ausschalten der IP-ACL
- Wiederherstellung des Werkszustands
- 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.gude.info erhältlich und befindet sich auch auf der beiliegenden CD-ROM.



Oberfläche GBL_Conf.exe

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 only".
- 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.

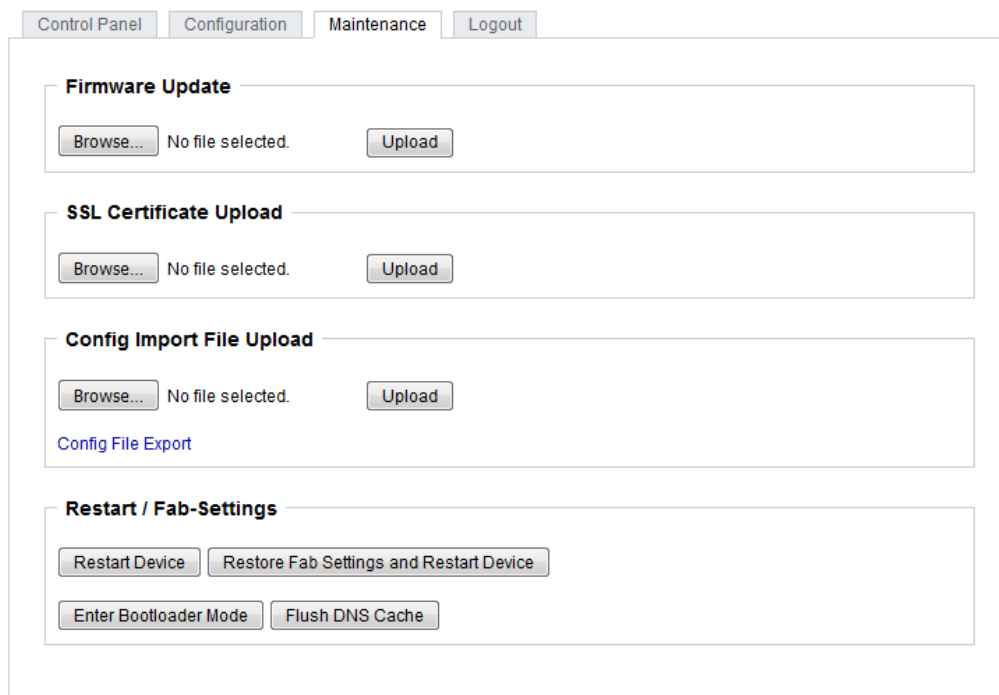
Werkzustand

Das Gerät lässt sich per Webinterface von der Maintenance Seite ^[18] oder aus dem Bootloader-Modus (siehe Kapitel Bootloader-Aktivierung ^[27]) 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.




Firmware Update: Führt ein Firmware-Update durch.


SSL Certificate Upload: Speichert ein eigenes SSL Zertifikat ab. Siehe das Kapitel "SSL [47]" 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 Relais-zustände.

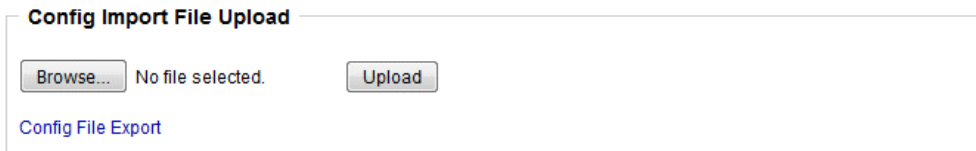
Restore Fab Settings and Restart Device: Führt einen Neustart aus und setzt das Gerät in den Werkszustand [22].

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.




Config Import File Upload

Browse... No file selected. Upload

[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
```

Kein Ausgabe der Default-Werte

Die Konfigurationsdatei enthält (mit Ausnahmen) nur Werte die vom Default abweichen. Der Befehl "system fabsettings" (gehe zu Werkszustand) 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 das Programm "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 wieder herstellen.

 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"

Werkszustand

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 Software:

- 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)

Konfiguration

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 Output Ports

The screenshot shows the 'Output Ports' configuration page. At the top, there are tabs for 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. Below these, there is a breadcrumb trail: 'Ports · Ethernet · Protocols · Sensors · E-Mail · Front Panel'. Underneath, there are links for 'Output Ports' and 'Input Ports'. The main content area is titled 'Output Ports' and contains a list of configuration items for the first output port, '1: Output Port'. The items are: 'Choose Output Port to configure:' (a dropdown menu showing '1: Output Port'), 'Label:' (a text input field containing 'Output Port'), 'Initialization status (coldstart):' (radio buttons for 'on', 'off', and 'remember last state', with 'off' selected), 'Initialization delay:' (a text input field containing '0' followed by 's'), 'Repower delay:' (a text input field containing '0' followed by 's'), 'Reset duration:' (a text input field containing '10' followed by 's'), and 'Enable watchdog:' (radio buttons for 'yes' and 'no', with 'no' selected). An 'Apply' button is located at the bottom of the configuration area.

Choose Output Port to configure: Dieses Feld dient zur Selektion des Output Ports der konfiguriert werden soll.

Label: Hier kann ein Name mit maximal 15 Zeichen für jeden der Output Ports vergeben werden. Mit Hilfe des Namens kann eine Identifikation des an den Port angeschlossenen Gerätes erleichtert werden.

Einschaltüberwachung

Es ist wichtig das der Zustand der Output Ports nach einem Stromausfall bei Bedarf wiederhergestellt werden kann. Daher lässt sich jeder Output Port mit Initialization status auf einen bestimmten Einschaltzustand konfigurieren. Diese Einschaltsequenz kann über den Parameter Initialization Delay verzögert durchgeführt werden. Es findet in jedem Fall eine minimale Verzögerung von einer Sekunde zwischen dem Schalten der Ports statt.

Initialization status (coldstart): Dies ist der Schaltzustand, den der Output Port beim Einschalten des Gerätes annehmen soll (on, off, remember last state). Die Einstellung *remember last state* speichert im EEPROM den zuletzt manuell eingestellten Zustand des Output Ports.

Initialization delay: Hier kann eine Verzögerung des Output Ports festgelegt werden, wenn der Output Port durch Einschalten des Geräts geschaltet werden soll. Die Verzögerung kann bis zu 8191 Sekunden dauern. Das entspricht ungefähr einem Zeitraum von zwei Stunden und 20 Minuten. Ein Wert von Null bedeutet, dass die Initialisierung ausgeschaltet ist.

Repower delay: Wenn diese Funktion aktiviert ist (Wert größer als 0), schaltet sich der Power Port nach einer vorgegebenen Zeit automatisch wieder ein, nachdem er deaktiviert wurde. Im Gegensatz zum *Reset* Schalter gilt diese Funktion für alle Schaltvorgänge, auch über SNMP oder die serielle Schnittstelle.

Reset Duration: Wenn der *Reset* Schalter im Switching Menü ausgelöst wird, wartet das Gerät die hier eingegebene Zeit (in Sekunden) zwischen Aus- und Wiedereinschalten des Output Ports.

Enable watchdog: Aktiviert die Watchdog Funktion für diesen Output Port.

3.1.1 Watchdog

• Enable watchdog: yes no

• Ping type: ICMP TCP

• Hostname:

• Ping interval: s

• Ping retries:

• Watchdog mode:

- Reset port when host down:
 - Infinite wait for booting host after reset
 - Repeat reset on booting host after ping timeouts
- Switch off once when host down
- IP Master-Slave port:
 - host comes up -> switch on, host goes down -> switch off
 - host goes down -> switch on, host comes up -> switch off

Mit der Watchdog Funktion können verschiedene Endgeräte überwacht werden. Dafür werden entweder ICMP-Pings oder TCP-Pings an das zu überwachende Gerät geschickt. Werden diese Pings innerhalb einer bestimmten Zeit (sowohl die Zeit, als auch die Anzahl der Versuche sind einstellbar) nicht beantwortet, wird der Output Port zurückgesetzt. Dadurch können z.B. nicht antwortende Server oder NAS Systeme automatisch neu gestartet werden. Die Betriebsart IP Master-Slave port erlaubt es, einen Port in abhängig von der Erreichbarkeit eines Endgerätes zu schalten.

Im Switching-Fenster geben die Watchdogs, wenn aktiviert verschiedene Informationen aus. Die Informationen werden farblich gekennzeichnet.

- Grüner Text: Der Watchdog ist aktiv und empfängt regelmäßig Ping-Antworten.
- Oranger Text: Der Watchdog wird gerade aktiviert, und wartet auf die 1. Ping-Antwort.
- Roter Text: Der Watchdog ist aktiv und empfängt keine Ping-Antworten mehr von der eingetragenen IP Adresse.

Bei der Aktivierung des Watchdogs bleibt die Anzeige solange orange bis der Watchdog das erste Mal eine Ping-Antwort empfängt. Erst danach schaltet der Watchdog auf aktiv um. Auch nach einer Watchdog Auslösung und einem anschließenden Output Port Reset bleibt die Anzeige orange, bis das neugestartete Gerät wieder auf Ping requests antwortet.

Sie können sowohl Geräte in Ihrem eigenen Netzwerk überwachen, als auch Geräte in einem externen Netzwerk um beispielsweise die Betriebsbereitschaft Ihres Router zu prüfen.

Enable watchdog: Aktiviert die Watchdog Funktion für diesen Output Port.

Watchdog type: Hier können Sie zwischen der Überwachung per ICMP Pings oder TCP Pings auswählen.

- ICMP Pings: Die klassischen Pings (ICMP echo request). Sie können genutzt werden um die Erreichbarkeit von Netzwerkgeräten (zum Beispiel einem Server) zu prüfen.
- TCP Pings: Mit TCP-Pings können Sie prüfen, ob ein TCP-Port auf dem Zielgerät einen TCP-Connect annehmen würde. Es sollte daher ein erreichbarer TCP-Port ausgesucht werden. Eine klassische Wahl wäre z.B. Port 80 für http, oder Port 25 für SMTP.

TCP port: Den zu überwachende TCP-Port eingeben. Bei ICMP-Pings muss kein TCP-Port eingegeben werden.

Hostname: Name oder IP-Adresse des zu überwachenden Netzwerkgeräts.


Ping interval: Bestimmen Sie die Häufigkeit (in Sekunden) mit der das Ping Paket zum jeweiligen Netzwerkgeräte geschickt wird, um dessen Einsatzbereitschaft zu prüfen.

Ping retries: Nach dieser Anzahl von aufeinander folgenden, nicht beantworteten Ping Requests gilt das Gerät als inaktiv.

Watchdog mode: Bei der Einstellung Reset port when host down wird der Output Port ausgeschaltet, und nach der in der Reset Duration eingestellten Zeit wieder eingeschaltet. Bei Switch off once when host down bleibt der Output Port deaktiviert.

Im Auslieferungszustand (Infinite wait for booting host after reset) überwacht der Watchdog das angeschlossene Gerät. Antwortet dieses nach einer eingestellten Zeit nicht mehr, führt der Watchdog die eingestellte Aktion durch, i.R. einen Reset des Output Ports. Jetzt wartet der Watchdog bis sich das überwachte Gerät wieder am Netz meldet. Dies kann je nach Bootdauer des überwachten Gerätes mehrere Minuten dauern. Erst wenn dieses Gerät im Netz wieder erreichbar ist wird der Watchdog neu scharf gestellt. Ist die Option Repeat reset on booting host after x ping timeout aktiviert, wird dieser Mechanismus überbrückt. Jetzt wird der Watchdog nach N Ping Intervallen (Eingabefeld ping timeouts) automatisch wieder scharf geschaltet.

Setzt man den Watchdog in den IP Master-Slave Betrieb, wird der Port abhängig von der Erreichbarkeit eines Endgerätes geschaltet. Abhängig von der Konfiguration der Port wird eingeschaltet, wenn das Endgerät erreichbar ist, oder umgekehrt.

 Die Option Repeat reset on booting host after x ping timeout birgt folgende Gefahr: Ist an dem zu überwachenden Port z.B. ein Server angeschlossen der lange für einen Bootvorgang benötigt, weil er einen Filesystemcheck durchführt, so würde der Server vermutlich die Auslösezeit des Watchdog überschreiten. Der Server würde aus- und wieder eingeschaltet, und der Filesystemcheck erneut gestartet. Dies würde sich endlos wiederholen.

3.2 Input Ports

Output Ports - [Input Ports](#)

Configuration - Input Ports

- Choose Input port to configure: Input 1 : Input
- Name: Input
- Inverted input: yes no
- Input HI text message: on / closed
- Input LOW text message: off / open
- Enable input events: yes no
 - Message channels: Syslog SNMP Email
- On input is HI: Switch port - to -
- On input is LOW: Switch port - to -

Apply

Choose Input port to configure: Dieses Feld dient zur Selektion des Input Ports der konfiguriert werden soll.

Name: Hier kann ein Name mit maximal 15 Zeichen für jeden der Input Ports vergeben werden. Mit Hilfe des Namens kann eine Identifikation des an den Port angeschlossenen Gerätes erleichtert werden.

Inverted Input: Invertiert die Zuordnung des Eingangsignals zu einem logischen HI / LOW Status.

Input HI Text Message: Text Anzeige im Control Panel und in Nachrichten wenn ein HI Signal am Input Port anliegt.

Input LOW Text Message: Text Anzeige im Control Panel und in Nachrichten wenn ein LOW Signal am Input Port anliegt.

Enable input events: Schaltet die Überwachung der Input Ports ein.

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

On input is HI: Schaltaktion wenn Input Port von LOW zu HI wechselt.

On input is LOW: Schaltaktion wenn Input Port von HI zu LOW wechselt.

3.3 Ethernet

3.3.1 IP Address

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

Hostname

• Hostname:

IPv4

• Use IPv4 DHCP: yes no

• IPv4 Address:

• IPv4 Netmask:

• IPv4 Gateway address:

• IPv4 DNS address:

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.

IP V4 Address: Die IP-Adresse des Gerätes.

IPv4 Netmask: Die Netzmaske im verwendeten Netz.

IPv4 Gateway address: 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

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.

IPv6 (manual)

- IPv6 Addresses:

2007:7dd0:ffc1:0:219:32ff:fe00:996d	/64
	/64
	/64
	/64

- IPv6 DNS addresses:

2007:7dd0:ffc1:0:20c:29ff:feaf:93c

- IPv6 Gateway address:

fe80::20c:29ff:feaf:93c

3.3.2 IP ACL

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

ICMP Ping

- Reply ICMP ping requests: yes no

IP Access Control List

- Enable IP filter: yes no


1. Grant IP access to host/net:	1234::4ef0:eec1:0:219:32ff:fe00:f12	Delete	Add
2. Grant IP access to host/net:	192.168.1.84	Delete	Add
3. Grant IP access to host/net:	mypc.locdom	Delete	Add
4. Grant IP access to host/net:	192.168.1.0/24	Delete	Add
5. Grant IP access to host/net:	1234:4ef0:eec1:0::/64	Delete	Add

Apply

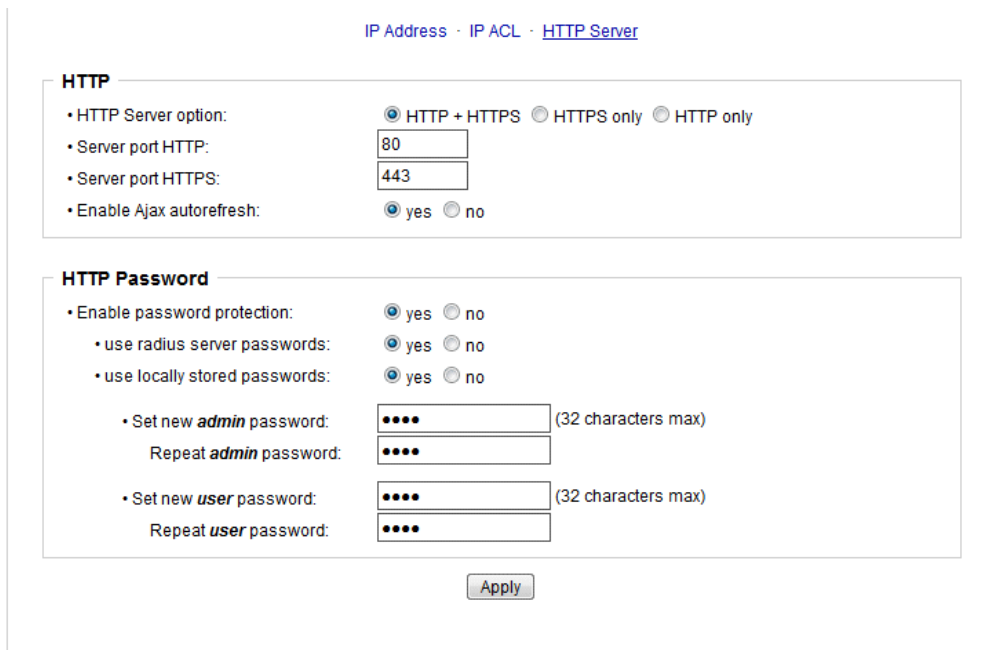
Reply ICMP ping requests: Wenn Sie diese Funktion aktivieren, antwortet das Gerät auf ICMP Pings aus dem Netzwerk.

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.

3.3.3 HTTP




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.

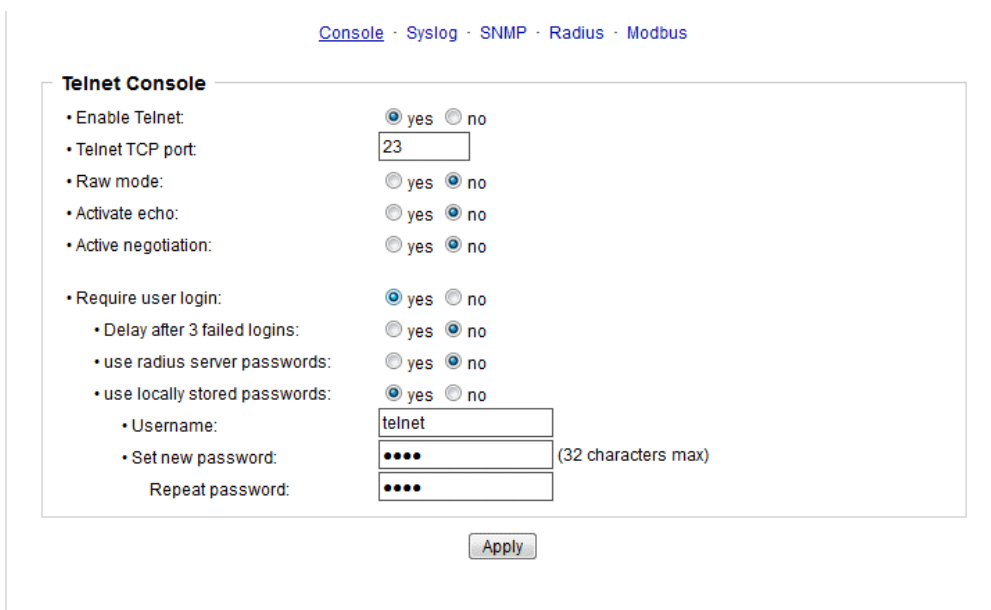
Use locally stored passwords: Username und Passwort werden lokal gespeichert. In diesem Fall müssen ein Admin-Passwort und ein User-Passwort vergeben werden. Das Passwort darf maximal 31 Zeichen besitzen. In der Passwordeingabemaske des Browsers sind für den Usernamen "admin" und "user" vorgesehen. Im Werkszustand 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 Software GBL_Conf.exe.

3.4 Protocols

3.4.1 Console



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.

Serial console

- Enable serial console: yes no
- Raw mode: yes no
- Activate echo: yes no
- Enable binary KVM protocol: yes no
- Enable UTF-8 support: 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 serial console: Aktiviert die serielle Konsole.

Raw mode: Die VT100 Editierfunktionen sind deaktiviert.

Activate echo: Die Echo-Einstellung.

Enable binary KVM protocol: Schaltet das KVM Protokoll zusätzlich ein.

Enable UTF8 support: Aktiviert die Zeichenkodierung in UTF8.

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.

3.4.2 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.

3.4.3 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.

SNMP v2 public Community: Das Passwort für die SNMP-get Arbeitsgruppe.


SNMP v2 private Community: 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: 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.

Weitere Informationen zu den SNMP-Einstellungen erhalten Sie durch unseren Support oder finden Sie im Internet unter www.gude.info/wiki.

3.4.4 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.

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.

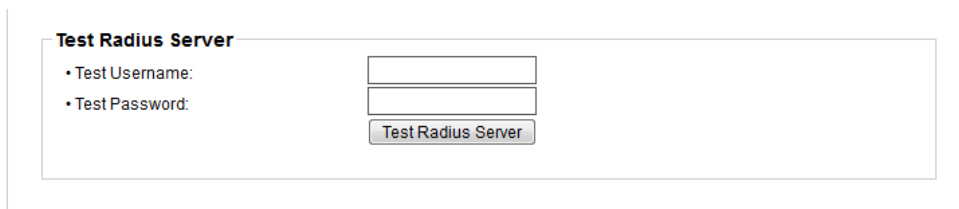
Use Backup Server: Aktiviert einen Radius Backup Server.

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

Shared secret: Radius Shared Secret.

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.

3.4.5 Modbus TCP



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

Modbus TCP

- Enable Modbus TCP: yes no
- Modbus TCP port:

Enable Modbus TCP: Aktiviert Modbus TCP Unterstützung.

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

3.5 Sensors

Control Panel Configuration Maintenance Logout

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

Sensors Config

- Sensor: 1: 7102 - 7102
- Sensor Name: 7102
- 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
- When above Max value: Switch port 1: Output Port to Off
- When below Max value: Switch port 1: Output Port to On
- When above Min value: Switch port 2: Output Port to On
- When below Min value: Switch port 2: Output Port to Off

Misc sensor options

- Min/Max measurement period: 24 Hours

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, bei denen Meldungen per SNMP-Trap, Syslog oder E-Mail versendet werden sollen.

Hysteresis: Legt den Abstand fest, der nach einem Überschreiten eines Grenzwertes eines externen Sensors überschritten 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.

Hysterese Beispiel

Konfiguration

Ein Hysteresewert verhindert, dass zu viele 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:

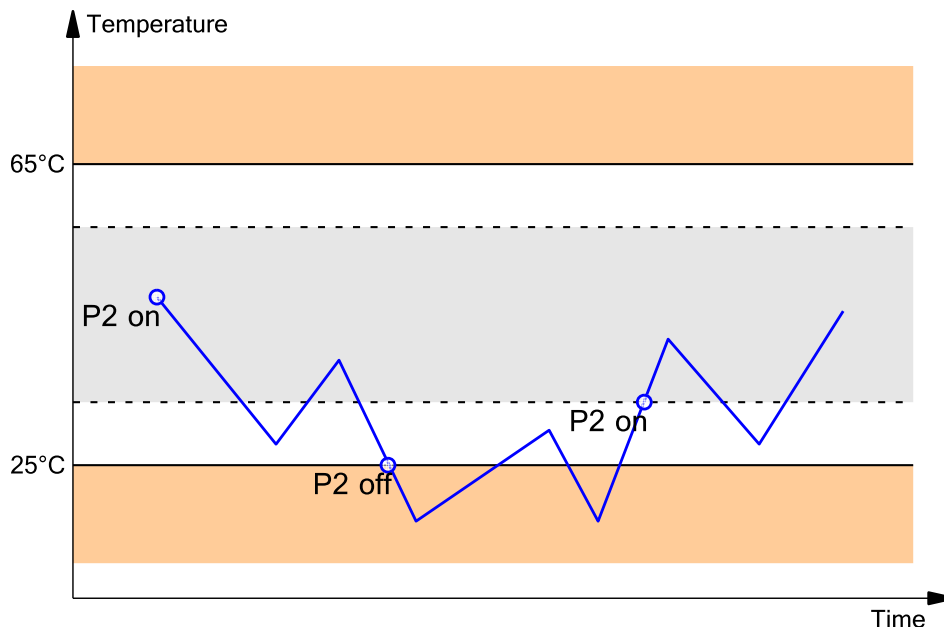
49,9 °C - unterhalb der Obergrenze
50,0 °C - eine Nachricht für das Erreichen der oberen Grenze wird erzeugt
50,1 °C - ist oberhalb der Obergrenze
...

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

3.5.1 Port Switching

In Abhängigkeit der gemessenen Stromstärke und gemessener Sensorwerte können Schaltaktionen ausgelöst werden. Im laufenden Betrieb werden die Aktionen ausgeführt, die für die Durchschreitung der Grenzwerte konfiguriert wurden. Wandert z.B. ein Wert aus dem Bereich "above max value" in den Bereich "below max value", so wird die Funktion durchgeführt, die bei "below max value" gesetzt ist. Bei Gerätestart, der Konfiguration oder Einstecken des Sensors werden die Aktionen geschaltet, die dem Bereich entsprechen, in dem sich die aktuelle Temperatur befindet.

Beispiel mit "Maximum value" von 65 °C, "Minimum value" von 25 °C und Hysterese von 3 °C. Die gestrichelte Linie zeigt die Hysterese.




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

Aktionen bei der Konfiguration, Gerätestart oder Einstecken des Sensors (für Beispiel):

aktuelle Temperatur bei Konfigurationseingabe	Aktionen
70 °C	Port 1 Off (above max) + Port 2 On (above min)
45 °C	Port 1 On (below max) + Port 2 On (above min)
20 °C	Port 1 On (below max) + Port 2 Off (below min)

Aktionenmatrix im laufenden Betrieb bei Überschreiten von Grenzwerten (für Beispiel):

	zu "above max"	zu "below max"	zu "above min"	zu "below min"
von "above max"	-	P1 On	P1 On	P1 On + P2 Off
von "below max"	P1 Off	-	-	P2 Off
von "above min"	P1 Off	-	-	P2 Off
von "below min"	P1 Off + P2 On	P2 On	P2 On	-

 Es werden nur die Schaltvorgänge ausgelöst, für die Aktionen definiert wurden. Ist für einen Port kein "On" oder "Off" definiert, so kann der Port diesen Zustand niemals durch Überschreiten von Sensorwerten erreichen. Es sei denn, es ist der Anfangszustand.

3.6 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. 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 Authentication (password): Authentifizierungsmethode des E-Mailservers.

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

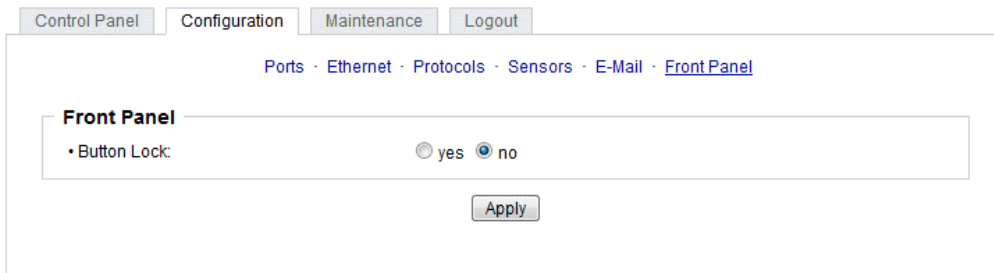
Set new password: Tragen Sie hier das Passwort für die Anmeldung beim E-Mailserver ein.

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.

3.7 Front Panel



The screenshot shows the 'Front Panel' configuration page. At the top, there are navigation tabs: 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. Below these, a breadcrumb trail reads 'Ports · Ethernet · Protocols · Sensors · E-Mail · Front Panel'. The main content area is titled 'Front Panel' and contains a single configuration item: 'Button Lock:'. This item has two radio buttons: 'yes' (unselected) and 'no' (selected). Below the radio buttons is an 'Apply' button.

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

Spezifikationen


4 Spezifikationen

4.1 IP ACL

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 Werkszustand 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 sie 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 Attribute 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
Konsole 49	Lesen/Schreiben aller Konfigurationsdaten Lesen/Schreiben aller Statusinformationen

SNMP 43	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 53	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. Der Aufbau der CGI Kommandos und der JSON Daten ist in unserem Wiki-Artikel näher erklärt:
http://wiki.gude.info/EPC_HTTP_Interface

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 Konfiguration einstellen.

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 und v2c

SNMP v1 und v2c authentifiziert die Netzerkfragen 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.


Authentifizierung

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-snmv3-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 Zweifels-

fall 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.

Änderung 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
```

bzw.

```
/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 Geräte MIB 2302

Es folgt eine Tabelle aller gerätespezifischen OID's die über SNMP angesprochen werden können. Bei der numerischen OID Darstellung wurde der Präfix "1.3.6.1.4.1.28507" zur Gude Enterprise OID aus Platzgründen bei jedem Eintrag in der Tabelle weggelassen. Die komplette OID würde daher z.B. "1.3.6.1.4.1.28507.70.1.1.1.1" 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.
enc2302TrapCtrl	0 = off 1 = Ver. 1 2 = Ver. 2 3 = Ver. 3	.70.1.1.1.1.0	Integer32	RW
enc2302TrapIPIndex	A unique value, greater than zero, for each receiver slot.	.70.1.1.1.2.1.1.x	Integer32	RO
enc2302TrapAddr	DNS name or IP address specifying one Trap receiver slot. A port can optionally be specified: 'name:port' An empty string disables this slot.	.70.1.1.1.2.1.2.x	OCTETS	RW
enc2302portNumber	The number of Relay Ports	.70.1.3.1.1.0	Integer32	RO
enc2302PortIndex	A unique value, greater than zero, for each Relay Port.	.70.1.3.1.2.1.1.x	Integer32	RO
enc2302PortName	A textual string containing name of a Relay Port.	.70.1.3.1.2.1.2.x	OCTETS	RW
enc2302PortState	current state a Relay Port	.70.1.3.1.2.1.3.x	INTEGER	RW
enc2302PortSwitchCount	The total number of switch actions occurred on a Relay Port. Does not count switch commands which will not switch the relay state, so just real relay switches are displayed here.	.70.1.3.1.2.1.4.x	Integer32	RO
enc2302PortStartupMode	set Mode of startup sequence (off, on , remember last state)	.70.1.3.1.2.1.5.x	INTEGER	RW
enc2302PortStartupDelay	Delay in sec for startup action	.70.1.3.1.2.1.6.x	Integer32	RW
enc2302PortRepowerTime	Delay in sec for repower port after switching off	.70.1.3.1.2.1.7.x	Integer32	RW
enc2302ActiveInputs	Number of supported Input Channels.	.70.1.5.6.1.0	Unsigned32	RO
enc2302InputIndex	None	.70.1.5.6.2.1.1.x	Integer32	RO
enc2302Input	Input state of device	.70.1.5.6.2.1.2.x	INTEGER	RO
enc2302SensorIndex	None	.70.1.6.1.1.1.x	Integer32	RO
enc2302TempSensor	actual temperature	.70.1.6.1.1.2.x	Integer32	RO
enc2302HygroSensor	actual humidity	.70.1.6.1.1.3.x	Integer32	RO
enc2302InputSensor	logical state of input sensor	.70.1.6.1.1.4.x	INTEGER	RO
enc2302AirPressure	actual air pressure	.70.1.6.1.1.5.x	Integer32	RO
enc2302DewPoint	dew point for actual temperature and humidity	.70.1.6.1.1.6.x	Integer32	RO
enc2302DewPointDiff	difference between dew point and actual temperature (Temp - DewPoint)	.70.1.6.1.1.7.x	Integer32	RO

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. Wenn in der erzeugten Schlüsseldatei nicht "-----BEGIN RSA PRIVATE KEY-----" sondern nur "-----BEGIN PRIVATE KEY-----" steht, wird der Schlüssel nicht erkannt.

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 ²² bleibt ein hochgeladenes Zertifikat erhalten.

Performance Betrachtungen

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 Konsoleigenschaften werden über das Webinterface ³⁷ konfiguriert.

Befehlssatz

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

back	Eine Befehlsebene zurückgehen
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
```

bzw.

```
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

Bitfeld-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_BEEPER=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).

Editierfunktionen

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
link, rechts	bewegt Cursor nach links oder rechts
Pos1, Ende	setzt den Cursor auf Anfang oder Ende der Zeile
Entf	löscht Zeichen unter dem Cursor
Rück	löscht Zeichen links vom Cursor
rauf, runter	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)*.

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)*, *Voltage (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 2302

Command	Description	Note
logout	go to login prompt when enabled	2
quit	quits telnet session - nothing in serial console	2
back	back one cmd level	2
help	show all cmds from this level	2
help all	show all cmds	2
console	enters cmd group "console"	
console version	shows unique console version number	
console telnet enabled set {OFF=0 ON=1}	enables telnet on/off	
console telnet enabled show	shows if telnet enabled	
console telnet port set {ip_port}	sets telnet port	
console telnet port show	shows telnet port	
console telnet raw set {OFF=0 ON=1}	sets raw mode (disables editing) on/off	
console telnet raw show	shows if raw mode enabled	
console telnet echo set {OFF=0 ON=1}	enables echo on/off	
console telnet echo show	shows if echo enabled	
console telnet activeneg set {OFF=0 ON=1}	enables telnet active negotiation (IAC) on/off	
console telnet activeneg show	shows if active negotiation enabled	
console telnet login set {OFF=0 ON=1}	enables login on/off	
console telnet login show	shows if login enabled	
console telnet login local set {OFF=0 ON=1}	enables local login on/off	

console telnet login local show	shows if local login enabled	
console telnet login radius set {OFF=0 ON=1}	enables login for RADIUS on/off	
console telnet login radius show	shows if RADIUS login enabled	
console telnet login delay set {OFF=0 ON=1}	enables delay (after 3 login fails) on/off	
console telnet login delay show	shows if login delay enabled	
console telnet user set "{username}"	sets login user name	
console telnet user show	shows login user name	
console telnet passwd set "{passwd}"	sets login password	
console telnet passwd hash set "{passwd}"	sets login hashed password	
console serial enabled set {OFF=0 ON=1}	enables serial console on/off	
console serial enabled show	shows if serial console enabled	
console serial raw set {OFF=0 ON=1}	sets raw mode (disables editing) on/off	
console serial raw show	shows if raw mode enabled	
console serial echo set {OFF=0 ON=1}	enables echo on/off	
console serial echo show	shows if echo enabled	
console serial kvm set {OFF=0 ON=1}	enables binary KVM cmds on serial port on/off	
console serial kvm show	shows if binary KVM cmds enabled	
console serial utf8 set {OFF=0 ON=1}	enables UTF8 support	
console serial utf8 show	shows if UTF8 enabled	
console serial login set {OFF=0 ON=1}	enables login on/off	
console serial login show	shows if login enabled	
console serial login local set {OFF=0 ON=1}	enables local login on/off	
console serial login local show	shows if local login enabled	
console serial login radius set {OFF=0 ON=1}	enables login for RADIUS on/off	
console serial login radius show	shows if RADIUS login enabled	
console serial login delay set {OFF=0 ON=1}	enables delay (after 3 login fails) on/off	
console serial login delay show	shows if login delay enabled	
console serial user set "{username}"	sets login user name	
console serial user show	shows login user name	
console serial passwd set "{passwd}"	sets login password	
console serial passwd hash set "{passwd}"	sets login hashed password	
email	enters cmd group "email"	
email enabled set {OFF=0 ON=1}	enables email on/off	
email enabled show	shows if email is enabled	
email sender set "{email_addr}"	sets email sender address	
email sender show	shows email sender address	
email recipient set "{email_addr}"	sets email recipient address	
email recipient show	shows email recipient address	
email server set "{dns_name}"	sets email SMTP server address	
email server show	shows email SMTP server address	
email port set {ip_port}	sets email SMTP port	
email port show	shows email SMTP port	
email security set {NONE=0 STARTTLS=1 SSL=2}	sets SMTP connection security	
email security show	shows SMTP connection security	
email auth set {NONE=0 PLAIN=1 LOGIN=2}	sets email authentication	
email auth show	show email authentication	
email user set "{username}"	sets SMTP username	
email user show	shows SMTP username	
email passwd set "{passwd}"	sets SMTP password	
email passwd hash set "{passwd}"	sets crypted SMTP password	
email testmail	send test email	
ethernet	enters cmd group "ethernet"	
ethernet mac show	shows MAC address	
ethernet link show	shows ethernet link state	
ethernet phyprefer set {10MBIT_HD=0 10MBIT_FD=1 100MBIT_HD=2 100MBIT_FD=3}	sets preferred speed for PHY Auto Negotiation	
ethernet phyprefer show	shows preferred speed for PHY Auto Negotiation	
extsensor	enters cmd group "extsensor"	
extsensor {port_num} {sen_field} value show	shows sensor value	6
extsensor {port_num} {sen_type} label set "{name}"	sets sensor name to label	6
extsensor {port_num} {sen_type} label show	shows label of sensor	6
extsensor {port_num} type show	shows type of sensor	
extsensor {port_num} {sen_type} {sen_field} events set {off=0 on=1}	enables sensor events on/off	6
extsensor {port_num} {sen_type} {sen_field} events show	shows if sensor events are enabled	6
extsensor {port_num} {sen_type} {sen_field} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	enables different event types	6
extsensor {port_num} {sen_type} {sen_field}	shows what event types are enabled	6

events type show		
extsensor {port_num} {sen_type} {sen_field} maxval set {num}	sets maximum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} maxval show	shows maximum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} minval set {num}	sets minimum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} minval show	shows minimum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} hyst set {num}	sets hysteresis value for sensor	6
extsensor {port_num} {sen_type} {sen_field} hyst show	shows hysteresis value for sensor	6
extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port set {port_num}	sets Port for Power Port Switching actions	6
extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port show	shows Port for Power Port Switching actions	6
extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} state set {OFF=0 ON=1 DISABLED=2}	sets Port state for Power Port Switching actions	6
extsensor {port_num} {sen_type} {sen_field} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} state show	shows Port state for Power Port Switching actions	6
extsensor period set {24H=0 12H=1 2H=2 1H=3 30MIN=4}	sets sensor Min/Max measurement period	
extsensor period show	shows sensor Min/Max measurement period	
http	enters cmd group "http"	
http server set {HTTP_BOTH=0 HTTPS_ONLY=1 HTTP_ONLY=2}	sets connection types the webserver accepts	
http server show	shows webserver accepting connection types	
http port set {ip_port}	sets http port	
http port show	shows http port	
http portssl set {ip_port}	sets https port	
http portssl show	shows https port	
http ajax enabled set {OFF=0 ON=1}	enables ajax autorefresh on/off	
http ajax enabled show	shows if ajax autorefresh enabled	
http passwd enabled set {OFF=0 ON=1}	enables http password on/off	
http passwd enabled show	shows if http password enabled	
http passwd user set "{passwd}"	sets http user password	
http passwd admin set "{passwd}"	sets http admin password	
http passwd hash user set "{passwd}"	sets hashed http user password	
http passwd hash admin set "{passwd}"	sets hashed http admin password	
input	enters cmd group "input"	
input {port_num} state show	shows input state	
input all state {MODE0=0 MODE1=1 MODE2=2} show	shows input state of all ports in 3 different view modes	4
input {port_num} name set "{name}"	sets sensor name to label	
input {port_num} name show	shows label of sensor	
input {port_num} invert enabled set {off=0 on=1}	inverts input on/off	
input {port_num} invert enabled show	shows if input inverted	
input {port_num} label {LOW=0 HIGH=1} set "{name}"	sets input low/high text	
input {port_num} label {LOW=0 HIGH=1} show	shows inputs low/high text	
input {port_num} events set {off=0 on=1}	enables input events on/off	
input {port_num} events show	shows if input events are enabled	
input {port_num} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	enables different event types	
input {port_num} events type show	shows what event types are enabled	
input {port_num} {LOW=0 HIGH=1} port set {port_num}	sets Port for Power Port Switching actions	
input {port_num} {LOW=0 HIGH=1} port show	shows Port for Power Port Switching actions	
input {port_num} {LOW=0 HIGH=1} state set {OFF=0 ON=1 DISABLED=2}	sets Port state for Power Port Switching actions	
input {port_num} {LOW=0 HIGH=1} state show	shows Port state for Power Port Switching actions	
input volt3 state show	shows state of 3V input voltage {ON=1 VERR=3}	
input volt12 state set {OFF=0 VLO=1 VHI=2}	sets state of 12V input voltage	
input volt12 state show	shows state of 12V input voltage {OFF=0 VLO=1 VHI=2 VERR=3} incl possible error condition	
ip4	enters cmd group "ip4"	

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

Spezifikationen

port {port_num} watchdog type show	shows port watchdog type
port {port_num} watchdog host set "{dns_name}"	sets port watchdog host target
port {port_num} watchdog host show	shows port watchdog host target
port {port_num} watchdog port set {ip_port}	sets port watchdog TCP port
port {port_num} watchdog port show	shows port watchdog TCP port
port {port_num} watchdog pinginterval set {num}	sets port watchdog ping interval
port {port_num} watchdog pinginterval show	shows port watchdog ping interval
port {port_num} watchdog pingretries set {num}	sets port watchdog ping retries
port {port_num} watchdog pingretries show	shows port watchdog ping retries
port {port_num} watchdog retrybooting set {OFF=0 ON=1}	sets port watchdog retry booting to on/off
port {port_num} watchdog retrybooting show	shows port watchdog retry booting state
port {port_num} watchdog bootretries set {num}	sets port watchdog retry boot timeout
port {port_num} watchdog bootretries show	shows port watchdog retry boot timeout
radius	enters cmd group "radius"
radius {PRIMARY=0 SECONDARY=1} enabled set <off=0/on=1>	enables radius client
radius {PRIMARY=0 SECONDARY=1} enabled show	show if radius client enabled
radius {PRIMARY=0 SECONDARY=1} server set "<dns_name>"	sets radius server address
radius {PRIMARY=0 SECONDARY=1} server show	shows radius server address
radius {PRIMARY=0 SECONDARY=1} password set "{passwd}"	sets radius server shared secret
radius {PRIMARY=0 SECONDARY=1} password hash set "{passwd}"	sets radius server crypted shared secret
radius {PRIMARY=0 SECONDARY=1} auth timeout set {num_secs}	sets server request timeout
radius {PRIMARY=0 SECONDARY=1} auth timeout show	shows server request timeout
radius {PRIMARY=0 SECONDARY=1} retries set {num}	sets server number of retries
radius {PRIMARY=0 SECONDARY=1} retries show	shows server number of retries
radius chap enabled set <off=0/on=1>	enables CHAP
radius chap enabled show	shows if CHAP is enabled
radius message auth set <off=0/on=1>	enables request message authentication
radius message auth show	shows if request message authentication is enabled
radius default timeout set {num_secs}	sets default session timeout (when not returned as Session-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	show if SNMP GET cmds are enabled
snmp snmpset enabled set {OFF=0 ON=1}	enables SNMP SET cmds on/off
snmp snmpset enabled show	show if SNMP SET cmds are enabled
snmp snmpv2 enabled set {OFF=0 ON=1}	enables SNMP v2 on/off
snmp snmpv2 enabled show	show if SNMP v2 is enabled
snmp snmpv2 public set "{text}"	enables SNMP v3 on/off
snmp snmpv2 public show	show if SNMP v3 is enabled
snmp snmpv2 private set "{text}"	sets SNMP v2 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	show SNMP v3 authentication algorithm
snmp snmpv3 privalg set {NONE=0 DES=1 3DES=2 AES128=3 AES192=4 AES256=5 AES192*=6 AES256*=7}	sets SNMP v3 privacy algorithm
snmp snmpv3 privalg show	show SNMP v3 privacy algorithm
snmp snmpv3 authpasswd set "{passwd}"	sets SNMP v3 authentication password
snmp snmpv3 privpasswd set "{passwd}"	sets SNMP v3 privacy password
snmp snmpv3 authpasswd hash set "{passwd}"	sets SNMP v3 authentication hashed password
snmp snmpv3 privpasswd hash set "{passwd}"	sets SNMP v3 privacy hashed password
snmp trap type set {NONE=0 V1=1 V2=2 V3=3}	sets type of SNMP traps
snmp trap type show	show SNMP trap type
snmp trap receiver {trap_num} set "{dns_name}"	sets address and port of SNMP trap receiver {trap_num}

snmp trap receiver {trap_num} show	show address and port of SNMP trap receiver {trap_num}
syslog	enters cmd group "syslog"
syslog enabled set {OFF=0 ON=1}	enables syslog msgs on/off
syslog enabled show	show if syslog enabled
syslog server set "{dns_name}"	sets address of syslog server
syslog server show	shows address of syslog server
system	enters cmd group "system"
system restart	restarts device
system fabsettings	restore fab settings and restart device
system bootloader	enters bootloader mode
system flushdns	flush DNS cache
system uptime	number of seconds the device is running
system panel enabled set {OFF=0 ON=1}	blocks panel buttons when not enabled
system panel enabled show	shows if panel buttons are enabled
vt100	enters cmd group "vt100"
vt100 echo set {OFF=0 ON=1}	sets console echo state
vt100 echo show	shows console echo state
vt100 numeric set {OFF=0 ON=1}	sets numeric mode
vt100 numeric show	shows numeric mode state
vt100 reset	resets terminal

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. N/A
6. Bitte die **Tabellen Externer Sensor Feld und Externer Sensor Typ** konsultieren, um den richtigen Index zu finden

Externer Sensor Typ Tabelle "{sen_type}"

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

Index	Beschreibung	Produkte
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	Beschreibung	Einheit
0	Temperatur	°C
1	Luftfeuchtigkeit	%
2	Digitaler Input	bool
3	Luftdruck	hPa
4	Taupunkt	°C
5	Taupunkt Temperatur Differenz	°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 Gude Geräte gehalten. Je nach Gerätetyp sind Ports oder bestimmte Sensoren nicht verfügbar.

Adressbereich:

Geräte Resource	Start	Ende	Modbus Data Type
Power/Output Ports	0x000	0x3ff	Coils
DC Eingänge	0x400	0x7ff	Discrete Inputs
Info Bereich	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 0x100f
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:

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

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, dass 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 Field	Unit
0	Temperature	0.1 °C
1	Humidity	0.1 %
2	Digital Input	bool
3	Air Pressure	1 hPa (milibar)
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):

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

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



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 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

 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 Nachrichtentypen 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
- Schalten der Ports
- Überschreiten von Max/Min Werten der Sensoren
- Änderung des Sensor Digitaleingang

SNMP-Traps

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

- Schalten der Ports
- Überschreiten von Max/Min Werten der Sensoren
- Änderung des Sensor Digitaleingang

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
- Schalten der Ports
- Überschreiten von Max/Min Werten der Sensoren
- Änderung des Sensor Digitaleingang

Support

5 Support

Auf unseren Internetseiten unter www.gude.info steht Ihnen die aktuelle Software zu unseren Produkten kostenlos zum Download zur Verfügung. Bei weiteren Fragen zu Installation oder Betrieb des Geräts wenden Sie sich bitte an unser Support-Team. Weiterhin stellen wir in unserem Support-Wiki unter www.gude.info/wiki FAQs und Konfigurations-Beispiele 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 Konsole 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 Kontakt

GUDE Systems GmbH
Von-der-Wettern-Straße 23
51149 Köln

Telefon: 0221-912 90 97
Fax: 0221-912 90 98
E-Mail: mail@gude.info
Internet: www.gude.info
shop.gude.info

Geschäftsführer: Dr.-Ing. Michael Gude

Registergericht: Köln
Registernummer: HRB-Nr. 17784
WEEE-Nummer: DE 58173350
Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz:
DE 122778228

5.3 Konformitätserklärungen

Dieses Produkt aus der **Expert Net Control 2302-Serie** ist zu den auf dieses Produkt anzuwendenden europäischen Richtlinien für die CE-Kennzeichnung konform. Die vollständige CE-Konformitätserklärung für dieses Produkt finden Sie auf der Webseite www.gude.info in der Download-Rubrik des Produktes.

5.4 FAQ

1. Was kann man 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^[16] 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^[22] 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^[45].

- A -

Antennenanschluss 8
automatisierte Zugriffe 42

- B -

Bedienung am Gerät 14
Beschreibung 6
Bootloader-Modus 21

- C -

Certificate Upload 18
Control Panel 14

- D -

Datensicherheit 64
Default Display 39

- E -

E-Mail 38

- F -

FAQ 65
Firmware Upload 18

- G -

Geräte MIB 46

- H -

HTTP 30
HTTPS 30

- I -

Inbetriebnahme 8
IP-ACL 29, 41
IP-Adresse 28
IPv6 41

- K -

Konfigurationsmanagement 20
Konformitätserklärungen 65

- L -

Lastausgänge 8
Lieferumfang 6

- M -

Maintenance 18
Modbus TCP 58

- N -

Nachrichten 62
Netzanschluss 8
Netzwerkanschluss 8

- P -

Ports 24

- R -

Radius 42
Restart 18
RS232 Anschluss 8

- S -

Sensoranschlüsse 8
Sensoren 10, 36
Sicherheitserklärung 6
Signalstärke 8
SIM-Karte 8
SNMP 33, 43
SSL 46
Status LED 8
Status-LED 14
Syslog 32

- T -

Tastensperre 39
Technische Daten 10

TLS 46

- W -

Watchdog 25

- Z -

Zertifikats Erzeugung 46



Expert Net Control 2301
© 2019 GUDE Systems GmbH
04.04.2019