Bedienungsanleitung

Automatischer Netzumschalter

ANS3100RM/ANS3000RM

KESS
power solutions

Manual_ANS31000RM_2021_DE

Content

1. Gerätebeschreibung....4
1.1 Sicherheitserklärung.... 4
1.2 Lieferumfang....4
1.3 Beschreibung.... 5
1.4 Anschluss und Inbetriebnahme.... 6
1.5 Arbeitsweise des Umschalters 7
1.6 Technische Daten....9
1.6.1 Elektrische Messgrößen....10
1.7 Sensoren.... 10

2. Bedienung....13
2.1 Bedienung am Gerät....13
2.2 Control Panel.... 13
2.3 Maintenance.... 14
2.3.1 Maintenance Seite.... 16
2.3.2 Konfigurationenmanagement....18
2.3.3 Bootloader-Aktivierung.... 19

3. Konfiguration.... 21
3.1 Konfiguration per Webinterface....21
3.2 ETS....21
3.3 Ethernet....22
3.3.1 IP-Address....22
3.3.2 IP ACL.... 24
3.3.3 HTTP....24
3.4 Protocols.... 26
3.4.1 Console.... 26
3.4.2 Syslog....27
3.4.3 SNMP....27
3.4.4 Radius.... 29
3.4.5 Modbus TCP....30
3.4.6 MQTT.... 30
3.5 Clock....32
3.5.1 NTP.... 32
3.5.2 Timer.... 33
3.5.3 Timer Konfiguration.... 33
3.6 Sensors....39
3.7 E-Mail.... 40
3.8 Front Panel 41

Content

4. Spezifikationen....42
4.1 Automatisierte Zugriffe....42
4.2 Nachrichten....43
4.3 IP ACL....45
4.4 IPv6....46
4.5 Radius....46
4.6 SNMP....47
4.6.1 Geräte MIB....51
4.7 SSL....53
4.8 Konsole....55
4.8.1 SSH....60
4.8.2 Console CMD 8801....61
4.9 Modbus TCP....76
4.10 MQTT....81
4.10.1 Beispiel HIVEMQ....84

5. Support....85
5.1 Datensicherheit....85
5.2 Kontakt....85
5.3 Konformitätserklärung....85
5.4 FAQ....86

1. GERÄTEBESCHREIBUNG

1.1 SICHERHEITSERKLÄRUNG

Das Gerät darf nur von qualifiziertem Personal installiert und verwendet werden. Der Hersteller übernimmt keine Haftung für durch die unsachgemäße Verwendung des Geräts entstandene Schäden oder Verletzungen.

Eine Reparatur des Geräts durch den Kunden ist nicht möglich. Reparaturen dürfen nur durch den Hersteller durchgeführt werden.

Dieses Betriebsmittel enthält stromführende Teile mit gefährlichen Spannungen und darf nicht geöffnet oder zerlegt werden.

Das Gerät darf nur an ein 230 Volt Wechselstromnetz (50Hz oder 60 Hz) angeschlossen 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, Styroporteile etc. könnten für Kinder zu einem gefährlichen Spielzeug werden. Bitte recyclen Sie das Verpackungsmaterial.

Sollten Sie sich über den korrekten Anschluss nicht im Klaren sein oder sollten sich Fragen ergeben, die nicht durch die Bedienungsanleitung abgeklärt werden, so setzen Sie sich bitte mit unserem Support in Verbindung.

Schließen Sie nur Elektrogeräte an, die keine eingeschränkte Einschaltdauer haben. Das heißt, alle angeschlossenen Elektrogeräte müssen im Fehlerfall eine Dauereinschaltung verkraften, ohne Schäden anzurichten.

1.2 LIEFERUMFANG

Im Lieferumfang enthalten sind:

- Automatischer Netzumschalter ANS3100RM
- 2 x Netz-Anschlusskabel (IEC C19, max. 16A)
- Schnellstart-Anleitung

1.3 BESCHREIBUNG

Der ANS3100RM/ANS300RM ist ein automatischer Transferschalter (ATS) zur redundanten Versorgung von Stromverbrauchern.

Leistungsmerkmale:

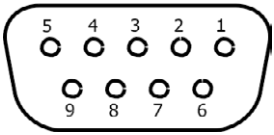
- Automatische Umschaltung auf alternative Stromversorgung B bei Ausfall der Stromversorgung A
- Berechnung des Phasenversatzes
- Umschaltung auch bei Phasenversatz
- Bei Wiederkehr der Stromversorgung A automatische Rückschaltung möglich
- Umschaltzeit bei Phasengleichheit (Fast on Sync eingeschaltet): Typ. 7 ms (Manuell) oder Typ. 15 ms (Automatisch)
- Umschaltzeit bei Phasenversatz: Typ. 10 ms (Manuell) oder Typ. 18 ms (Automatisch)
- Messung von Strom, Spannung, Phasenwinkel, Leistungsfaktor, Frequenz, Wirk-, Schein- und Blindleistung
- Messung des Fehlerstroms / Differenzstrom (entsprechend Typ A) nur beim Modell ANS3100RM
- 2 Energiezähler, ein Zähler zählt dauerhaft, der andere Zähler ist rücksetzbar
- Gut ablesbares LED-Display zur Anzeige von Gesamtstrom, IP-Adresse, und Sensorwerten
- 2 Anschlüsse für optionale Sensoren zur Umgebungsüberwachung (Temperatur und Luftfeuchtigkeit)
- Konsolen Kommandos über SSH und Telnet
- SSH Support mit Public Key und Passwörtern
- Programmierbare Zeitpläne für Konsolen Kommandos
- Dual TCP/IP Stack mit IPv4 und IPv6 Unterstützung (IPv6-ready)
- Steuerung und Überwachung des Geräts über Ethernet mit einem integrierten
- Webserver mit SSL Verschlüsselung (TLS 1.1, 1.2, 1.3)
- Konfigurierung mit CGI Parametern und JSON Nachrichten über HTTP (REST API)
- SNMP (v1, v2c und v3, Traps)
- MQTT 3.1.1 Support
- Modbus TCP Support
- Radius Support
- Erzeugung von Nachrichten (E-Mail, Syslog und SNMP Traps) in Abhängigkeit von
- Sensor Grenzwerten
- Firmware-Update im laufenden Betrieb über Ethernet möglich
- Verschlüsselte E-Mails (SSL, STARTTLS)
- Zugriffsschutz durch IP-Zugriffskontrolle
- Geringer Eigenverbrauch
- Entwickelt und produziert in Deutschland

1.4 ANSCHLUSS UND INBETRIEBNAHME

Anschluss und Bedienelemente

- 1. Status LED
- 2. Taster Select
- 3. Taster Ok
- 4. Netzwerkanschluss (RJ45)
- 5. Sensoranschlüsse (RJ45)
- 6. D-Sub 9 Anschluss (Signalisierung)
- 7. Klartextanzeigen (A / B) für den Zustand der beiden Eingänge
- 8. Klartextanzeige für Phasengleichheit („phase 0 degree“ / „reverse phase“)
- 9. Klartextanzeigen (A / B) welcher Netzanschluss auf die Lastausgänge geschaltet ist
- 10. Aktuelle Stromaufnahme der geschalteten Phase (7-Segment Anzeige)

D-Sub 9 Anschluss (Signalisierung)



- 1. Relais Öffner für Eingang A
- 2. nicht verbinden!
- 3. nicht verbinden!
- 4. Relais Mittelkontakt für Eingang A
- 5. nicht verbinden!
- 6. Relais Öffner für Eingang B
- 7. Relais Mittelkontakt für Eingang B
- 8. Relais Schließer für Eingang B
- 9. Relais Schließer für Eingang A

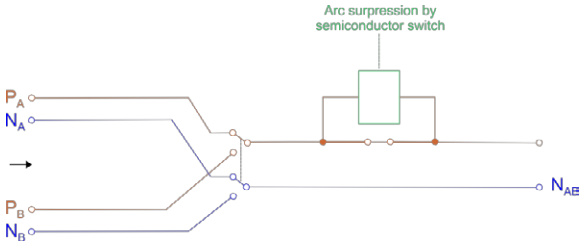
- 1. 1 x Lastausgang (IEC C19, max. 16 A)
- 2. 6 x Lastausgänge (IEC C13, max. 10 A)
- 3. Netzanschluss B (IEC C20, max. 16 A)
- 4. Netzanschluss A (IEC C20, max. 16 A)

Inbetriebnahme

Verbinden Sie Eingang A mit dem primären Stromnetz, und Eingang B mit dem sekundären Stromnetz. Die Zuleitungsstecker sind von der Bauart her gegen unbeabsichtigtes Lösen gesichert. Sie müssen bis zum Anschlag eingesteckt werden, sonst besteht keine sichere Verbindung. Der Stecker darf nicht in der Buchse wackeln, ansonsten ist der Stecker noch nicht bis zum Anschlag eingesteckt.

Stecken Sie das Netzwerkkabel in die Ethernetbuchse (RJ45).
Stellen Sie bei Bedarf eine Verbindung mit dem Signalisierungsanschluss (D-Sub 9) her.
Stecken Sie die optionalen externen Sensoren in die Sensoranschlüsse.
Verbinden Sie die zu schaltenden Verbraucher mit den Lastausgängen (IEC C20, max. 16 A) oder (IEC C13, max. 10 A).

1.5 ARBEITSWEISE DES UMSCHALTERS



Das Gerät verfügt über Sicherheitsrelais, die die Eingänge jeweils einzeln vom Netz trennen können, über ein Hauptrelais, das zwischen den Eingängen A und B umschaltet, sowie über ein Relais vor den Lastausgängen. Die Sicherheitsrelais schalten nur den Eingang auf das Gerät frei, welcher auch an der Stromversorgung angeschlossen ist. Liegt an einem der beiden Anschlüsse keine Spannung an, ist dieser Eingang komplett vom Gerät getrennt.

Im normalen Betrieb wird kontinuierlich die Spannung an den beiden Eingängen überwacht. Verlässt die Spannungskurve des Eingangs zu lange den Bereich eines vordefinierten Templates, wird ein Fehlerzustand erreicht. Über die Konfigurationsoption Sensitivity wird die Empfindlichkeit des Templates definiert. Die speziellen ANS Konfigurationsoptionen werden in dem Kapitel Konfiguration - ETS beschrieben. Das Gerät schaltet auf den anderen Eingang, wenn dort die Analyse der Eingangsspannung keinen Fehler erkennt. Um zu vermeiden, dass eine kurze Störung eines Eingangs einen unnötigen Schaltvorgang auslöst, muss die Spannung über einen Zeitraum von ca. 2 ms den erlaubten Bereich verlassen. Die Analyse der Spannung erkennt, ob Phase und Polarität der beiden Eingänge A und B identisch sind oder nicht. Diese Information wird auf der „Control Panel“ Webseite und auf dem Gerätedisplay als „phase 0 degree“ bzw. „reverse phase“ ausgegeben.

Ein Schaltvorgang von einem Eingang auf den anderen, wird entweder durch ein manuelles Kommando oder durch einen Fehlerzustand ausgelöst. Beim Schaltvorgang wird zunächst die Last am Ausgang abgetrennt, dann auf den anderen Eingang umgeschaltet und dann die Last wieder zugeschaltet. Wenn die Option Fast on Sync eingeschaltet ist und die beiden Eingänge A und B keinen Phasenversatz aufweisen, wird der Schaltvorgang schneller ohne das Ab- und Zuschalten der Last ausgeführt.

Es empfiehlt sich immer, die Eingänge möglichst ohne Phasenversatz an das Stromnetz anzuschließen, da dies zu schnelleren Umschaltzeiten führt.

Bevorzugtes Schalten

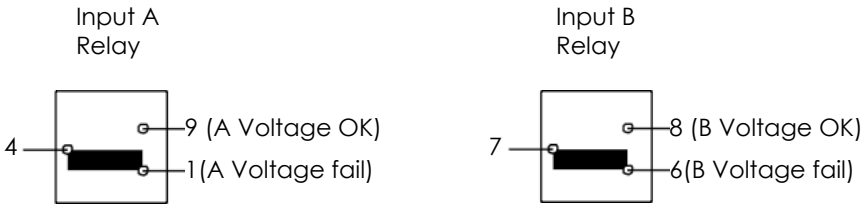
Die Option Preferred bestimmt, welcher Eingang bevorzugt wird, wenn die Spannung an beiden Eingängen keinen Fehler erkennen lässt. Nur wenn der Wert „none" eingestellt ist, kann manuell geschaltet werden, und der „toggle connected input" Button auf der Control Panel Webseite ist verfügbar.

Eingangsüberwachung

Liegt an einem der beiden Eingänge A oder B keine Spannung an, oder entspricht nicht den Vorgaben, dann wird das im Display durch ein rotes Blinken signalisiert. Zusätzlich ertönt der Summer, wenn die Option Beeper Enabled in der ETS Konfiguration aktiviert ist.

D-Sub 9 Signalisierung

Der Zustand der Spannung an den beiden Eingängen wird zusätzlich durch zwei galvanisch getrennte Relais signalisiert. Ergibt die Analyse, dass die Spannung am Eingang innerhalb der Toleranzen ist, wird das jeweilige Relais auf den Schließerkontakt (Voltage OK) geschaltet. Für die D-Sub 9 Pinbelegung siehe Kapitel „Anschluss und Inbetriebnahme".



1.6 TECHNISCHE DATEN

Anschlüsse	1 x Ethernetanschluss (RJ45) 2 x Netzanschlüsse (IEC C20, max. 16 A) 6 x Lastausgänge (IEC C13, max. 10 A) 1 x Lastausgang (IEC C19, max. 16 A) 2 x RJ45 für externen Sensor 1 x Galvanisch getrennter Ausgang (Sub-D 9-polig)
Netzwerkanbindung	10/100 MBit/s 10baseT Ethernet
Eingangsspannungs-bereich	230 V AC / -5% / +5%
Eigenverbrauch (230 V AC, 25 ° C)	A und B versorgt, A geschaltet: Typ. 60 mA (5,5 W) A und B versorgt, B geschaltet: Typ. 75 mA (7,5 W) A Spannung, A geschaltet: Typ. 40 mA (4 W) B Spannung, B geschaltet: Typ. 55 mA (6 W)
Schaltzeiten (Phasensynchron FastonSync ein)	15 ms (automatisch) 7 ms (manuell)
Schaltzeiten (Phasenversatz)	18 ms (automatisch) 10 ms (manuell)
D-Sub 9 Relais	DC 30V, 1A AC 24V, 1A
Betriebstemperatur	0 °C - 50 °C
Lagertemperatur	-20 °C - 70 °C
Luftfeuchtigkeit	0% - 95% (nicht kondensierend)
Gehäuse	Pulverbeschichtetes, verzinktes Stahlblech
Maße	19 Zoll, 1 HE, (Tiefe 195 mm)
Gewicht	Ca. 2,5 kg

1.6.1 ELEKTRISCHE MESSGRÖSSEN

Typische Fehlertoleranzen für Ta = 25°C, I = 1Arms...16Arms, Un = 90Vrms...265Vrms

Elektrische Messgrößen				
Messwert	**Bereich**	**Einheit**	**Auflösung**	**Ungenauigkeit (typisch)**
Spannung (voltage)	230	V	0,01	<1 %
Strom (current)	0 bis 16	A	0,001	<1,5 %
Frequenz (frequency)	45 bis 65	Hz	0,01	<0,03 %
Phasenwinkel (phase)	-180 bis +180	°	0,1	<1 %
Wirkleistung (active power)	0 bis 4000	W	1	<1,5 %
Blindleistung (reactive power)	0 bis 4000	Var	1	<1,5 %
Scheinleistung (apparent power)	0 bis 4000	VA	1	<1,5 %
Powerfaktor (PF)	0 bis 1	-	0,01	<3 %
Energiezähler				
Wirkenergie (total)	9.999.999,999	kWh	0,001	<1,5 %
Wirkenergie (temp)	9.999.999,999	kWh	0,001	<1,5 %

1.7 SENSOREN

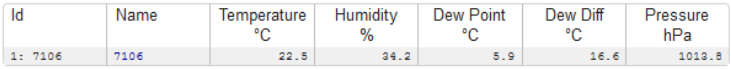
Am ANS3100RM können zwei externe Sensoren angeschlossen werden. Aktuell sind folgende Sensoren verfügbar:

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

Name	**7101**	**7104-1**	**7105-1**	**7106-1**
Kalibrierter Sensor	**-**	**7014-2**	**7104-2**	**7106-2**
Kabellänge	Ca. 2 Meter	Ca. 2 Meter	Ca. 2 Meter	Ca. 2 Meter
Anschluss	RJ45	RJ45	RJ45	RJ45
Temperatur-bereich	-20°C bis +80°C bei ±2°C (max.) und ±1°C (typisch)	-20°C bis +80°C bei ±2°C (max.) und ±1°C (typisch)	-20°C bis +80°C bei ±2°C (max.) und ±1°C (typisch)	-20°C bis +80°C bei ±2°C (max.) und ±1°C (typisch)
Luftfeuchte-bereich (nicht kondensierend)	-	-	0-100%, ±3% (max.) und ±2% (typisch)	0-100%, ±3% (max.) und ±2% (typisch)
Luftdruck-bereich (voll)	-	-	-	± 1 hPa (typisch) bei 300 ... 1100 hPa, 0 ... +40 °C
Luftdruck-bereich (erw.)	-	-	-	± 1.7 hPa(typisch) bei 300 ...1100 hPa, -20 ... 0°C
Schutz	IP68	-	-	-

Name	7201	7202
Kabellänge	-	-
Anschluss	RJ45	RJ45
Temperatur-bereich	-20°C bis +80°C bei ±2°C (max.) und ±1°C (typisch)	-20°C bis +80°C bei ±2°C (max.) und ±1°C (typisch)
Luftfeuchte-bereich (nicht kondensierend)	-	0-100%, ±3% (max.) und ±2% (typisch)

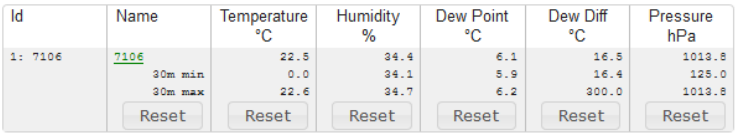
Die Sensoren werden nach dem Anschließen automatisch erkannt. Die grüne LED am Sensorport leuchtet dann dauerhaft. Auf der „Control Panel“ Webseite werden die Sensorwerte direkt angezeigt:



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

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	Pressure hPa
1: 7106	7106	22.5	34.4	6.1	16.5	1013.8
	30m min	0.0	34.1	5.9	16.4	125.0
	30m max	22.6	34.7	6.2	300.0	1013.8
	Reset	Reset	Reset	Reset	Reset	Reset

2. BEDIENUNG

2.1 BEDIENUNG AM GERÄT

Manuelles Schalten
Den aktuellen Schaltzustand erkennt man an den dazugehörigen Klartext-Anzeigen im Display. Möchte man über die Taster manuell Schalten, müssen beide Eingänge Strom haben (grüne Anzeige), und die Option Preferred muss auf „none“ stehen. Wird auf „Select“ gedrückt, blinkt in der Anzeige der Eingang, auf den geschaltet wird, sobald man die Taste „Ok“ betätigt.

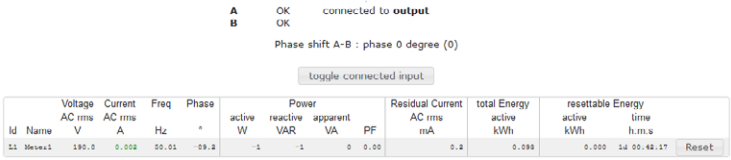
Anzeige Informationen
Wurde „Select“ nicht gedrückt, werden durch wiederholtes Drücken des „Ok“ Tasters nacheinander die IP-Adresse und die Werte der externen Sensoren im Display (7-Segment Anzeige) dargestellt.

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

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

2.2 CONTROL PANEL

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



Die Webseite bietet einen Überblick über den Schaltzustand, und zeigt die gemeinsamen Messwerte der Lastausgänge. Sowie die Sensoren, sofern sie angeschlossen sind. Der Eingang kann mit der Schaltfläche „toggle connected input“ gewechselt werden, wenn an beiden Eingängen Spannung anliegt und die Option Preferred auf „none“ steht. Sollte hinter den den Buchstaben für die Eingänge (A und B) nicht „OK“ stehen, so entspricht die Qualität der Eingangspannung nicht den definierten Erwartungen (siehe Kapitel Arbeitsweise des Umschalters) . Man kann diese Empfindlichkeit mit der Parameter Sensitivity (siehe Kapitel Konfiguration - ETS) herabsetzen.

Optional kann das Gerät auch über ein Perl-Skript oder externe Programme wie wget konfiguriert werden.

2.3 MAINTENANCE

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

Maintenance im Webinterface

Folgende Funktionen sind auf der Maintenace Website 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 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.

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

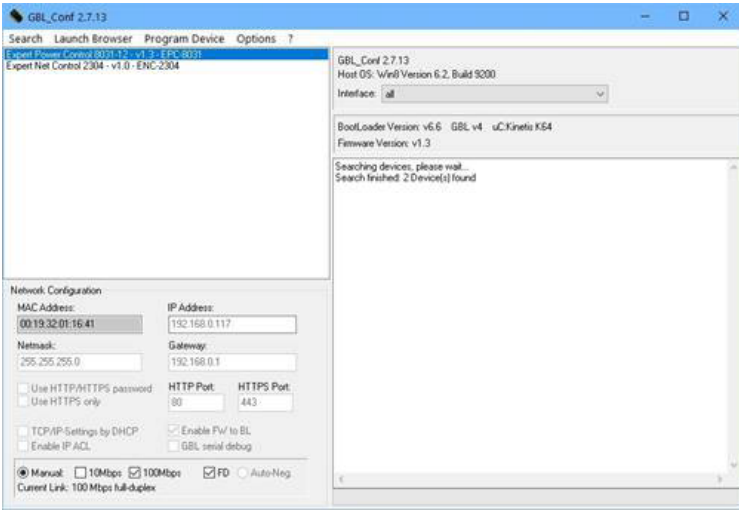
Aktionen im Bootloader-Modus

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

- Setzen von IPv4-Adresse, Netzmaske, Gateway
- Ein- und Ausschalten des HTTP-Passworts
- Ein- und Ausschalten der IP-ACL
- Wiederherstellung des 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.kess.at erhältlich.



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 IPAdresse 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 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.

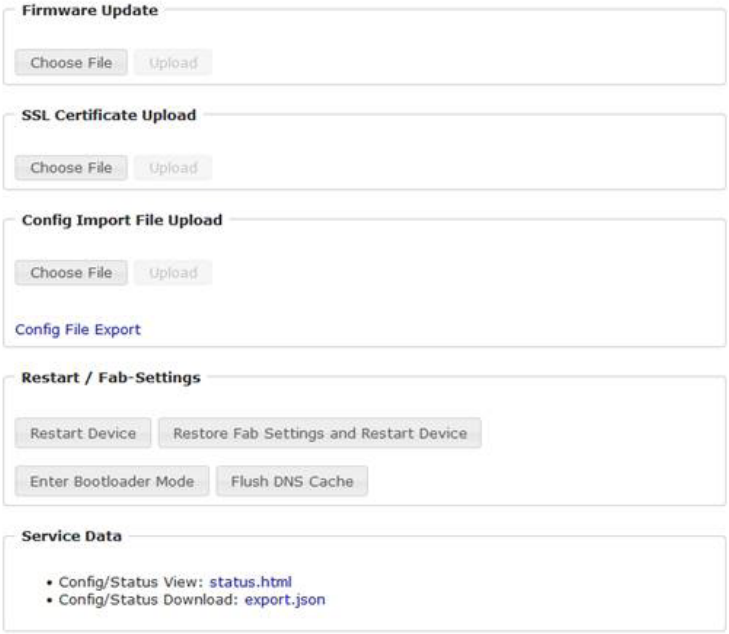
Werkszustand

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

Ein Firmware-Update oder ein hochgeladenes Zertifikat bleiben erhalten, wenn man das Gerät in den Werkszustand 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 „ für die Generierung eines Zertifikats im richtigen Format.

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

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

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

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

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

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

Enter Bootloader Mode: Springt in den Bootloader-Modus, in welchem mit „Gbl_Conf.exe“ Einstellungen vorgenommen werden können.

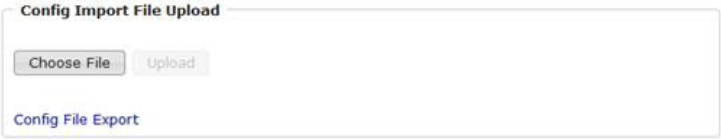
Flush DNS Cache: Alle Einträge im DNS-Cache werden verworfen und Adressauflösungen werden neu angefordert.

Config/Status View: status.html: Zeigt die status.html Seite mit den JSON Daten an.

Config/Status Download: export.json: Direkter Datei Download der JSON Daten aus status.hml.

2.3.2 KONFIGURATIONENMANAGEMENT

Die Gerätekonfiguration lässt sich im Maintenance Bereich speichern und wiederherstellen.



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

Aktivierung des Bootloader Modus

1) per Taster: Halten Sie beide Taster für 3 Sekunden gedrückt

oder

2) - 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

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 Werkszustand 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

oder

2) 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“

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

Werkszustand

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

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

1) per Taster: Halten Sie beide Taster für 3 Sekunden gedrückt
   - 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)

3. KONFIGURATION

Automatische Konfiguration per DHCP

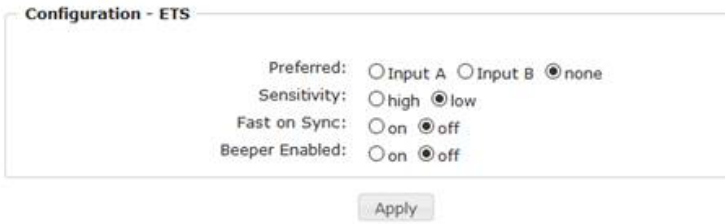
Nach dem Einschalten sucht das Gerät im Ethernet einen DHCP-Server und fordert bei diesem eine freie IP-Adresse an. Prüfen Sie in den Einstellungen des DHCP-Servers, welche IP-Adresse zugewiesen wurde und stellen Sie gegebenenfalls ein, dass dieselbe IP-Adresse bei jedem Neustart verwendet wird. Zum 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 KONFIGURATION PER WEBINTERFACE

Rufen Sie das Webinterface wie folgt auf: http://“IP-Adresse des Geräts“/ und loggen Sie sich ein. Über die Schaltfläche „Configuration“ haben Sie nach dem Login die Möglichkeit in das Konfigurationsmenü zu gelangen.

3.2 ETS



Preferred: Der bevorzugte Eingang, der auf die Lastausgänge geschaltet wird.

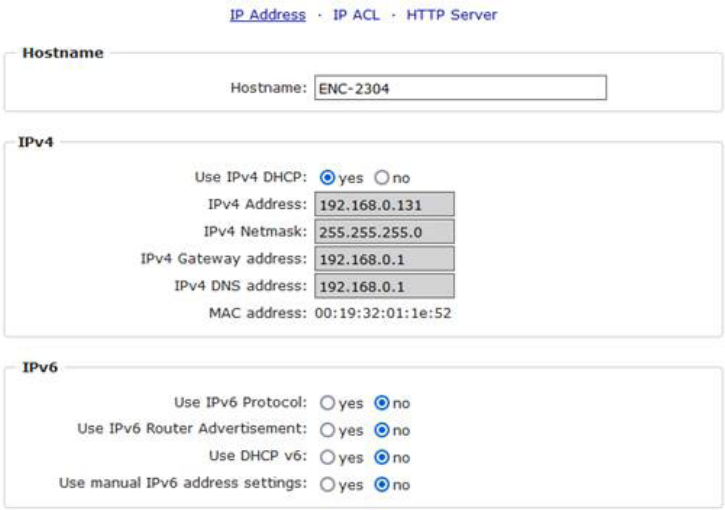
Sensitivity: Die Empfindlichkeit des Templates während der Spannungs-überwachung.

Fast on Sync: Es wird schneller geschaltet, falls beide Eingänge keinen Phasen-versatz haben.

Beeper Enabled: Der Summer ertönt, wenn einer der beiden Eingänge ohne Spannung ist.

3.3 ETHERNET

3.3.1 IP-ADDRESS



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 DHCPServer 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.

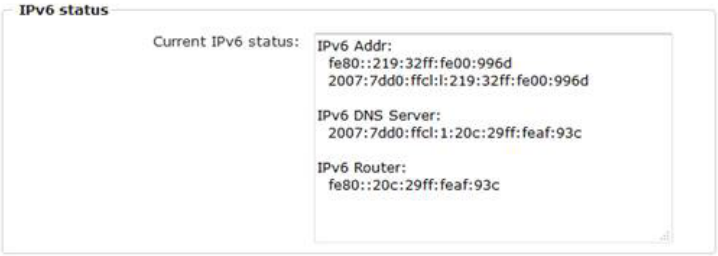
Use IPv6 Protocol: Aktiviert das IPv6-Protokoll.

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 DCHP-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.

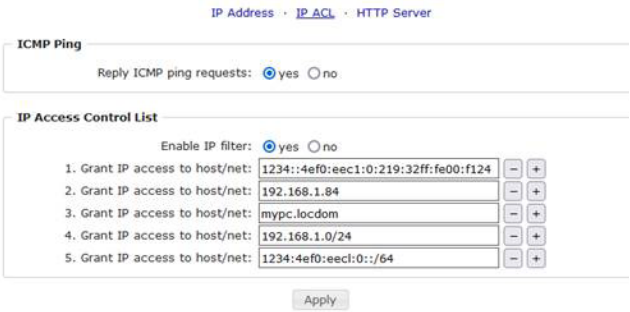


Für IP-Änderungen ist ein Neustart der Firmware notwendig. Dies kann im Maintenance Bereich vorgenommen werden. Ein Neustart des Geräts führt in keinem Fall zu einer Änderung der Relaiszustände.

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.

3.3.2 IP ACL



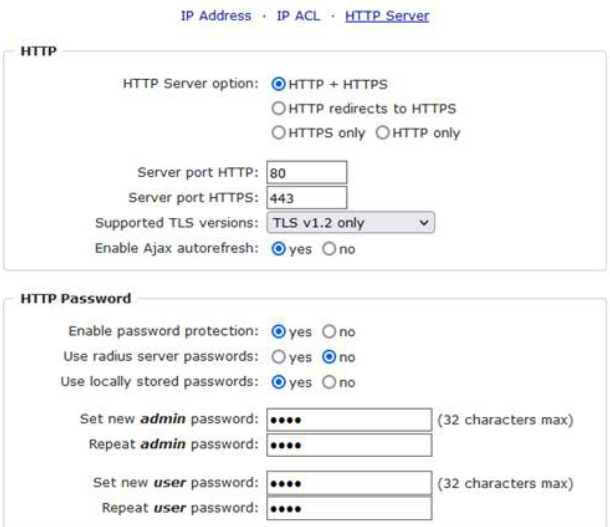
Reply ICMP ping requests: Wenn Sie diese Funktion aktivieren, antwortet das Gerät auf ICMP-Pings aus dem Netzwerk.

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 Werkszustand 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.

Supported TLS versions: Beschränkt die unterstützten TLS Versionen.

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 Sever validiert.

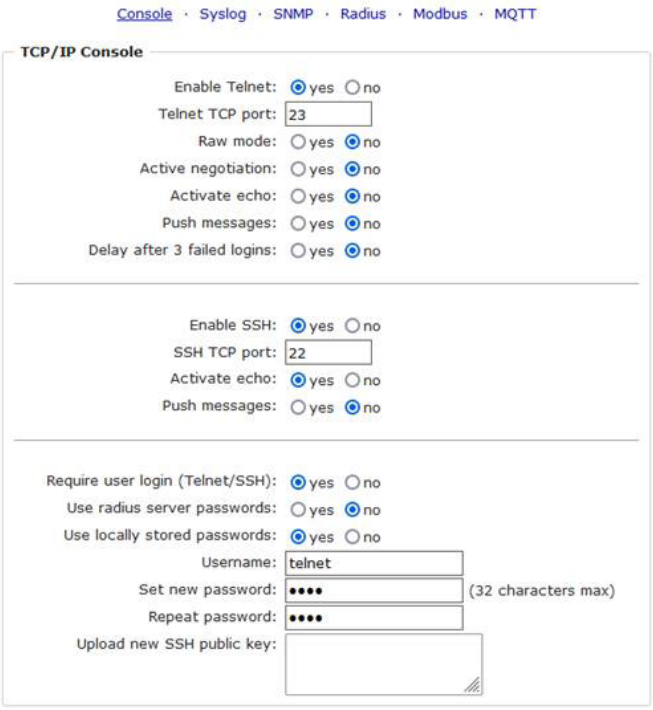
Use locally stored passwords: Username und Passwort werden lokal gespeichert. In diesem Fall müssen ein Admin-Passwort und ein User-Passwort vergeben werden. Das Passwort darf maximal 31 Zeichen besitzen. In der Passworteingabemaske des Browsers sind für den Usernamen „admin" und „user" vorgesehen. Im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

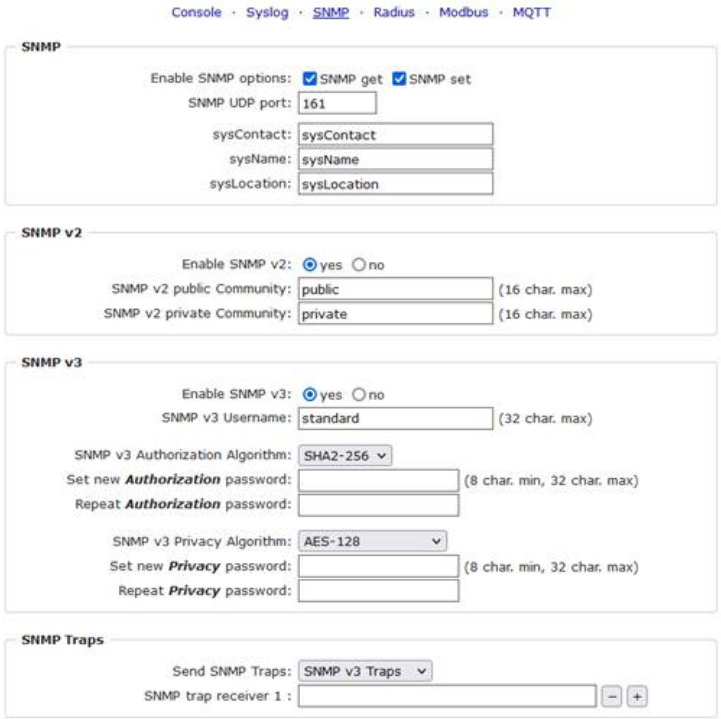
Use locally stored passwords: Username und Passwort werden lokal gespeichert.

3.4.2 SYSLOG

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



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.

sysContact: Wert von RFC 1213 sysContact.

sysName: Wert von RFC 1213 sysName.

sysLocation: Wert von RFC 1213 sysLocation.

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.

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.

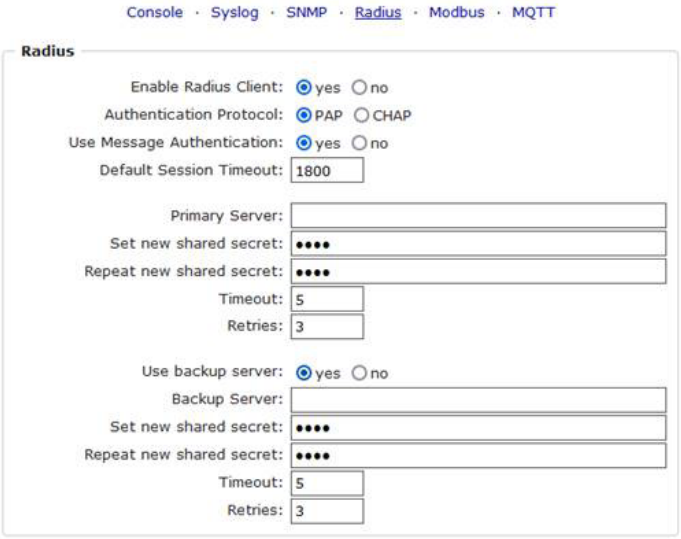
Send SNMP traps: Hier können Sie festlegen ob, und in welchem Format das Gerät SNMP-traps versenden soll.

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.kess.at

3.4.4 RADIUS



Enable Radius Client: Aktiviert die Validierung über Radius.

Use CHAP: Benutze CHAP Passwort Kodierung.

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

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

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

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

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

Use Backup Server: Aktiviert einen Radius Backup Server.

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

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

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

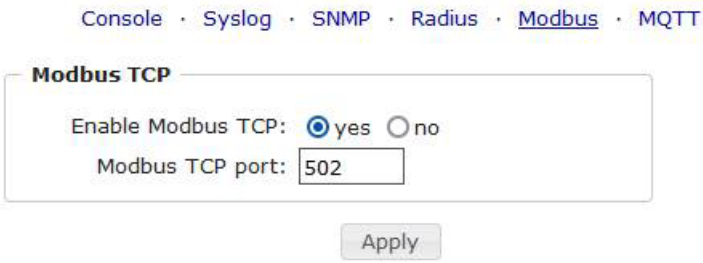
Retries: Wie oft ein Authentication Request nach einem Timeout wiederholt wird.

Test 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.

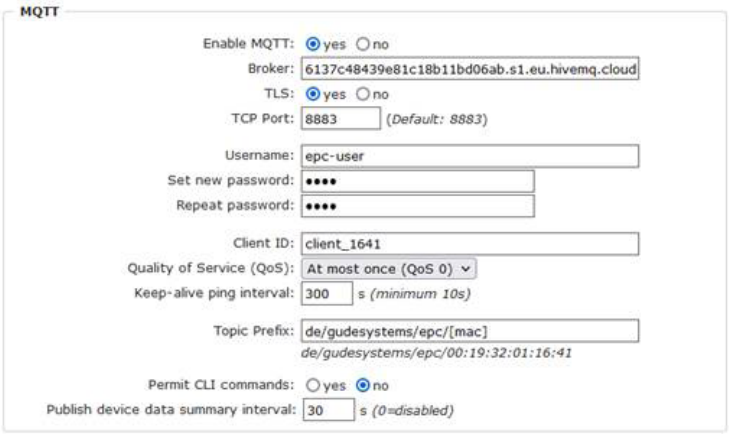
3.4.5 MODBUS TCP



Enable Modbus TCP: Aktiviert Modbus TCP Unterstützung.

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

3.4.6 MQTT



Enable MQTT: Aktiviert MQTT Unterstützung.

Broker: DNS oder IP-Adresse des MQTT Brokers.

TLS: Schaltet TLS-Vershclüsselung an.

Modus TCP port: Die TCP/IP Portnummer des Brokers.

Username: Der MQTT Benutzername.

password: Das Passwort zum Benutzernamen.

Client ID: Die MQTT Client ID.

Die Client IDs eines Benutzers müssen unterschiedlich sein! Wenn zwei Clients eines Benutzers den gleichen Namen haben, wird normalerweise die Verbindung eines Clients abgebrochen.

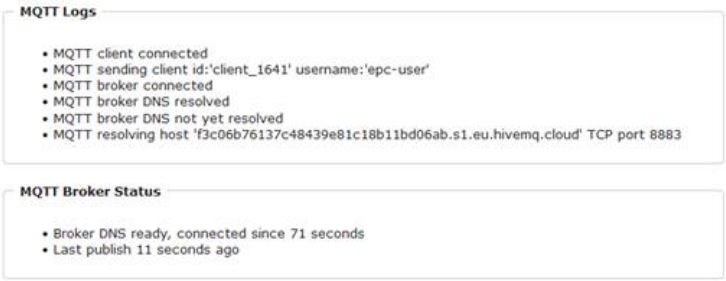
Quality of Service (QoS): Stellt den QoS Wert (0 oder 1) der MQTT publishes ein.

Keep-alive ping interval: Dies bestimmt das Zeitintervall in dem der Client einen MQTT Ping schickt.

Topic Prefix: Definiert des Anfang des Topics mit dem alle Nachrichten geschickt werden. Die Strings [mac] und [host] symbolisieren dabei die MAC-Adresse oder den Hostname des Gerätes.

Permit CLI commands: Aktiviert die Ausführung von Konsolen Kommandos.

Publish device data summary interval: Zeitintervall in dem Nachrichten mit dem globalen Zustand des Gerätes verschickt werden.

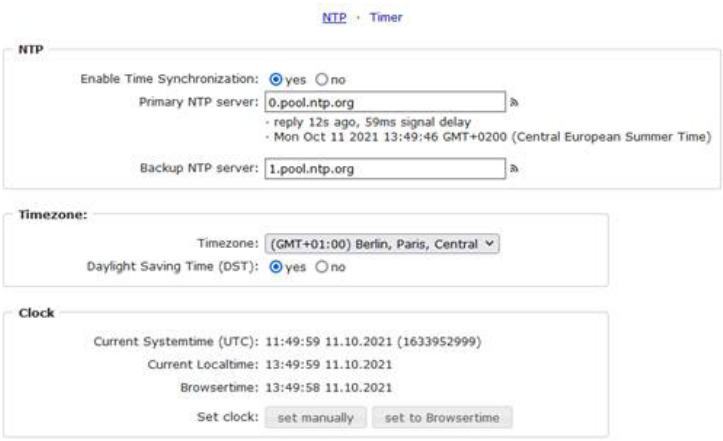


MQTT Logs: Gibt einzelne Logmeldungen zu dem Verbindungsaufbau aus.

MQTT Broker Status: Zeitinformationen über Verbindungsdauer, dem letzten publish und dem letzten keep-alive.

3.5 CLOCK

3.5.1 NTP



Enable Time Synchronisation: Schaltet das NTP Protokoll ein.

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

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

Timezone: Die eingestellte Zeitzone für die lokale Zeit.

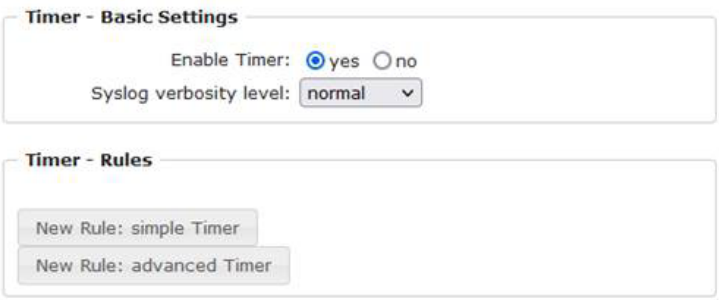
Daylight Saving Time: Falls aktiviert, wird die lokale Zeit in die Mitteleuropäische Sommerzeit umgerechnet.

set manually: Der Benutzer kann manuell eine Uhrzeit setzen.

set to Browsertime: Setzt die Uhrzeit des Webbrowsers.

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

3.5.2 TIMER



Enable Timer: Schaltet alle Timer global ein oder aus.

Syslog verbosity level: Setzt die "verbosity" Stufe für Timer Syslog Ausgaben.

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

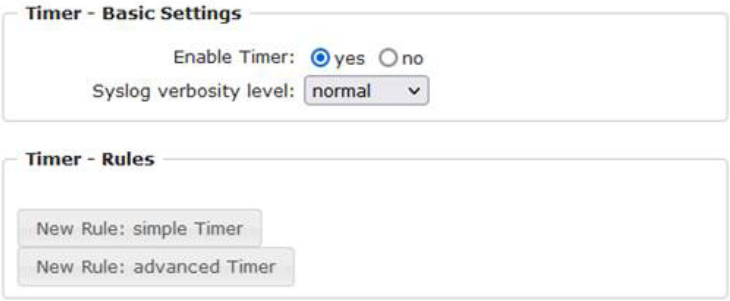
New Rule advanced Timer: Bringt den Dialog für komplexe Timer Einstellungen.

3.5.3 TIMER KONFIGURATION

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

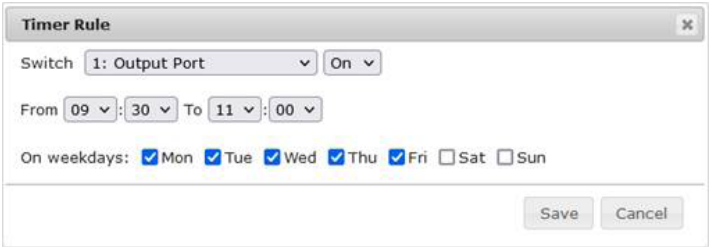
Timer Regeln werden nur dann ausgeführt, wenn das Gerät eine valide Uhrzeit hat. Siehe Konfiguration NTP.

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

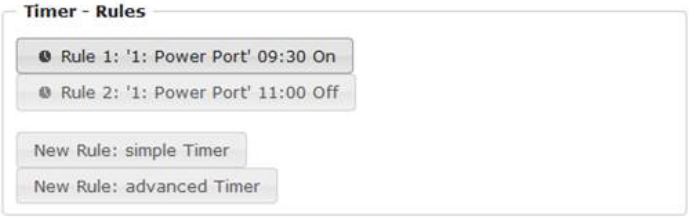


Einen einfachen Timer anlegen

Aktiviert man „New Rule: simple Timer“ wird folgender Dialog angezeigt:



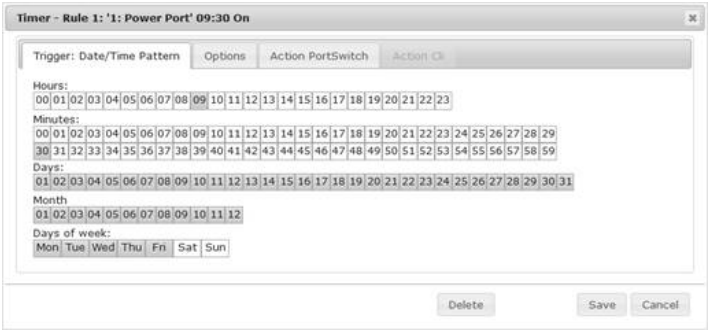
Man stellt hier ein, welcher Port für welchen Zeitraum geschaltet werden soll, und an welchen Wochentagen die Regel aktiv ist. In diesem Beispiel ist im Vergleich zur Default-Eingabemaske der Zeitraum 9:00 bis 17:00 zu 9:30 bis 11:00 geändert. Auch soll diese Regel nicht an Samstag und Sonntag angewendet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



Wir haben jetzt 2 Regeln angelegt, ein für den Einschaltzeitpunkt und die zweite zum Ausschalten des Ports.

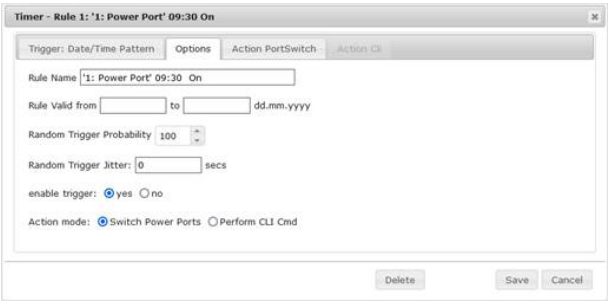
Einen komplexen Timer anlegen

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

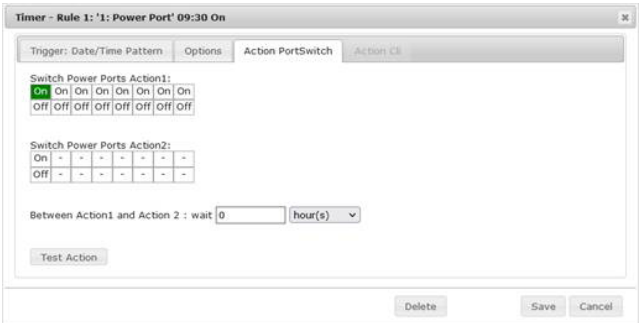


Man sieht hier die erweiterte Darstellung der ersten Regel des einfachen Timers aus dem vorherigen Beispiel. Die Aktion wird jeden Tag jedes Monats um 9:30 gestartet. Die Wochentage Samstag und Sonntag sind ausgeschlossen. Eine bestehende Regel kann mit dem „Delete“ Schalter entfernt werden.

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



Ein einfacher Timer wird direkt „enabled“, bei einem neue angelegten komplexen Timer muss „enable trigger“ manuell eingeschaltet werden. Man kann für die Timer-Regeln eine Wahrscheinlichkeit und eine Streuung einstellen. Hier wird die Regel mit 100% Wahrscheinlichkeit ausgeführt. Ein Jitter von 0 besagt, dass die Aktion exakt am programmierten Zeitpunkt stattfindet. Als Aktionsmodus werden Ports geschaltet, alternativ kann auch ein Konsolen Kommando (CLI Cmd) ausgeführt werden.

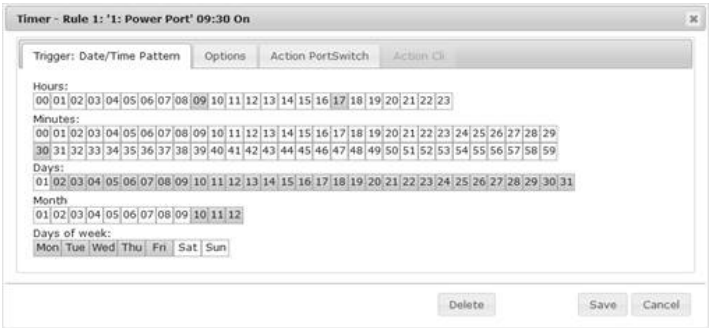


Auf dem „Action PortSwitch“ Register ist die Schaltfunktion detaillierter einstellbar. Port 1 wird eingeschaltet. Man könnte die Regel erweitern und weitere Ports ein- oder ausschalten. Zusätzlich kann man im Feld nach „Between Action1 and Action 2 : wait“ eine Zeit für einen Batchmode anlegen, der nach abgelaufener Zeit „Action 2“ auslöst. Allerdings hat der Batchmode den Nachteil, dass er bei einem Neustart des Gerätes nicht wieder automatisch gestartet wird. Auch ist der Port gegen manuelle Bedienung auf der Webseite gesperrt, solange der Batchmode läuft.

Die Funktion „Action PortSwitch“ steht nur bei Geräten mit schaltbaren Ports zur Verfügung.

Eine Regel erweitern

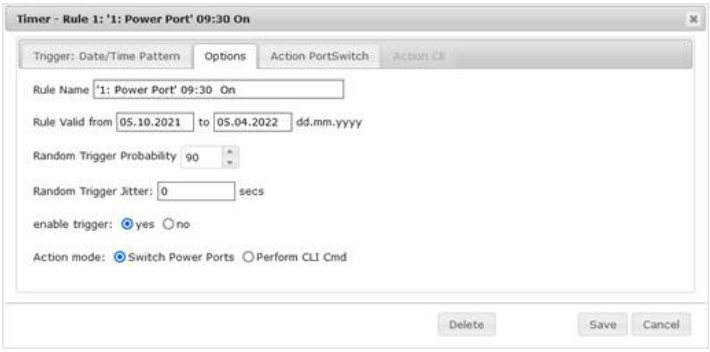
Zur Demonstration wird hier der einfache Timer aus dem vorherigen Beispiel erweitert:



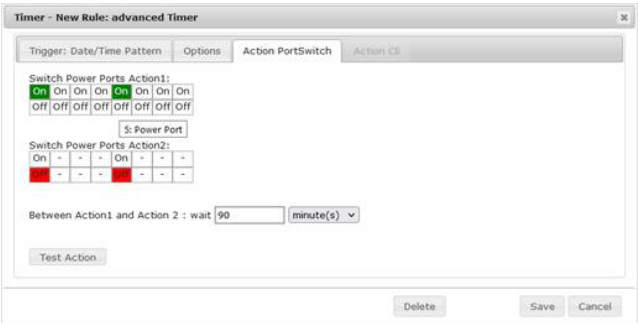
Die Aktion wird jetzt nicht nur um 9:30 gestartet, sondern zusätzlich um 17:30. Es gibt weitere Veränderungen: Der Timer ist nur zwischen Oktober und Dezember aktiv, auch findet die Aktion nicht am ersten Tag eines Monats statt.

Da immer alle Felder in der Maske berücksichtigt werden, ist es in einer einzigen Timer-Regel nicht möglich, die Zeitpunkte 9:30 und 17:10 zu definieren. Man benötigt dafür eine zweite Regel. Setzt man die Stunden 9 und 17, sowie die Minuten 10 und 30, dann wären die vier Zeitpunkte 9:10, 9:30, 17:10 und 17:30 programmiert.

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



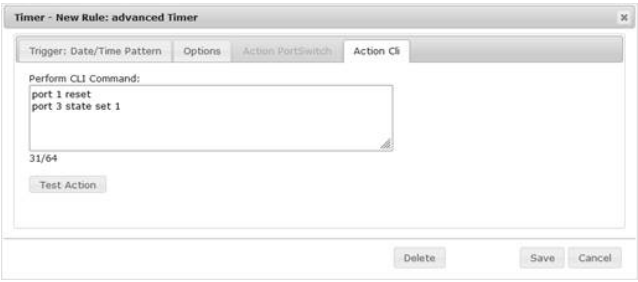
Bei dieser Regel ist auf dem "Options" Register der Zeitraum auf den Bereich zwischen dem 5.10.2021 und dem 5.4.2022 eingeschränkt. Die Timer-Regel wird in diesem Beispiel nur mit einer Wahrscheinlichkeit (Random Trigger Probability) von 90% ausgeführt.



In diesem Beispiel werden Port 1 und Port 5 aktiviert und nach 90 Minuten durch Batchmode wieder deaktiviert.

Ein Popup beim Mauszeiger zeigt die Portnummer des Feldes.

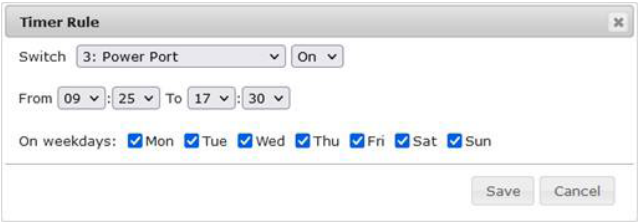
Konsolen Kommandos



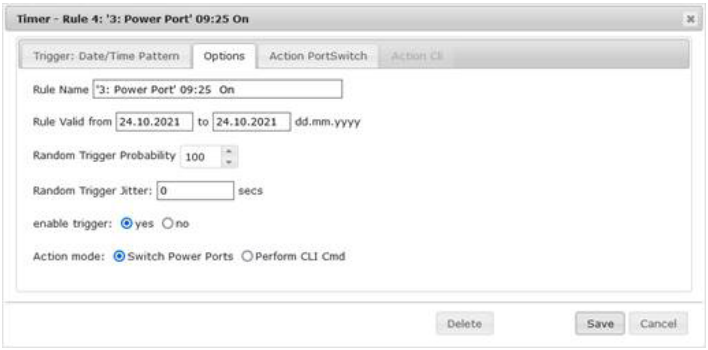
Anstatt einen Port zu schalten, kann man einen oder mehrere Konsolen Kommandos ausführen lassen. Diese Befehle werden im "Action CLI" Register eingetragen. Der "Action Cli" Register ist nur dann anwählbar, wenn bei "Options" die Option "Perform CLI Cmd" aktiviert ist.

Beispiel Port an einem Datum schalten

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

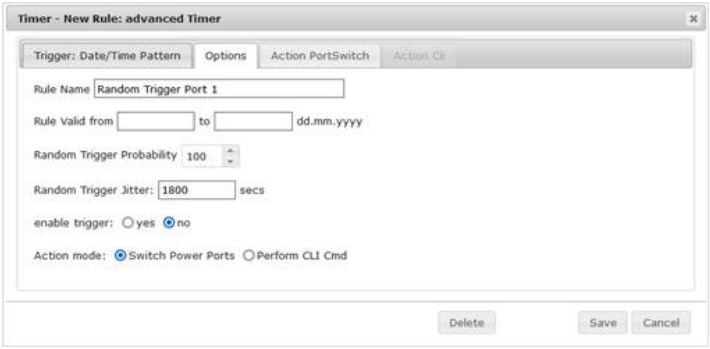


Schaltet jeden Tag Port 3 um 9:25 ein, und um 17:30 wieder aus. Man speichert.



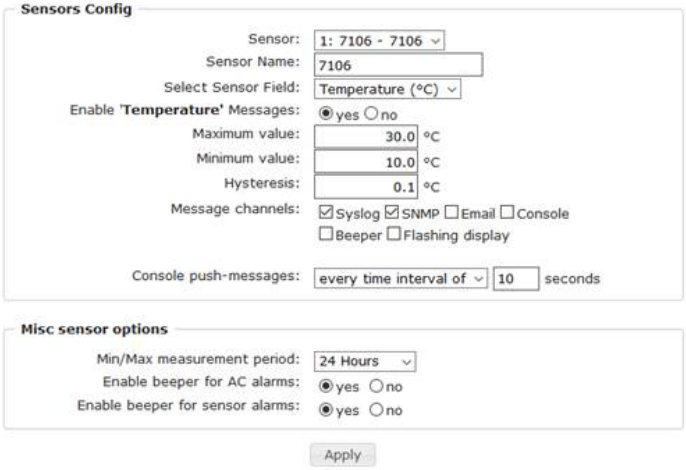
Danach ruft man die beiden angelegten Timer Regeln auf ("On" und "Off") und trägt dort jeweils im "Options" Register das Datum ein, an dem der Schaltvorgang stattfinden soll.

Beispiel Jalousiesteuerung



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

3.6 SENSORS



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

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

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

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

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

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

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

Durch Flashing Display blinkt die 7-Segment Anzeige. Bei einem Druck auf einen Frontblenden Taster werden Beeper und die blinkende Anzeige wieder zurückgesetzt.

Console push-messages: Diese Option ermöglicht die Ausgabe von Sensorwerten auf der Konsole in einem konfigurierten Zeitintervall, oder wenn sich eine bestimmte Größenänderung des Wertes ergeben hat.

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

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

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

Hysterese Beispiel

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

Beispiel:
49,9 °C - unterhalb der Obergrenze
50,0 °C - Meldung 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 - Meldung für das Überschreiten der oberen Grenze inklusive Hysterese-Bereich

3.7 E-MAIL

Enable E-Mail: Hier können Sie einstellen ob E-Mails versendet werden sollen.

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

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

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

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

SMTP Connection Security: Übertragung per SSL oder ohne Verschlüsselung.

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

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

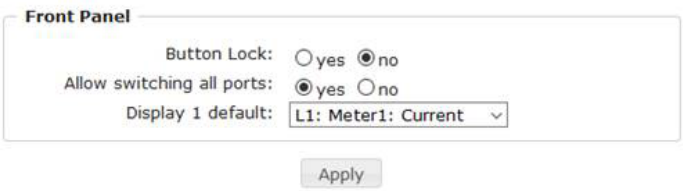
Set new password: Tragen Sie hier das Passwort, für die Anmeldung beim E-Mail-server, ein.

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.

3.8 FRONT PANEL



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

Allow switching all ports: Ermöglicht es mit den Frontblenden Tasten alle Ports entweder ein- oder auszuschalten.

Display 1 default: Wählt die Ansicht von Sensorwerten für das Display.

4. SPEZIFIKATIONEN

4.1 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, SSH und serielle) bieten den kompletten Zugriff auf das Gerät.

Dieses Kapitel ist allgemein für alle Modelle gehalten. Je nach Modell sind Ports, bestimmte Sensoren oder andere Features nicht verfügbar.

Liste der unterschiedlichen Zugriffsmöglichkeiten:

Schnittstelle	Umfang des Zugriffs
HTTP	- Lesen/Schreiben Zustand der Powerports (Relais oder eFuses) - Lesen/Schreiben aller Konfigurationsdaten - Lesen/Schreiben aller Statusinformationen (vollständiger Zugriff auf das Gerät)
Konsole	- Lesen/Schreiben Zustand der Powerports (Relais oder eFuses) - Lesen/Schreiben aller Konfigurationsdaten - Lesen/Schreiben aller Statusinformationen (vollständiger Zugriff auf das Gerät)
SNMP	- Lesen/Schreiben Zustand der Powerports (Relais oder eFuses) - Lesen/Schreiben Namen der Powerports (Relais oder eFuses) - Lesen/Schreiben Zustand der Port Startkonfiguration - Lesen/Schreiben Zustand Buzzer - Lesen/Schreiben Konfiguration der Stromquellen (EPC 8291) - Lesen/Schreiben Konfiguration des Lüfters (EPC 8291) - Lesen Messwerte externer Sensoren - Lesen Messwerte aller Energiesensoren - Lesen NTP Zeit und Status - Rücksetzen der Energiezähler - Lesen Zustand Overvoltage Protection
Modbus TCP	- Lesen/Schreiben Zustand der Powerports (Relais oder eFuses) - Lesen Zustand der Eingänge - Lesen/Schreiben Konfiguration der Stromquellen (EPC 8291) - Lesen/Schreiben Konfiguration des Lüfters (EPC 8291) - Lesen Messwerte externer Sensoren - Lesen Messwerte aller Energiesensoren - Lesen Zustand Overvoltage Protection
MQTT	Ausführen von Konsolenkommandos

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

4.2 NACHRICHTEN

In Abhängig von einstellbaren Ereignissen können vom Gerät verschiedene Nachrichtenarten verschickt werden. Dieser Abschnitt ist für alle Modelle allgemein gehalten, und beinhaltet auch Nachrichten, die nicht jedes Modell unterstützt. Folgende Nachrichtenkanäle werden unterstützt:

- Syslog Nachrichten
- SNMP Traps
- Telnet / SSH Meldungen
- MQTT published Nachrichten
- Versendung von E-Mails

Globale Benachrichtigungen

Diese Nachrichten werden automatisch an alle Nachrichtenkanäle geschickt. Sie beinhalten wichtige Informationen über den Zustand des Geräts. Auf Kundenwunsch kann man jetzt Port-Schaltnachrichten konfigurieren, da z.B. nicht jeder auch eine Email-Benachrichtigung beim Schalten haben möchte. Folgende globale Nachrichten können in der Sensorkonfiguration unter System eingestellt werden:

- Port-Schaltnachrichten
- eFuse Auslösung

Value-Threshold Nachrichten

Bei elektrischen Messwerten und externen Sensoren kann man Grenzwerte für Maximum und Minimum einstellen. Ein Überschreiten der Grenzwerte, und die Rückkehr in den Normalbereich erzeugt den Nachrichtenversand.

Time-Interval Nachrichten

Diese Nachrichten kommen in einem voreingestellten Zeit-Intervall und beinhalten den aktuellen Messwert. Als Nachrichtenkanäle sind nur MQTT oder eine Konsolenverbindung (Telnet, SSH, seriell) möglich.

Value-Delta Nachrichten

Hier konfiguriert man einen Betrag für eine Abweichung. Nachrichten werden verschickt, wenn Messwerte sich um den eingestellten Betrag vergrößern oder verkleinern. Als Nachrichtenkanäle sind nur MQTT oder eine Konsolenverbindung (Telnet, SSH, seriell) möglich.

Aktivierung der Nachrichten-Kanäle

Für die jeweiligen Nachrichtentypen können die entsprechenden Kanäle in der Sensor-Konfiguration unter „Message Channels“ aktiviert werden. Nur wenn dort ein Häkchen gesetzt ist, wird dieser Nachrichten-Kanal auch verwendet.

Nachrichten Übersichtstabelle

Hier ist die Übersicht, welche Nachrichten auf welchem Kanal verschickt werden.

	SNMP Trap	Konsole	MQTT	Syslog	E-Mail
Global					
Gerät gestartet	x	x	x	x	x
Stromversorgung Status	x	x	x	x	x
Umschaltung Strom-versorgung	x	x	x	x	x
Syslog ein-/ausgeschaltet				x	
MQTT Verbindung aufgebaut			x	x	
Value-Threshold					
externe Sensoren (Strom, Differenzstrom Type A)	x	x	x	x	x
Time-Interval					
externe Sensoren (Strom, Differenzstrom Type A)		x	x		
Value-Delta					
externe Sensoren (Strom, Differenzstrom Type A)		x	x		

SNMP-Traps

Es gibt gemeinsame Traps für Zustandsänderungen der gleichen Geräte-Resource. Z.B. wird beim Ein- oder Ausschalten eines Ports ein SwitchEvtPort Trap gesendet. Die Zustandsänderung selber wird durch die mitgelieferten Daten innerhalb des Traps übermittelt.

MQTT published Daten

Die Nachrichten auf dem MQTT Kanal werden im JSON Format gesendet.

Beispiel: *Einen Port schalten: "{"type": "portswitch", "idx": 2, "port": "2", "state": 1, "cause": {"id": 2, "txt": "http"}, "ts": 1632}"*

Konsolen Push-Nachrichten

Auf den Konsolen-Kanälen (Telnet, SSH oder serielle Konsole) können Push Messages aktiviert werden, die Sensorwerte in zeitlichen Abständen (alle n Sekunden) oder ab einer einstellbaren Größenänderung des Sensorwertes auf diesem Kanal ausgeben. Die erzeugte Nachricht beginnt immer mit einem „#“ und endet mit einem CR/LF.

Beispiel einen Port schalten: "*#port 2 ON*"

Öffnet man eine Telnet oder SSH Verbindung, sind die Push-Nachrichten entweder vorkonfiguriert, oder man schaltet mit "console telnet pushmsgs set 1" (bzw. "console ssh pushmsgs set 1") die Push Messages temporär ein. Auf diesem Kanal werden fortan asynchron Push Messages gesendet. Die Asynchronität der Nachrichten kann auf einer Verbindung Probleme bereiten, wenn man selber gleichzeitig Kommandos schickt. Es gibt dann die Möglichkeiten:

- Man filtert alle eingehenden Zeichen zwischen „#“ und CR/LF
- oder öffnet einen zweiten Kanal (Telnet, SSH, seriell) und schaltet dort die Push-Nachrichten ein

4.3 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.

4.4 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-Identifier. 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.

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

4.5 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, das 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.

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

SNMP v3

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

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 "draftblumenthal-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-snmpv3-usm-3desede-00") eingesetzt wird. Ist man kein SNMP Experte, empfiehlt es sich, jeweils die Einstellungen mit und ohne "...-3DESKey" auszuprobieren.

Passwörter

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

Sicherheit

Folgende Aspekte gibt es zu beachten:

- Sollen Verschlüsselung oder Authentifizierung zum Einsatz kommen, dann SNMP v1 und v2c ausschalten, da sonst darüber auf das Gerät zugegriffen werden kann.
- Wird nur authentifiziert, dann sind die neuen „HMAC-SHA-2“ Verfahren den MD5 oder SHA-1 Hashing Algorithmen überlegen. Da nur SHA-256 in Hardware beschleunigt wird, und SHA-384 sowie SHA-512 rein in Software berechnet werden, sollte man im Normalfall SHA-256 auswählen. Vom kryptographischen Standpunkt reicht die Sicherheit eines SHA-256 zur Zeit vollkommen aus.
- Für SHA-1 gibt es derzeit etwas weniger Angriffsszenarien als für MD5. Im Zweifelsfall ist SHA-1 vorzuziehen.
- Die Verschlüsselung „DES“ gilt als sehr unsicher, nur im Notfall aus Kompatibilitätsgründen einsetzen!
- Es gilt bei Kryptologen als umstritten, ob „HMAC-MD5-96“ und „HMAC-SHA-96“ genügend Entropie für die Schlüssellängen von „AES-192“ oder „AES-256“ aufbringen können.
- Ausgehend von den vorhergehenden Betrachtungen empfehlen wir zur Zeit „HMACSHA-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 epc8221 SwitchEvtPort12. 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 Kommando-zeilen Tools (snmpget, snmpset, snmpwalk, etc.) NET-SNMP ist u.a. für Linux und Windows verfügbar. Nach der Installation von NET-SNMP sollten Sie die Geräte-spezifische 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

4.6.1 GERÄTE MIB

Änderung im Trap-Design

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 Enterprise OID aus Platzgründen bei jedem Eintrag in der Tabelle weggelassen. Die komplette OID würde daher z.B. „1.3.6.1.4.1.28507.41.1.1.1.1" 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.
ets8801TrapCtrl	0 = off, 1 = Ver. 1, 2 = Ver. 2c, 3 = Ver. 3	41.1.1.1.1.0	Integer32	RW
ets8801TrapIPIndex	A unique value, greater than zero, for each receiver slot	.41.1.1.1.2.1.1.x	Integer32	RO
ets8801TrapAddr	DNS name or IP address specifying one Trap receiver slot. A port can optionally be specified: ‚name:port' An empty string disables this slot	.41.1.1.1.2.1.2.x	OCTETS	RW
ets8801Buzzer	turn Buzzer on and off	.41.1.3.10.0	Integer32	RW
ets8801Active PowerChan	Number of supported Power Channels	.41.1.5.1.1.0	Unsigned32	RO
ets8801PowerIndex	Index of Power Channel entries	.41.1.5.1.2.1.1.x	Integer32	RO
ets8801ChanStatus	0 = data not active, 1 = data valid	.41.1.5.1.2.1.2.x	Integer32	RO
ets8801 AbsEnergyActive	Absolute Active Energy counter	.41.1.5.1.2.1.3.x	Unsigned32	RO
ets8801PowerActive	Active Power	.41.1.5.1.2.1.4.x	Integer32	RO
ets8801Current	Actual Curent on Power Channel	.41.1.5.1.2.1.5.x	Unsigned32	RO
ets8801Voltage	Actual Voltage on Power Channel	.41.1.5.1.2.1.6.x	Unsigned32	RO
ets8801Frequency	Frequency of Power Channel	.41.1.5.1.2.1.7.x	Unsigned32	RO
ets8801PowerFactor	Power Factor of Channel between -1.0 and 1.00	.41.1.5.1.2.1.8.x	Integer32	RO
ets8801Pangle	Phase Angle between Voltage and L Line Current between -180.0 and 180.0	.41.1.5.1.2.1.9.x	Integer32	RO
ets8801 PowerApparent	L Line Mean Apparent Power	.41.1.5.1.2.1.10.x	Integer32	RO
ets8801 PowerReactive	L Line Mean Reactive Power	.41.1.5.1.2.1.11.x	Integer32	RO
ets8801 AbsEnergyReactive	Absolute Reactive Energy counter	.41.1.5.1.2.1.12.x	Unsigned32	RO
ets8801AbsEnergy ActiveResettable	Resettable Absolute Active Energy counter. Writing ‚0' resets all resettable counter	.41.1.5.1.2.1.13.x	Unsigned32	RW

Name	Description	OID	Type	Acc.
ets8801AbsEnergy-ReactiveResettable	Resettable Absolute Reactive Energy counter	.41.1.5.1.2.1.14.x	Unsigned32	RO
ets8801ResetTime	Time in seconds since last Energy Counter reset	.41.1.5.1.2.1.15.x	Unsigned32	RO
ets8801 ForwEnergyActive	Forward Active Energy counter	.41.1.5.1.2.1.16.x	Unsigned32	RO
ets8801ForwEnergy-Reactive	Forward Reactive Energy counter.	.41.1.5.1.2.1.17.x	Unsigned32	RO
ets8801ForwEnergy ActiveResettable	Resettable Forward Active Energy counter	.41.1.5.1.2.1.18.x	Unsigned32	RO
ets8801ForwEnergy-ReactiveResettable	Resettable Forward Reactive Energy counter	.41.1.5.1.2.1.19.x	Unsigned32	RO
ets8801 RevEnergyActive	Reverse Active Energy counter	.41.1.5.1.2.1.20.x	Unsigned32	RO
ets8801RevEnergy ActiveResettable	Resettable Reverse Active Energy counter	.41.1.5.1.2.1.22.x	Unsigned32	RO
ets8801RevEnergy ReactiveResettable	Resettable Reverse Reactive Energy counter	.41.1.5.1.2.1.23.x	Unsigned32	RO
ets8801Residual-Current	Actual Residual Current on Power Channel. According Typ A IEC 60755. Only visible on models that support this feature.	.41.1.5.1.2.1.24.x	Unsigned32	RO
ets8801 LineSensorName	A textual string containing name of a Line Sensor	41.1.5.1.2.1.100.x	OCTETS	RW
ets8801FuseIndex	None	.41.1.5.2.1.1.x	Integer32	RO
ets8801FuseStatus	Shows the status of the C13 Output Block Fuse	.41.1.5.2.1.2.x	INTEGER	RO
ets8801 PrimaryPowerAvail	Not zero if primary Power available	.41.1.5.11.1.0	INTEGER	RO
ets8801Secondary PowerAvail	Not zero if secondary Power available	.41.1.5.11.2.0	INTEGER	RO
ets8801 LineSelectRequest	Sends change request to select line 1 (A) or 2 (B)	.41.1.5.11.3.0	INTEGER	RW
ets8801 PowerLineSelected	None	.41.1.5.11.4.0	INTEGER	RO
epc8801 NTPTimeValid	Show if valid Time is received	.41.1.5.15.1.0	INTEGER	RO
epc8801NTPUnixTime	Show received NTP time as unixtime (secs since 1 January 1970)	.41.1.5.15.2.0	Unsigned32	RO
epc8801NTPLast ValidTimestamp	Show seconds since last valid NTP timestamp received	.41.1.5.15.3.0	Unsigned32	RO
ets8801SensorIndex	None	.41.1.6.1.1.1.x	Integer32	RO
ets8801TempSensor	Actual temperature	.41.1.6.1.1.2.x	Integer32	RO
ets8801HygroSensor	Actual humidity	.41.1.6.1.1.3.x	Integer32	RO
ets8801InputSensor	Logical state of input sensor	.41.1.6.1.1.4.x	INTEGER	RO
ets8801AirPressure	Actual air pressure	.41.1.6.1.1.5.x	Integer32	RO

Name	Description	OID	Type	Acc.
ets8801DewPoint	Dew point for actual temperature and humidity	.41.1.6.1.1.6.x	Integer32	RO
ets8801DewPointDiff	Difference between dew point and actual temperature (Temp - DewPoint)	.41.1.6.1.1.7.x	Integer32	RO
ets8801ExtSensor-Name	A textual string containing name of a external Sensor	.41.1.6.1.1.32.x	OCTETS	RW

4.7 SSL

TLS Standard

Das Gerät ist kompatibel zu den Standards TLS v1.1 bis TLS v1.3. Wegen fehlender Sicherheit sind SSL v3.0, TLS 1.0, sowie die Verschlüsselungen RC4, MD5, SHA1 und DES deaktiviert. Alle Ciphers nutzen einen Diffie-Hellman Schlüsselaustausch (Perfect Forward Secrecy).

TLS 1.3 Performance

Beim Zusammenspiel von TLS 1.3 und unsicheren Zertifikaten und einem Webbrowser mit Chromium Engine (Google Chrome oder MS Edge) kann es zu Performance-Einbußen, und damit längeren Ladezeiten kommen. In dieser Konstellation unterstützt die Chromium Engine nicht korrekt den SSL Session Cache (Session Tickets) und die Mathematikeinheit der Embedded CPU kann mit andauernden RSA Operationen überfordert
sein. Mögliche Abhilfen:

- Einsatz von sicheren Zertifikaten (offizielle Zertifizierungsstelle oder im OS als sicher markiert)
- oder Nutzung vom Firefox Browser
- oder Verwendung von ECC 256 (kein RSA) Zertifikaten
- oder auf „TLS v1.2 only“ konfigurieren

Erstellen eigener Zertifikate

Der SSL Stack wird mit einem eigens neu generierten self-signed 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 (2048/4096) und ECC (Elliptic Curve Cryptography) Zertifikate.

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

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

Hier einige Beispiele zur Generierung mit OpenSSL:

Erstellung eines RSA 2048-Bit self-signed Zertifikats

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

RSA 2048-Bit Zertifikat mit Sign Request:

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

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

ECC Zertifikat mit Sign Request:

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

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

Linux: *cat server.crt server.key > server.pem*
Windows: *copy server.crt + server.key server.pem*

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

Sollen mehrere Zertifikate (Intermediate CRT‘s) zusätzlich auf das Gerät geladen werden, so sollte man darauf achten, in der Reihenfolge als erstes das Server-Zertifikat, und dann die Intermediates zusammenzufügen. Z.B: *cat server.crt IM1.crt IM2.crt server.key > server.pem*

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

4.8 KONSOLE

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

Befehlssatz

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

back	Eine Befehlsebene 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 der 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
links, 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

Sensor Beispiele

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.

>extsensor 1 0 value show

Zeigt Temperatur des Sensors an Port 1

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).

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

Diese Varianten geben die Sensorwerte der Feldliste oder eines Sensors an Line 1. Bei Geräten mit Overvoltage Protection wird bei dem "linesensor all" Kommando der Zustand der Protection mit ausgegeben ("OVP=x"). Eine "1" bedeutet Ok, eine "0" ein Ausfall der Protection.

c) Port-Sensoren

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

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

>portsensor 2 „0,1,2,3,12“ show
>portsensor 2 1 show

Diese Varianten geben die Sensorwerte der Feldliste oder eines Sensors an Outlet Port 2.

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 in 3 möglichen Formaten zurück.

e) Port-Relais schalten

>port all state set „1,2,12“ 1
OK.

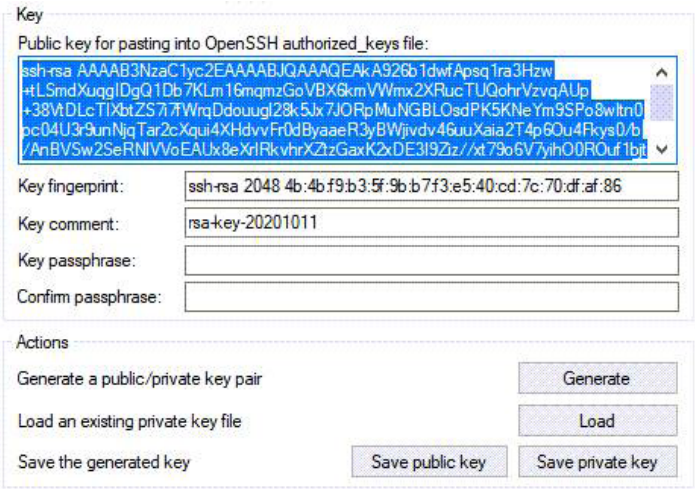
Die Befehlssyntax „port all state set „{port_list}“ {OFF=0|ON=1}“ setzt eine Liste von Ports auf den Zustand ON=1 oder OFF=0.

4.8.1 SSH

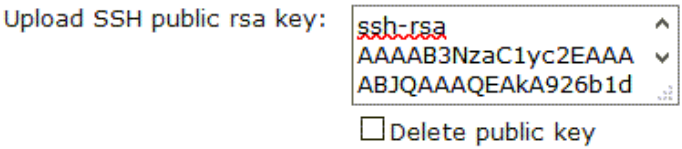
Das Gerät unterstützt SSH-2 Verbindungen entweder mit Public Key Authentifizierung oder Benutzernamen und Passwort. Der "login" muss für SSH aktiviert sein. Benutzer und Passwörter können lokal gespeichert sein, oder über einen Radius Server abgefragt werden. Möchte man SSH in einem Terminal verwenden, sollte Activate echo eingeschaltet sein.

Public Keys

Es werden RSA und ECDSA Public Keys akzeptiert.



Generierte Schlüssel können z.B. direkt aus putty gen kopiert,



und direkt in das Configuation - Console Eingabefeld eingefügt werden. Public Keys werden im SSH2 oder OpenSSH Format angenommen.

4.8.2 CONSOLE CMD ANS3100RM/ANS3000RM

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
clock	enters cmd group „clock“	
clock ntp enabled set {OFF=0|ON=1}	enables ntp	
clock ntp enabled show	shows if ntp enabled	
clock timezone set {minutes}	sets timezone	
clock timezone show	shows timezone	
clock dst enabled set {OFF=0|ON=1}	enables dst	
clock dst enabled show	shows if dst is enabled	
clock manual set „{hh:mm:ss yyyy-mm-dd}“	sets time and date manually	
clock show	shows actual time and date	
clock ntp server {PRIMARY=0|BACKUP=1} set„{dns_name}“	sets ntp server name	
clock ntp server {PRIMARY=0|BACKUP=1} show	shows ntp server name	
console	enters cmd group „console“	
console version	shows unique console version number	
console telnet enabled set {OFF=0|ON=1}	enables telnet on/off	
console telnet enabled show	shows if telnet enabled	
console telnet port set {ip_port}	sets telnet port	
console telnet port show	shows telnet port	
console telnet raw set {OFF=0|ON=1}	sets raw mode (disables editing) on/off	
console telnet raw show	shows if raw mode enabled	
console telnet echo set {OFF=0|ON=1}	enables echo on/off	
console telnet echo show	shows if echo enabled	
console telnet activeneg set {OFF=0|ON=1}	enables telnet active negotiation (IAC) on/off	
console telnet activeneg show	shows if active negotiation enabled	
console telnet login set {OFF=0|ON=1}	enables login on/off	
console telnet login show	shows if login enabled	

Command	Description	Note
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 pushmsgs config set {OFF=0 | ON=1}	enables persistent push msgs	
console telnet pushmsgs config show	shows if persistent push msgs are enabled	
console telnet pushmsgs set {OFF=0 | ON=1}	enables temporary push msgs	
console telnet pushmsgs show	shows if temporary push msgs are 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 ssh enabled set {OFF=0 | ON=1}	enables SSH	
console ssh enabled show	shows if SSH enabled	
console ssh port set {ip_port}	sets SSH port	
console ssh port show	shows SSH port	
console ssh echo set {OFF=0 | ON=1}	enables echo on/off	
console ssh echo show	shows if echo enabled	
console ssh pushmsgs config set {OFF=0 | ON=1}	enables persistent push msgs	
console ssh pushmsgs config show	shows if persistent push msgs are enabled	
console ssh pushmsgs set {OFF=0 | ON=1}	enables temporary push msgs	
console ssh pushmsgs show	shows if temporary push msgs are enabled	
console ssh public hash set „{passwd}“	sets hash of SSH public key	
console ssh public hash show	shows hash of SSH public key	
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	

Command	Description	Note
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	show email authentication	
email user set „{username}“	sets 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	
ets	eneters cmd group „ets“	
ets {line_num} state show	shows if line has power	
ets line selected set {1..2}	select line when power avail and preferred = none	
ets line selected show	shows selected line	
ets line preferred {NONE=0|INPUTA=1|INPUTB=2} set	set preferred line	
ets line preffered show	shows preferred line	
ets sensitivity set {LOW=0|HIGH=1}	sets sensitivity	

Command	Description	Note
ets sensitivity show	shows sensitivity	
ets fastonsync set {OFF=0|ON=1}	sets faster switching when on same phase	
ets fastonsync show	shows if faster switching enabled	
ets beeper set {OFF=0|ON=1}	enables beeper when line not avail	
ets beeper show	shows ets beeper state	
extsensor	enters cmd group „extsensor“	
extsensor all show	shows all values from connected external sensors	
extsensor all show	shows all plugged sensors and fields	
extsensor {port_num} {sen_field} value show	shows sensor value	6
extsensor {port_num} {sen_type} label set „{name}“	sets sensor name to label	6
extsensor {port_num} {sen_type} label show	shows label of sensor	6
extsensor {port_num} type show	shows type of sensor	
extsensor {port_num} {sen_type} {sen_field} events set {off=0|on=1}	enables sensor events on/off	6
extsensor {port_num} {sen_type} {sen_field} events show	shows if sensor events are enabled	6
events type set „{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5,EVT_DISPLAY=6,EVT_CONSOLE=7,EVT_MQTT=8}“	enables different event types	6
extsensor {port_num} {sen_type} {sen_field} events type show	shows what event types are enabled	6
extsensor {port_num} {sen_type} {sen_field} maxval set {num}	sets maximum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} maxval show	sets maximum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} minval set {num}	sets minimum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} minval show	shows minimum value for sensor	6
extsensor {port_num} {sen_type} {sen_field} hyst set {num}	sets hysterese value for sensor	6
extsensor {port_num} {sen_type} {sen_field} hyst show	shows hysterese value for sensor	6
extsensor {port_num} {sen_type} {sen_field} publish mode set {NONE=0|INTERVAL=1|DELTA=2|INTERV_DELTA=3}	sets publish mode	
extsensor {port_num} {sen_type} {sen_field} publish mode show	shows publish mode	

Command	Description	Note
extsensor {port_num} {sen_type} {sen_field} publish mqtt retain set {OFF=0|ON=1}	sets mqtt retain	
extsensor {port_num} {sen_type} {sen_field} publish mqtt retain show	shows if mqtt retain set	
extsensor {port_num} {sen_type} {sen_field} publish timer set {num_secs}	sets publish time interval	
extsensor {port_num} {sen_type} {sen_field} publish timer show	shows publish time interval	
extsensor {port_num} {sen_type} {sen_field} publish delta set {float}	sets publish delta value	
extsensor {port_num} {sen_type} {sen_field} publish delta show	shows publish delta value	
extsensor period set {24H=0|12H=1|2H=2|1H=3|30MIN=4}	sets sensor Min/Max measurement period	
extsensor period show	shows sensor Min/Max measurement period	
extsensor beeper set {OFF=0|ON=1}	enables beeper sensor alarms	
extsensor beeper show	shows if beeper sensor alarms are enabled	
http	enters cmd group „http“	
http server set {HTTP_BOTH=0|HTTPS_ONLY=1|HTTP_ONLY=22|HTTPS_REDIR=3}	sets accepted connection types	
http server show	shows accepted connection types	
http port set {ip_port}	sets http port	
http port show	shows http port	
http portssl set {ip_port}	sets https port	
http portssl show	shows https port	
http tls mode set {TLS12=0|TLS13_12=1|TLS13=2|TLS13_12_11=3}	restricts TLS mode	
http tls mode show	shows TLS mode restriction	
http 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 local set {OFF=0|ON=1}	enables local login on/off	
http passwd local show	shows if local login enabled	
http passwd radius set {OFF=0|ON=1}	enables login for RADIUS on/off	
http passwd radius show	shows if RADIUS login enabled	
http passwd user set „{passwd}“	sets http user password	
http passwd admin set „{passwd}“	sets http admin password	

Command	Description	Note
http passwd admin set „{passwd}“	sets http admin password	
http passwd hash user set „{passwd}“	sets hashed http user password	
http passwd hash admin set „{passwd}“	sets hashed http admin password	
ip4	enters cmd group „ip4“	
ip4 hostname set „{name}“	sets device hostname	
ip4 hostname show	shows device hostname	3
ip4 address set „{ip_address}“	sets IPv4 address	
ip4 address show	shows IPv4 address	3
ip4 netmask set „{ip_address}“	sets IPv4 netmask	
ip4 netmask show	shows IPv4 netmask	3
ip4 gateway set „{ip_address}“	sets IPv4 gateway address	
ip4 gateway show	shows IPv4 gateway address	3
ip4 dns set „{ip_address}“	sets IPv4 DNS server address	
ip4 dns show	shows IPv4 DNS server address	3
ip4 dhcp enabled set {OFF=0|ON=1}	enables IPv4 DHCP on/off	
ip4 dhcp enabled show	shows IPv4 DHCP state	3
ip6	enters cmd group „ip6“	
ip6 enabled set {OFF=0|ON=1}	enables IPv6 on/off	
ip6 enabled show	shows if IPv6 is enabled	3
ip6 routadv enabled set {OFF=0|ON=1}	enables IPv6 router advertisement	
ip6 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

Command	Description	Note
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}	
linesensor	enters cmd group „linesensor“	
linesensor all {field_list} show	shows energy sensors according field list of all line sensors	5
linesensor {line_num} {field_list} show	shows energy sensors according field list of one line sensor	5
linesensor {line_num} {energy_sensor} value show	shows energy sensor of given line	5
linesensor {line_num} ovp show	show state of Overvoltage Protection	
linesensor {line_num} counter reset	resets energy metering counter	
linesensor {line_num} label set „{name}“	sets line meter to label	
linesensor {line_num} label show	shows label of line meter	
linesensor {line_num} {energy_sensor} events set {OFF=0|ON=1}	enables events on/off	
linesensor {line_num} {energy_sensor} events show	shows if events are enabled	
linesensor {line_num} {energy_sensor} events type set „{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}“		
linesensor {line_num} {energy_sensor} events type show	shows what event types are enabled	
linesensor {line_num} {energy_sensor} maxval set {float}	sets maximum value for line meter	
linesensor {line_num} {energy_sensor} maxval show	shows maximum value for line meter	
linesensor {line_num} {energy_sensor} minval set {float}	sets minimum value for line meter	
linesensor {line_num} {energy_sensor} minval show	shows minimum value for line meter	
linesensor {line_num} {energy_sensor} hyst set {float}	sets hysterese value for line meter	

Command	Description	Note
linesensor {line_num} {energy_sensor} hyst show	shows hysterese value for line meter	
linesensor {line_num} {energy_sensor} publish mode set {NONE=0|INTERVAL=1|DELTA=2|INTERV_DELTA=3}	sets publish mode	
linesensor {line_num} {energy_sensor} publish mode show	shows publish mode	
linesensor {line_num} {energy_sensor} publish mqtt retain set {OFF=0|ON=1}	sets mqtt retain	
linesensor {line_num} {energy_sensor} publish mqtt retain show	shows if mqtt retain set	
linesensor {line_num} {energy_sensor} publish timer set {num_secs}	sets publish time interval	
linesensor {line_num} {energy_sensor} publish timer show	shows publish time interval	
linesensor {line_num} {energy_sensor} publish delta set {float}	sets publish delta value	
linesensor {line_num} {energy_sensor} publish delta show	shows publish delta value	
linesensor {line_num} events set {OFF=0|ON=1}	LEGACY - enables events on/off	L
linesensor {line_num} events show	LEGACY - shows if events are enabled	L
linesensor {line_num} events type set „{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SMS=3,EVT_GSMEMAIL=4,EVT_BEEPER=5,EVT_DISPLAY=6,EVT_CONSOLE=7,EVT_MQTT=8}“	LEGACY - enables different event types	L
linesensor {line_num} events type show	LEGACY - shows what event types are enabled	L
linesensor {line_num} maxval set {float}	LEGACY - sets maximum value for line meter	L
linesensor {line_num} maxval show	LEGACY - shows maximum value for line meter	L
linesensor {line_num} minval set {float}	LEGACY - sets minimum value for line meter	L
linesensor {line_num} minval show	LEGACY - shows minimum value for line meter	L
linesensor {line_num} hyst set {float}	LEGACY - sets hysterese value for line meter	L
linesensor {line_num} hyst show	LEGACY - shows hysterese value for line meter	L
linesensor beeper set {OFF=0|ON=1} enables beeper for line meter alarms	enables beeper for line meter alarms	
linesensor beeper show	shows if beeper for line meter alarms is enabled	
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	

Command	Description	Note
mqtt	enters cmd group „mqtt“	
mqtt {broker_idx} enabled set {OFF=0|ON=1}	enable mqtt	
mqtt {broker_idx} enabled show	shows if mqtt enabled	
mqtt {broker_idx} server set „{dns_name}“	sets broker name	
mqtt {broker_idx} server show	shows broker name	
mqtt {broker_idx} tls enabled set {OFF=0|ON=1}	enable TLS	
mqtt {broker_idx} tls enabled show	shows if TLS enabled	
mqtt {broker_idx} port set {ip_port}	set broker TCP/IP port	
mqtt {broker_idx} port show	shows broker TCP/IP port	
mqtt {broker_idx} user set „{username}“	sets username	
mqtt {broker_idx} user show	shows username	
mqtt {broker_idx} passwd set „{passwd}“	sets password	
mqtt {broker_idx} passwd hash set „{passwd}“	sets hashed passwd	
mqtt {broker_idx} client set „{name}“	sets client name	
mqtt {broker_idx} client show	shows client name	
mqtt {broker_idx} qos set {QOS0=0|QOS1=1}	sets QoS level	
mqtt {broker_idx} qos show	shows QoS level	
mqtt {broker_idx} keepalive set {num_secs}	sets keep-alive time	
mqtt {broker_idx} keepalive show	shows keep-alive time	
mqtt {broker_idx} topic set „{name}“	sets topic prefix	
mqtt {broker_idx} topic show	shwos topic prefix	
mqtt {broker_idx} console enabled set {OFF=0|ON=1}	permit console cmds	
mqtt {broker_idx} console enabled show	shows if console cmds allowed	
mqtt {broker_idx} device data timer set {num_secs}	sets telemetry interval	
mqtt {broker_idx} device data timer show	shows telemetry interval	
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	

Command	Description	Note
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 {0..99}	sets server number of retries	
radius {PRIMARY=0|SECONDARY=1} retries show	shows server number of retries	
radius chap enabled set <off=0/on=1>	enables CHAP	
radius chap enabled show	shows if CHAP is enabled	
radius message auth set <off=0/on=1>	enables request message authentication	
radius message auth show	shows if request message authentication is enabled	
radius default timeout set {num_secs}	sets default session timeout (when not returned as Session-Timout Attribute)	
radius default timeout show	shows default session timeout	
snmp	enters cmd group „snmp“	
snmp port set {ip_port}	sets SNMP UDP port	
snmp port show	shows SNMP UDP port	
snmp snmpget enabled set {OFF=0|ON=1}	enables SNMP GET cmds on/off	
snmp snmpget enabled show	show if SNMP GET cmds are enabled	
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 isenabled	

Command	Description	Note
snmp snmpv2 private show	shows SNMP v2 public community	
snmp system {CONTACT=0|NAME=1|LOCATION=2} set „{text}“	sets sysLocation/sysName/sysContact	
snmp system {CONTACT=0|NAME=1|LOCATION=2} show	gets sysLocation/sysName/sysContact	
snmp snmpv3 enabled set {OFF=0|ON=1}	sets SNMP v2 private community	
snmp snmpv3 enabled show	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	

Command	Description	Note
system	enters cmd group „system“	
system beeper manual set {OFF=0|ON=1} {millisec}	manually sets beeper with optional duration	
system beeper manual show	shows beeper state	
system restart	restarts device	
system fabsettings	restore fab settings and restart device	
system bootloader	enters bootloader mode	
system flushdns	flush DNS cache	
system uptime	number of seconds the device is running	
system name show	shows device name	
system version show	shows actual firmware version	
system display {disp_num} default extsensor {port_num} {sen_type} set {sen_field}	shows external sensor	
system display {disp_num} default line-sensor {line_num} set {sen_field}	shows energy line sensor	
system display {disp_num} default set {BLANK=0,LOCAL_TIME=1,UTC_TIME=2}	shows other contents	
system display {disp_num} default show	shows default setting for display	
system display default hash set „{data}“	sets hashed display setting	
system display default hash show	shows hashed display setting	
system panel enabled set {OFF=0|ON=1}	blocks panel buttons when not enabled	
system panel enabled show	shows if panel buttons are enabled	
timer	enters cmd group „timer“	
timer enabled set {OFF=0|ON=1}	enables timer functions	
timer enabled show	shows if timer a enabled	
timer syslog facility set {0..23}	sets facility level for timer syslog	
timer syslog facility show	shows facility level for timer syslog	
timer syslog verbose set {0..7}	sets verbose level for timer syslog	
timer syslog verbose show	shows verbose level for timer syslog	
timer {rule_num} enabled set {OFF=0|ON=1}	enables rule	
timer {rule_num} enabled show	shows if rule is enabled	
timer {rule_num} name set „{name}“	sets name of rule	
timer {rule_num} name show	shows name of rule	
timer {rule_num} {FROM=0|UNTIL=1} set „{yyyymm-dd}“	sets date range of rule	

Command	Description	Note
timer {rule_num} {FROM=0 | UNTIL=1} show	shows date range of rule	
timer {rule_num} trigger jitter set {0..65535}	sets jitter for rule	
timer {rule_num} trigger jitter show	show jitter of rule	
timer {rule_num} trigger random set {0..100}	sets probability for rule	
timer {rule_num} trigger random show	shows rule probability	
timer {rule_num} trigger {HOUR=0 | MIN =1 | SEC=2 | DAY=3 | MON=4 | DOW=5} set „{time_date_list}“	sets time date list	
timer {rule_num} trigger {HOUR=0 | MIN=1 | SEC=2 | DAY=3 | MON=4 | DOW=5} show	shows time date list	
timer {rule_num} action mode set {SWITCH=1 | CLI=2}	sets switch or cli cmd	
timer {rule_num} action mode show	shows if switch or cli cmd	
timer {rule_num} action {SWITCH1=0 | SWITCH2=1} {OFF=0 | ON=1} set „{port_list}“	sets port list for switch cmd	
timer {rule_num} action {SWITCH1=0 | SWITCH2=1} {OFF=0 | ON=1} show	shows port list for switch cmd	
timer {rule_num} action delay set {0..65535}	delay between cmds	
timer {rule_num} action delay show	shows delay between cmds	
timer {rule_num} action console set „{cmd}“	sets cmd string	
timer {rule_num} action console show	shows cmd string	
timer {rule_num} action hash set „{data}“	sets action binary form	
timer {rule_num} action hash show	shows action binary form	
timer {rule_num} delete	delete one timer	
timer delete all	delete all timer	
vt100	enters cmd group „vt100“	
vt100 echo set {OFF=0 | ON=1}	sets console echo state	
vt100 echo show	shows console echo state	
vt100 numeric set {OFF=0 | ON=1}	sets numeric mode	
vt100 numeric show	shows numeric mode state	
vt100 reset	resets terminal	

Hinweise

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

Energie Sensor Tabelle „{energy_sensor}“

Index	Beschreibung	Einheit
0	Absolute Active Energy	Wh
1	Power Active	W
2	Voltage	V
3	Current	A
4	Frequency	0,01 hz
5	Power Factor	0,001
6	Power Angle	0,1 degree
7	Power Apparent	VA
8	Power Reactive	VAR
9	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 Actie 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	mA

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

Externer Sensor Typ Tabelle "{sen_type}"

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

Index	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

4.9 MODBUS TCP

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

Adressbereich Überblick:

Geräte Resource	Start	Ende	Modbus Data Typ
Power/Output/eFuse Ports	0x000	0x3ff	Coils
DC Eingänge	0x400	0x7ff	Discrete Inputs
Stop Condition aktiv	0x800	0x800	Discrete Inputs
POE aktiv	0x801	0x801	Discrete Inputs
Status Power Sources	0x1000	0x100f	Discrete Inputs
OVP aktiv (Line-Ins)	0x1010	0x101f	Discrete Inputs
eFuse Fehler	0x1100	0x11ff	Discrete Inputs
Info Bereich	0x000	0x005	Input Registers
CPU Messwerte	0x080	0x083	Input Registers
Externe Sensoren	0x100	0x1ff	Input Registers
Lüfter-Stufe	0x200	0x20f	Input Registers
Line Energie Sensoren	0x400	0x39ff	Input Registers
Port Energie Sensoren	0x3a00	0x81ff	Input Registers
Bank Energie Sensoren	0x8200	0x823f	Input Registers
Spannungsquellen Sen.	0x8240	0x827f	Input Registers
Residual Current Monitor	0x8280	0x82cf	Input Registers
Bank Power Source Auswahl	0x000	0x00f	Holding Registers
Lüfter Modus	0x010	0x01f	Holding Registers

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

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

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

Function	Request Code
Read Coils	0x01
Read Discrete Inputs	0x02
Write Single Coil	0x05
Write Multiple Coils	0x0f
Read Input Registers	0x04
Read Holding Registers	0x03
Write Holding Register	0x06
Write Multiple Holding Registers	0x10
Read Device Identification	0x2B / 0x0E

Coils

Geräte Resource	Start	Ende	Geräte Funktion
Power / Ouput / eFuse	0x000	0x3ff	Coil entspricht dem Port State
DC Eingänge	0x400	0x7ff	Eingang logisch 1
Stop Condition aktiv	0x800	0x800	Stop Eingang aktiv
POE aktiv	0x801	0x801	POE aktiv
Status Power Sources	0x1000	0x100f	Power Source aktiv
OVP aktiv (Line-Ins)	0x1010	0x101f	OVP aktiv
eFuse Fehler	0x1100	0x11ff	eFuse Fehler

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

Input Registers

Geräte Resource	Start	Ende	Geräte Funktion
Info Bereich	0x000	0x005	siehe Tabelle
CPU Messwerte	0x080	0x083	siehe Tabelle
Externe Sensoren	0x100	0x1ff	siehe Tabelle
Lüfter-Stufe	0x200	0x20f	0 (aus) bis 3 (maximal)
Line Energie Sensoren	0x400	0x39ff	siehe Tabelle
Port Energie Sensoren	0x3a00	0x81ff	siehe Tabelle
Bank Energie Sensoren	0x8200	0x823f	siehe Tabelle
Spannungsquellen Sen.	0x8240	0x827f	siehe Tabelle
Residual Current Monitor	0x8280	0x82cf	siehe Tabelle

Info Bereich

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

Address	Width	Information
0x080 to 0x083	16-bit (signed)	CPU Messwerte
0x100 to 0x1ff	16-bit (signed)	Externe Sensoren
0x400 to 0x39ff	32-bit (signed)	Line Energie Sensoren
0x3a00 to 0x81ff	32-bit (signed)	Port Energie Sensoren
0x8200 to 0x823f	16-bit (signed)	Bank Energie Sensoren
0x8240 to 0x827f	16-bit (signed)	Spannungsquellen Sensoren
0x8280 to 0x82cf	16-bit (signed)	Residual Current Monitor

CPU Messwerte

Offset	Sensor Field	Unit
0	Vsystem	0,01 V
1	Vaux	0,01 V
2	Vmain	0,01 V
3	CPU Temperature	0,1 °C

Externe Sensoren:

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

*0x100 + Port * 8 + Offset*

Bei der Expert Sensor Box 7213 / 7214 entspricht der interne Sensor dem Wert Port = 0. Dort ist bei Sensor 2 der Port = 1, und Port = 2 für Sensor 3.

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

Line und Port Energie Sensoren:

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

Line: 0x0400 + Line * 0x120 + Phase * 0x60 + Offset * 2
Port: 0x3a00 + Port * 0x120 + Phase * 0x60 + 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

Index	Beschreibung	Einheit
0	Absolute Active Energy	Wh
1	Power Active	W
2	Voltage	V
3	Current	A
4	Frequency	0,01 hz
5	Power Factor	0,001

Index	Beschreibung	Einheit
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 Actie 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

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.

Device Identification

Gibt Herstellernamen und Geräte Identifikationen zurück:

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

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
Numbers 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“

4.10 MQTT

Dieses Gerät unterstüzt MQTT 3.1.1 um konfigurierte Nachrichten zu verschicken und auch Kommandos entgeenzunehmen. Dieses Kapitel ist für allgemein gehalten, manche Modelle haben keine schaltbaren Ports.

- Default Port für eine unverschlüsselte Verbindung ist Port 1883.
- Default Port für eine TLS gesicherte Verbindung ist Port 8883.
- Wenn der Broker einen anonymen Login erlaubt, sind Benutzername und Passwort beliebig, aber ein Benutzername muss angegeben werden.
- Wenn mehrere MQTT Clients mit einem Broker verbunden sind, müssen die Namen der Clients verschieden sein. Aus diesem Grund wird als Default Name „client_xxxx“ generiert. Dabei sind „xxxx“ die 4 letzten Stellen der MAC-Adresse.

Nachrichtenformat

Die MQTT Nachrichten des Gerätes werden immer im JSON Format verschickt.

Z.B. *{"type": "portswitch", "idx": 2, "port": "2", "state": 1, "cause": {"id": 2, "txt": "http"}, "ts": 1632}*

Dies ist ein Schalten des zweiten Ports in den Zustand ("state") on. Die Quelle des Schaltkommando ist CGI ("http"). Der Index ist immer numerisch, "port" kann bei Geräten mit mehreren Banks auch alphanumerisch sein, z.B. "A2". Am Ende folgt ein timestamp ("ts"), der die Anzalh der Sekunden anzeigt, die das Gerät eingeschaltet ist, oder unixtime wenn das Gerät sich mit einem NTP-Server synchronisiert hat.

MQTT Topic Prefix

Das Topic Prefix für die Nachrichten ist in der MQTT Konfiguration einstellbar. Ein Default wäre z.B. "de/gudesystems/epc/[mac]". Hier steht "[mac]" als Platzhalter für die MAC-Adresse des Gerätes, ein weiterer möglicher Platzhalter ist "[host]", der den Host-Namen beinhaltet. Ein Beispiel Topic für eine Schaltnachricht des zweites Ports wäre dann:

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

Ausführen von Konsolen Kommandos

Das Gerät kann über MQTT komplett mit Konsolen Kommandos ferngesteuert werden. Eine Liste aller Kommandos findet sich im Kapitel Konsole . Je nach Topic werden die Kommandos in verschiedenen Formaten angenommen.

Als Default ist das Ausführen vom Kommandos nicht erlaubt, sondern muss in der MQTT Konfiguration („Permit CLI commands“) freigeschaltet werden!

Format 1: Kommando in JSON Syntax

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

Antwort vom Gerät an „*de/gudesystems/epc/00:19:32:01:16:41/cmdres*“
„*{„type“: „cli“, „cmdres“: [„OK.“], „result“: {„num“: 0, „hint“: „ok“}, „id“: 10}*“

Das JSON Objekt „result“ gibt zurück, ob das Kommando valide war. Das Objekt „id“ im Kommando ist optional und wird in der Antwort vom Gerät durchgereicht. Die Übergebene Nummer kann helfen eine Synchronizität zwischen Kommando und Antwort über den Broker herzustellen.

Format 2: Raw Text

Publish Topic: „*de/gudesystems/epc/00:19:32:01:16:41/cmd/cli*“ Publish Message: „*port 2 state set 1*“

Antwort vom Gerät an „*de/gudesystems/epc/00:19:32:01:16:41/cmdres/cli*“
„*OK.*

Format 3: Vereinfachtes Port schalten

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

Antwort vom Gerät an "de/gudesystems/epc/00:19:32:01:16:41/cmdres/port/2"
"0" oder "1"

Diese Spezialform existiert nur für die Port Schaltbefehle.

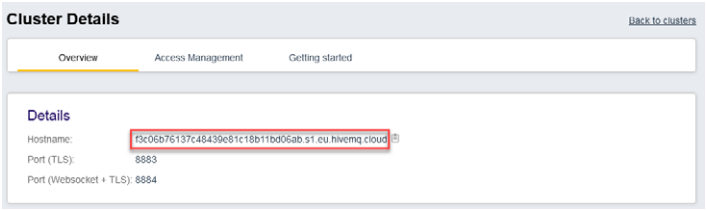
Device Data Summary

In der Device Data Summary werden in einem JSON Objekt die wichtigsten Daten des Gerätes zusammengefasst und in einem konfigurierbaren Zeitintervall periodisch verschickt. Diese Zusammenfassung hängt von den Eigenschaftes des Gerätes und der angeschlossenen Sensoren ab, und könnte z.B. so aussehen:
Topic: de/gudesystems/epc/00:19:32:01:16:41/device/telemetry
Nachricht:

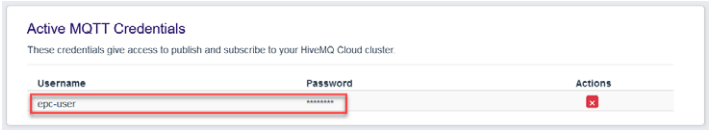

```
{
„type“: „telemetry“,
„portstates“: [{
„port“: „1“,
„name“: „Power Port“,
„state“: 1
}, {
„port“: „2“,
„name“: „Power Port“,
„state“: 0
}, {
„port“: „3“,
„name“: „Power Port“,
„state“: 0
}, {
„port“: „4“,
„name“: „Power Port“,
„state“: 0
}],
„line_in“: [{
„voltage“: 242.48,
„current“: 0.000
}],

„sensors“: [{
„idx“: 1,
„name“: „7105“,
„data“: [{
„field“: „temperature“,
„v“: 21.1,
„unit“: „deg C“
}, {
„field“: „humidity“,
„v“: 71.9,
„unit“: „%“
}, {
„field“: „dew_point“,
„v“: 15.8,
„unit“: „deg C“
}, {
„field“: „dew_diff“,
„v“: 5.3,
„unit“: „deg C“
}]
}],
„ts“: 210520
}
```

4.10.1 BEISPIEL HIVEMQ

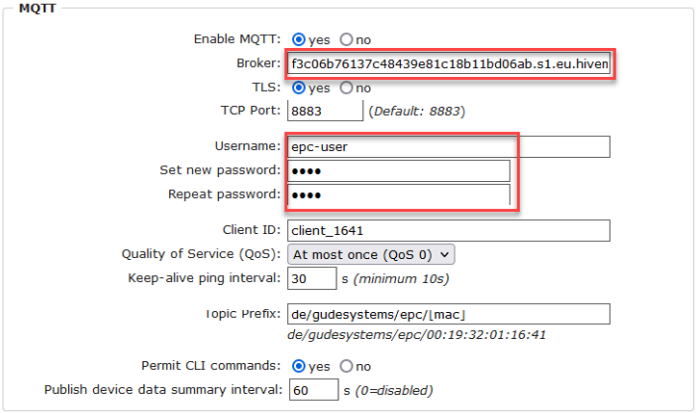
Wie sieht nun eine MQTT Konfiguration am Beispiel HiveMQ aus?



Man legt bei www.hivemq.com einen freien oder kommerziellen Account an, und erstellt einen neuen Cluster.



Im Bereich "Manage Clusters" geht man auf das "Access Management" und fügt einen MQTT Benutzer mit Name und Passwort hinzu.



In der MQTT Konfiguration des Gerätes übertragt man den Hostname des HiveMQ Brokers, sowie Benutzername und Passwort. Zusätzlich TLS aktivieren und den korrekten Port einstellen.

5. SUPPORT

Auf unseren Internetseiten unter www.kess.at 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.

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 (TLS) erlauben.
- Falls möglich TLS 1.3 nutzen, und TLS 1.1 vermeiden.
- In SNMPv3 Authentifizierung und Verschlüsselung einschalten.
- SNMP v2 abschalten.
- In der E-Mail Konfiguration STARTTLS bzw. SSL einschalten.
- Konfigurationsdateien sicher archivieren, sie enthalten sensible Informationen.
- In der IP ACL nur die Geräte eintragen, die Zugriff auf das Gerät benötigen.
- Wenn möglich SSH nutzen, da Telnet unverschlüsselt ist.
- Login für Telnet oder serielle Konsole setzen.
- MQTT 3.1.1 nur mit TLS und Passwort nutzen.
- Bei MQTT „Permit CLI commands“ nur einschalten wenn der Broker vertrauenswürdig ist.
- Modbus TCP ist unverschlüsselt, 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

KESS Power Solutions GmbH
Gewerbestraße 6
3580 Horn
Telefon: +43 720 895010-0
Fax: +43 720 895010-20
E-Mail: info@kess.at
Internet: www.kess.at

5.3 KONFORMITÄTSERKLÄRUNG

Dieses Produkt ist mit den europäischen Richtlinien für die CE-Kennzeichnung konform. Die vollständige CE-Konformitätserklärung für dieses Produkt erhalten Sie gerne auf Anfrage.

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 zu finden. Sehen Sie ihr Gerät in der Liste, überprüfen Sie die dort eingestellten TCP/IP-Parameter und korrigieren Sie die Werte gegebenenfalls.

Wird das Gerät im Bootloader-Modus nicht von GBL_Conf.exe gefunden, haben Sie noch die Möglichkeit, die Einstellungen in den Werkszustand zurückzusetzen.

2. Was kann man machen, wenn das Gerät nicht mehr erreichbar ist, aber die Tasten noch reagieren?

Ein Betreten oder Verlassen des Bootloader Modus verändert nicht den Zustand der Relais. Im Kapitel Maintenance findet sich eine Beschreibung, wie man durch die Tasten den Bootloader aktiviert und danach wieder beendet. Dies führt einen Restart der Firmware durch, ohne dass Relais geschaltet werden. Diese Prozedur hilft aber nicht, wenn das Netzwerk an sich falsch konfiguriert ist.

3. Wo ist in dem Gerät die Seriennummer gespeichert?

Die Seriennummer ist nicht im Gerät gespeichert, sondern nur auf dem Geräteaufkleber sichtbar. Man kann sich aber in der IP Address Konfiguration die MAC-Adresse anzeigen lassen. Wenn Sie mit der MAC-Adresse den Systems Support kontaktieren, geben wir Ihnen gerne die zugehörige Seriennummer.

4. 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.

5. Kann man mehrere E-Mail Empfänger eintragen?

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

6. 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

7. Einspielen einer älteren Firmware

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

8. Deaktivieren der Schalt-Events

Man kann das Senden von Syslog, emails etc. beim Schalten von Ports (betrifft nur Geräte mit Relais) unter "System" in der Sensor-Konfiguration einstellen.

KESS Power Solutions GmbH

Gewerbestraße 6
3580 Horn
Austria

Tel. +43 720895010-0

info@kess.at

www.kess.at