



# MultiBox-pro LAN+

ANTRAX Datentechnik GmbH

## Bedienungsanleitung

**ANTRAX Datentechnik GmbH**

Hasenbrink 4, 32052 Herford

+49 (0) 5221 929 66-0

+49 (0) 5221 929 66-28

Stand: 28.06.2017

# Contents

Bedienungsanleitung.....	1
1.Gerätebeschreibung.....	4
1.1.Sicherheitserklärung.....	4
1.2.Lieferumfang.....	4
1.3.Beschreibung.....	4
1.4.Anschluss und Inbetriebnahme.....	6
1.5.Überspannungsschutz.....	7
1.6.Status LED.....	7
1.7.Bootloader-Modus.....	7
1.8.Firmware-Update.....	8
1.9.Technische Daten.....	9
1.9.1.Elektrische Meßgrößen.....	10
1.10.Sensoren.....	11
2.Bedienung.....	12
2.1.Bedienung am Gerät.....	12
2.2.Control Panel.....	12
2.3.Maintenance Funktionen.....	14
3.Konfiguration.....	15
3.1.Konfiguration per Webinterface.....	16
3.1.1.Power-Ports.....	17
3.1.2.Watchdog.....	18
3.1.3.IP Address.....	20
3.1.4.IP ACL.....	21
3.1.5.HTTP.....	22
3.1.6.Console.....	23
3.1.7.Sensors.....	24
3.1.8.SNMP.....	26
3.1.9.Syslog.....	27
3.1.10.E-Mail.....	28
4.Spezifikationen.....	29
4.1.IP ACL.....	29
4.2.IPv6.....	29
4.3.SNMP.....	30

4.3.1.Geräte MIB.....	32
4.4.SSL.....	34
4.5 Konsole.....	36
4.5.1 Konsole Cmd 1202.....	38
4.6 Nachrichten.....	44
4.6.1.E-Mail.....	44
4.6.2.SNMP Traps.....	44
4.6.3.Syslog.....	44
5.Support.....	45
5.1.Datensicherheit.....	45
5.2.Kontakt.....	45
5.3.FAQ.....	45

# 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.
- Beachten Sie auch die Sicherheitshinweise in der Anleitung.
- 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 recyceln Sie das Verpackungsmaterial.
- Sollten Sie sich über den korrekten Anschluss nicht im Klaren sein oder sollten sich Fragen ergeben, die nicht durch die Bedienungsanleitung abgeklärt werden, so setzen Sie sich bitte mit unserem Support in Verbindung.
- Schließen Sie **nur** Elektrogeräte an, die keine eingeschränkte Einschaltdauer haben. D.h. alle angeschlossenen Elektrogeräte müssen im Fehlerfall eine Dauereinschaltung verkraften, ohne Schäden anzurichten.

## 1.2. Lieferumfang

Im Lieferumfang enthalten sind:

- **MultiBox-pro LAN+**
- Schnellstart-Anleitung

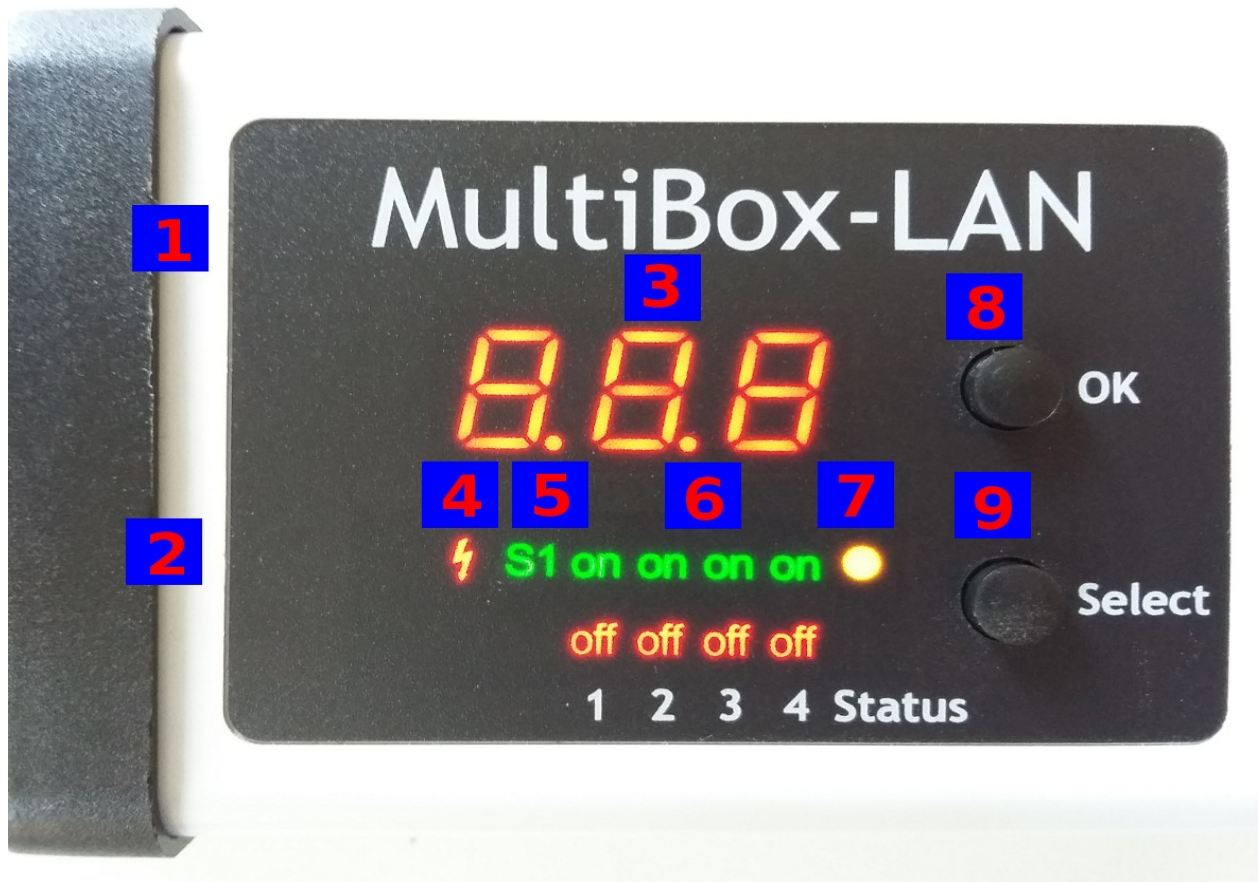
## 1.3. Beschreibung

Der **MultiBox-pro LAN+** kann 4 verschiedene Lastausgänge (Schuko-Steckdosen (CEE 7/3), max. 16A) schalten. Das Gerät hat folgende Features:

- 4 Power-Ports einzeln am Gerät, per HTTP(S), SNMP schaltbar
- Gehäuse ermöglicht Montage in 19 Zoll-Schränken

- Schaltzustand und Einschaltverzögerung (0...9999 Sekunden) für jeden Power-Port nach Stromausfall einstellbar
- Stromspitzen bei gleichzeitigen Schaltvorgängen werden durch eine automatische Latenzzeit von 1 Sekunde verhindert
- Programmierbare Ein-/Ausschaltsequenz 4-Kanal-Watchdog, jedem Power-Port kann ein eigener Watchdog (ICMP/TCP) zugewiesen werden
- Eingangsseitige Messung von Strom, Spannung, Phasenwinkel, Leistungsfaktor, Frequenz, Wirk-, Schein- und Blindleistung
- 2 Energiezähler, ein Zähler zählt dauerhaft, der andere Zähler ist rücksetzbar
- Gut ablesbares LED-Display am Gerät zur Anzeige von Gesamtstrom, IP-Adresse, Sensoren und Fehlermeldungen
- Anschluss für optionale Sensoren zur Umgebungsüberwachung (Temperatur und Luftfeuchtigkeit)
- Integrierter Überspannungsschutz verhindert Beschädigung des Geräts und angeschlossener Verbraucher (L-N 10 kA), Zustand über Netzwerk abrufbar
- Spezielle High-Inrush Relais verhindern Verschweißen der Relaiskontakte bei Einschaltstromspitzen
- Einfache und flexible Konfiguration über Webbrowser
- Erzeugung von Nachrichten (E-Mail, Syslog und SNMP Traps) bei dem Schalten der Relais und in Abhängigkeit von Grenzwerten der Energiemessung oder der externen Sensoren
- Firmware-Update im laufenden Betrieb über Ethernet möglich
- IPv6-ready
- HTTP/HTTPS, E-Mail (SSL, STARTTLS), DHCP, Syslog
- Konsolensteuerung über Telnet
- SNMPv1, v2c, v3 (Traps)
- TLS 1.0, 1.1, 1.2
- Zugriffsschutz durch IP-Zugriffskontrolle
- Secure Login über SSL
- Geringer Eigenverbrauch
- Entwickelt und produziert in Deutschland

## 1.4. Anschluss und Inbetriebnahme



1. Anschluss für Sensor
2. Netzwerkanschluss (RJ45)
3. Aktuelle Stromaufnahme (7-Segment Anzeige)
4. LED Indikator Overvoltage Protection (rot - inaktiv)
5. LED Anzeige für externen Sensor
6. 4 Klartextanzeigen (on/off) über den Zustand der Power-Ports
7. Status LED
8. Taster für OK
9. Taster für Select



Power-Ports 1 bis 4

## Inbetriebnahme

- Verbinden Sie das Stromkabel des Geräts mit dem Stromnetz.
- Stecken Sie das Netzkabel in die Ethernetbuchse (RJ45).
- Stecken Sie den optionalen externen Sensor in den Sensoranschluss.

### 1.5.Überspannungsschutz

Das Gerät verfügt über einen Überspannungsschutz (Overvoltage Protection). Dieser basiert auf eingangsseitigen Varistoren mit thermischer Sicherung zwischen Phase (L) und Neutralleiter (N) zum Schutz der internen Elektronik und der Power-Ports mit Ausfallerkennung (thermische Sicherung dauerhaft ausgelöst). Der Zustand des Schutzes wird an der Frontblende durch einen roten Blitz signalisiert. Ist der Blitz nicht sichtbar, bedeutet dies, dass der Schutz betriebsbereit ist, ein roter Blitz symbolisiert, dass das Überspannungsschutzmodul außer Funktion ist. Zusätzlich ist der Status des Überspannungsschutzes über das Webinterface (HTTP) und SNMP zu ermitteln. Das Überspannungsschutzmodul ist so ausgelegt, dass es in normalen Installationsumgebungen eine praktisch unbegrenzte Anzahl von Überspannungspulsen ableiten kann. In einer Umgebung mit vielen energiereichen Überspannungspulsen kann es durch Alterung des Überspannungsschutzelementes zu einem dauerhaften Ausfall der Funktion kommen.



Eine Wiederherstellung der Überspannungsschutzfunktion kann nur durch den Hersteller des Gerätes erfolgen. Im Normalfall wird das Gerät auch nach dem Ausfall der Schutzfunktion weiterarbeiten.



Eine Signalisierung mittels E-Mail, Syslog oder SNMP Trap erfolgt im laufenden Betrieb nur ein einziges Mal, und zwar genau in dem Moment, in dem der Schutz versagt. Zusätzlich wird beim Einschalten des Gerätes eine Nachricht erzeugt, sollte der Überspannungsschutz nicht betriebsbereit sein.

### 1.6.Status LED

Die Status-LED zeigt Ihnen 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, die TCP/IP Einstellungen wurden vorgenommen.
- regelmäßig blinkend: Das Gerät befindet sich im Bootloader-Modus.

### 1.7.Bootloader-Modus

#### Aktivierung des Bootloader Modus

per Taster:

- Halten Sie beide Taster für 3 Sekunden gedrückt


oder

- Entfernen Sie die Betriebsspannung
- Halten Sie den "Select" Taster gedrückt.
- Verbinden Sie die Betriebsspannung

per Webinterface:

- Drücken Sie "Enter Bootloader Mode" auf der [Maintenance](#) Webseite

Ob sich das Gerät im Bootloader-Modus befindet, erkennen Sie am Blinken der Status LED.

 Eine Aktivierung des Bootloader Modus sowie ein Verlassen des Bootloaders verändert nicht den Zustand der Power-Ports, solange die Betriebsspannung erhalten bleibt.

## Verlassen des Bootloader Modus

per Taster:


- Halten Sie beide Taster für 3 Sekunden gedrückt

oder

- Entfernen und verbinden Sie die Betriebsspannung ohne einen Taster zu betätigen

## Werkszustand

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

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

per Taster:

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

per Webinterface:

- Drücken Sie "Restore Fab Settings and Restart Device" auf der Maintenance Webseite

## 1.8.Firmware-Update


Ein Firmware-Update kann folgendermaßen über das Webinterface durchgeführt werden:

per Webinterface:

- Selektieren Sie mit "Browse" auf der [Maintenance](#) Webseite die gewünschte Firmware Datei, und drücken Sie "Upload".

Ein Firmware-Update wird im Gegensatz zu anderen Funktionen nicht als Netzwerk Broadcast geschickt. Deshalb muss vor einem Firmware-Update das Gerät eine gültige IP-Adresse und eine gültige Netzmaske haben.



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

## 1.9. Technische Daten

Anschlüsse	<p>1 x Ethernetanschluss (RJ45)</p> <p>1 x Netzanschluss (SchukoStecker, max. 16A), Länge ca. 2m</p> <p>4 x Lastausgänge (SchukoSteckdose, max. 16 A)</p> <p>1 x Mini-DIN für externen Sensor</p>
Netzwerkanbindung	10/100 MBit/s 10baseT Ethernet
Protokolle	TCP/IP, HTTP/HTTPS, SNMP v1/v2c/v3, SNMP traps, Syslog, E-Mail (SMTP)
Spannungsversorgung	internes Netzteil (230V AC / -15% / +10%)
Überspannungsschutz <ul style="list-style-type: none"> <li>• Maximale Betriebsspannung</li> <li>• einmal. Spitzenstrom für 20/80us Puls</li> <li>• Max. Begrenzungsspannung 20/80us Puls, I<sub>pk</sub>=100A</li> </ul>	Varistor 20 mm/190J Scheibe  300 VACrms  10000 A  710 V
Umgebung <ul style="list-style-type: none"> <li>• Betriebstemperatur</li> <li>• Lagertemperatur</li> <li>• Luftfeuchtigkeit</li> </ul>	0 °C - 50 °C -20 °C - 70 °C 0% - 95% (nicht kondensierend)
Gehäuse	Kunststoff
Maße	484mm x 46mm x 74mm (L x H x B)
Gewicht	ca. 1050 g

### 1.9.1. Elektrische Meßgrößen

<b>Elektrische Messgrößen</b>				
<b>Messwert</b>	<b>Bereich</b>	<b>Einheit</b>	<b>Auflösung</b>	<b>Ungenauigkeit (typisch)</b>
Spannung (voltage)	110-265	V	0,01	< 1%
Strom (current)	0,1 - 16	A	0,001	< 1,5%
Frequenz (frequency)	45-65	Hz	0,01	< 0,03%
Phasenwinkel (phase)	-180 - +180	°	0,1	< 1%
Wirkleistung (active power)	1 - 4000	W	1	< 1,5%
Blindleistung (reactive power)	1 - 4000	Var	1	< 1,5%
Scheinleistung (apparent power)	1 - 4000	VA	1	< 1,5%
Powerfaktor (PF)	0 - 1	-	0,01	< 3%
<b>Energiezähler</b>				
Wirkenergie (total)	9.999.999,999	kWh	0,001	< 1,5%
Wirkenergie (temp)	9.999.999,999	kWh	0,001	< 1,5%

## 1.10. Sensoren

An der **MultiBox-pro LAN+** kann ein externer Sensor angeschlossen werden. Aktuell sind folgende Sensoren verfügbar



Temperatursensor 7001	
Kabellänge	≈ 2m
Anschluss	Mini-DIN
Temperaturbereich	-20°C bis +80°C bei ±2°C (maximal) und ±1°C (typisch)



Feuchte/Tempsensor 7002	
Kabellänge	≈ 2m
Anschluss	Mini-DIN
Messbereich	Temp: -20 bis +80°C, ±0,5°C (maximal) und ±0,3°C (typisch) Feuchte: 0-100%, ±3% (maximal) und ±2% (typisch)

Die Sensoren werden nach dem Anschließen automatisch erkannt. Die grüne "S1" LED auf der Vorderseite leuchtet dann dauerhaft. Auf der "Control Panel" Webseite werden die Sensorwerte direkt angezeigt:

Port	Name	Temperature	24h min	24h max	
1: 7002	Temperature	26,3 °C	24,4 °C	26,3 °C	<input type="button" value="Reset min/max"/>

Port	Name	Humidity	24h min	24h max	
1: 7002	Humidity	32,3 %	31,3 %	33,6 %	<input type="button" value="Reset min/max"/>

## 2. Bedienung

### 2.1. Bedienung am Gerät

#### Schalten

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

#### Anzeige Informationen

Ist kein Port manuell selektiert, werden durch wiederholtes Drücken des "Ok" Tasters nacheinander die IP-Adresse und die Werte der externen Sensoren im Display (7-Segment Anzeige) dargestellt.

### 2.2. Control Panel

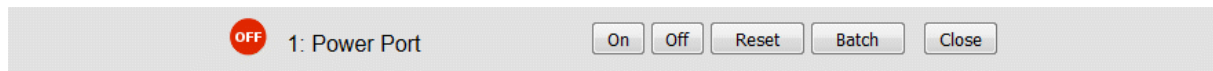
Rufen Sie das Webinterface unter <http://IP-Adresse> auf und loggen Sie sich ein.

The screenshot shows the 'Control Panel' web interface. At the top, there are navigation tabs: 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. Below the tabs, there are four power port status indicators, each with a red 'OFF' button and a label: '1: Power Port', '2: Power Port', '3: Power Port', and '4: Power Port'. Below these is a status indicator 'OVP operational'. A detailed view for '1: Power Port' is shown, featuring a red 'OFF' button, an 'On' button, an 'Off' button, and 'Reset', 'Batch', and 'Close' buttons. Below this is a table with the following data:

Line Id	Name	Voltage AC rms	Current AC rms	Freq	Phase	Power				total Energy	resettable Energy	
		V	A	Hz	°	active W	reactive VAR	apparent VA	PF	active kWh	active kWh	time h:m:s
I1	Meter1	224,4	0,000	50,00	-56,0	0	0	0	0,44	0,000	0,000	00:22:59

Below the table, there is a checkbox labeled 'show details' which is checked. At the bottom, it says 'auto logout in 293s'.

Die Webseite bietet einen Überblick über den Schaltzustand, und zeigt die Strom-Messwerte an. Sowie die Sensoren, sofern sie angeschlossen sind. Klickt man auf einen einzelnen Port, dann erscheinen die Schaltflächen, um den Port zu kontrollieren:



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



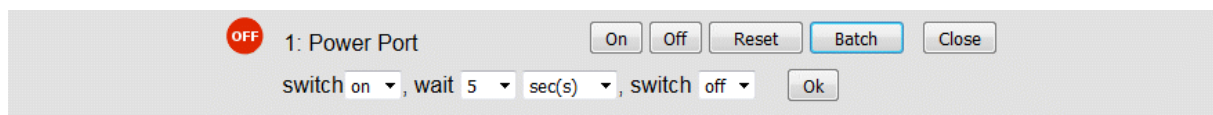
Ein aktivierter Watchdog wird durch ein Augensymbol dargestellt. Ein "X" bedeutet, dass die zu überwachende Adresse nicht aufgelöst werden konnte. Zwei kreisförmige Pfeile zeigen den Zustand Booting an.



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

## Batchmode

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



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

## 2.3.Maintenance Funktionen

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


The screenshot shows the 'Maintenance' section of the web interface. At the top, there are four tabs: 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. Below the tabs, there are three main sections:

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

Firmware Update: Führt ein Firmware-Update durch.

SSL Certificate Upload: Speichert ein eigenes SSL Zertifikat ab. Siehe das Kapitel "[SSL](#)" für die Generierung eines Zertifikats im richtigen Format.

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.

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

## 3. Konfiguration

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 dem sorgfältigen Umgang mit den erzeugten Konfigurationsdateien zu raten.

### Anpassung der Konfigurationsdatei

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

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

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

Der Befehl "system fabsettings" vom Anfang einer erzeugten Konfigurationsdatei bringt das Gerät in den Werkszustand, und führt dann die einzelnen Befehle aus, die Konfigurationsparameter verändern. Es kann gewünscht sein, die Änderungen relativ zur aktuellen Konfiguration durchzuführen, und nicht ausgehend vom Werkszustand. Dann sollte das "system fabsettings" entfernt werden.

## 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:

1. Funktion deaktivieren
2. vollständig parametrisieren
3. 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
```

## 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 nutzen Sie die Konfiguration über das Webinterface.

### 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.



### 3.1.1. Power-Ports

Control Panel Configuration Maintenance Logout

[Power Ports](#) · [IP Address](#) · [IP ACL](#) · [HTTP](#) · [Console](#) · [Sensors](#) · [SNMP](#) · [Syslog](#) · [E-Mail](#)

**Power Ports**

- Choose Power Port to configure: A1: Power Port
- Label: Power Port
- Connect twin port:  yes  no
- Initialization status (coldstart):  on  off  remember last state
- Initialization status (bank repower):  apply *Initialization status*  remain in current state
- Initialization delay: 0 s
- Repower delay: 0 s
- Reset duration: 10 s
- Enable watchdog:  yes  no

Apply

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

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

## Einschaltüberwachung

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

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

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

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

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

Enable watchdog: Aktiviert die Watchdog Funktion für diesen Power-Port.

### 3.1.2. Watchdog

The screenshot shows a web-based configuration interface for a power port. At the top, there are tabs for 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. Below these, there are navigation links: 'Power Ports', 'IP Address', 'IP ACL', 'HTTP', 'Console', 'Sensors', 'SNMP', 'Syslog', and 'E-Mail'. The main section is titled 'Power Ports' and contains the following settings:

- Choose Power Port to configure: A1: Power Port (dropdown menu)
- Label: Power Port (text input)
- Connect twin port:  yes  no
- Initialization status (coldstart):  on  off  remember last state
- Initialization status (bank repower):  apply Initialization status  remain in current state
- Initialization delay: 0 s (text input)
- Repower delay: 0 s (text input)
- Reset duration: 10 s (text input)
- Enable watchdog:  yes  no
  - Watchdog action:  reset  off
  - Watchdog type:  ICMP  TCP
  - Hostname: (text input)
  - Ping interval: 10 s (text input)
  - Ping retries: 6 (text input)
  - retry BOOTING after RESET failure:  no  yes

An 'Apply' button is located at the bottom of the configuration area.

Mit der Watchdog Funktion können verschiedene Endgeräte überwacht werden. Dafür werden entweder ICMP-Pings oder TCP-Pings an das zu überwachende Gerät geschickt. Werden diese Pings innerhalb einer bestimmten Zeit (sowohl die Zeit, als auch die Anzahl der Versuche sind einstellbar) nicht beantwortet, wird der Power-Port zurückgesetzt. Dadurch können z.B. nicht antwortende Server oder NAS Systeme automatisiert neu gestartet werden.

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

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

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

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

Enable watchdog: Aktiviert die Watchdog Funktion für diesen Power-Port.

Watchdog action: Bei der Einstellung *reset* wird der Power-Port ausgeschaltet, und nach der in der Reset Duration eingestellten Zeit wieder eingeschaltet. Bei "off" bleibt der Power-Port deaktiviert.

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

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

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

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

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

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

retry BOOTING after RESET failure:

Im Auslieferungszustand (nicht aktiviert) überwacht der Watchdog das angeschlossene Gerät. Antwortet dieses nach einer eingestellten Zeit nicht mehr, führt der Watchdog die eingestellte Aktion durch, i.R. einen Reset des Power-Ports. Jetzt wartet der Watchdog bis sich das überwachte Gerät wieder am Netz meldet. Dies kann je nach Bootdauer des überwachten Gerätes mehrere Minuten dauern. Erst wenn dieses Gerät im Netz wieder erreichbar ist wird der Watchdog neu scharf gestellt. Aktivieren Sie diese Option, wird dieser Mechanismus überbrückt. Jetzt wird der Watchdog nach der eingestellten Ping Zeit automatisch wieder scharf geschaltet.

retry Boot after N ping timeouts: Ist retry BOOTING after RESET failure aktiviert, dann wird N Ping Intervalle gewartet, bis bei einer ausbleibenden Antwort der Output Port aus- und wieder eingeschaltet wird.

• Enable watchdog:  yes  no

• Watchdog action:  reset  off

• Watchdog type:  ICMP  TCP

• Hostname:

• Ping interval:  s

• Ping retries:

• retry BOOTING after RESET failure:  no  yes

• retry Boot after N ping timeouts:

Apply

### 3.1.3.IP Address

Control Panel
Configuration
Maintenance
Logout

[Power Ports](#) · [IP Address](#) · [IP ACL](#) · [HTTP](#) · [Console](#) · [Sensors](#) · [SNMP](#) · [Syslog](#) · [E-Mail](#)

**Hostname**

• Hostname:

**IPv4**

• IPv4 Address:

• IPv4 Netmask:

• IPv4 Gateway address:

• IPv4 DNS address:

• Use IPv4 DHCP:  yes  no

**IPv6**

• Use IPv6 Protocol:  yes  no

• Use IPv6 Router Advertisement:  yes  no

• Use DHCP v6:  yes  no

• Use manual IPv6 address settings:  yes  no

**IPv6 status**

• Current IPv6 status:

```
IPv6 Addr:
fe80::219:32ff:fe00:996d
2007:7dd0:ffc1:0:219:32ff:fe00:996d

IPv6 DNS Server:
2007:7dd0:ffc1:0:20c:29ff:feaf:93c

IPv6 Router:
fe80::20c:29ff:feaf:93c
```

Hostname: Hier kann ein Name mit maximal 15 Zeichen vergeben werden. Mit diesem Namen erfolgt die Anmeldung beim DHCP-Server.



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

IP V4 Address: Die IP-Adresse des Gerätes.

IPv4 Netmask: Die Netzmaske im verwendeten Netz.

IPv4 Gateway address: IP-Adresse des Gateway.

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

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


Use IPv6 Protocol: Aktiviert das IPv6-Protokoll.

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

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

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

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

 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.

**IPv6 (manual)**

- IPv6 Addresses:
 

2007:7dd0:ffc1:0:219:32ff:fe00:996d	/64
	/64
	/64
	/64
  
- IPv6 DNS addresses:
 

2007:7dd0:ffc1:0:20c:29ff:feaf:93c	
  
- IPv6 Gateway address:
 

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

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

### 3.1.4. IP ACL

Control Panel
Configuration
Maintenance
Logout

[Power Ports](#) · [IP Address](#) · [IP ACL](#) · [HTTP](#) · [Console](#) · [Sensors](#) · [SNMP](#) · [Syslog](#) · [E-Mail](#)

**ICMP Ping**

• Reply ICMP ping requests:  yes  no

**IP Access Control List**


• Enable IP filter:  yes  no

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

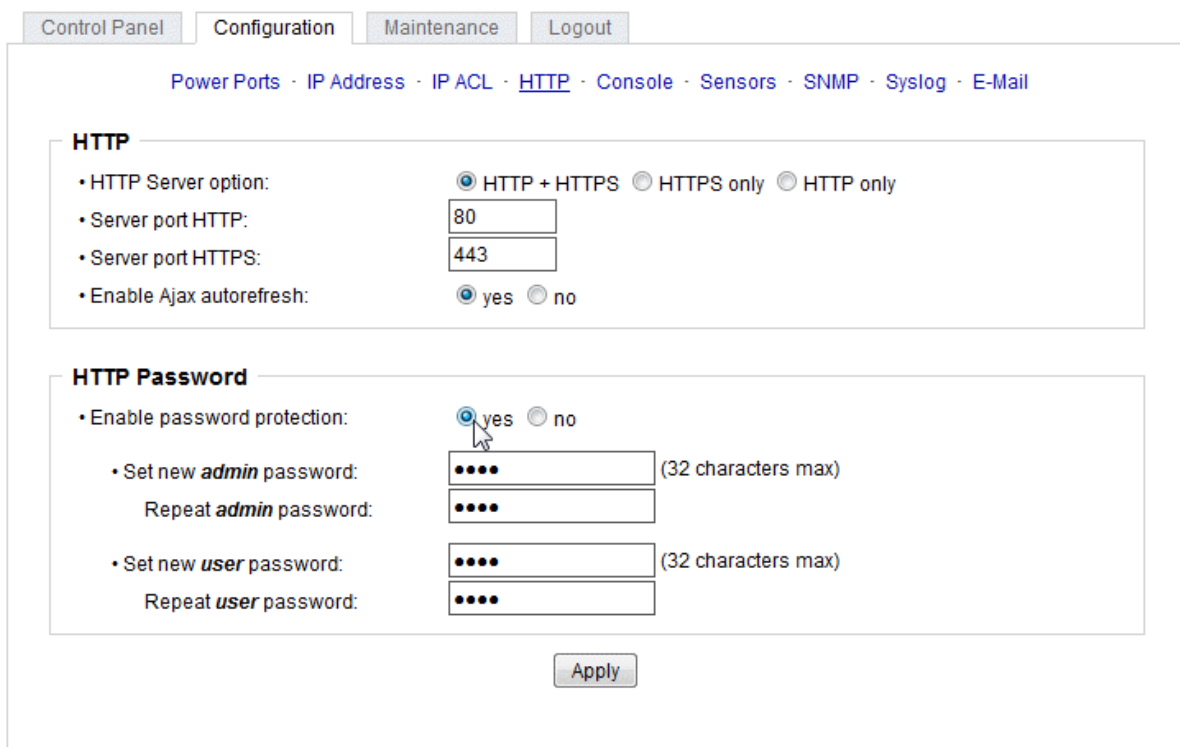
Reply ICMP ping requests: Wenn Sie diese Funktion aktivieren, antwortet das Gerät auf ICMP Pings aus dem Netzwerk.

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 setzen Sie das Gerät in den Werkszustand zurück.

### 3.1.5.HTTP



Control Panel Configuration Maintenance Logout

Power Ports · IP Address · IP ACL · HTTP · Console · Sensors · SNMP · Syslog · E-Mail

**HTTP**

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

**HTTP Password**

- Enable password protection:  yes  no
- Set new **admin** password:  (32 characters max)
- Repeat **admin** password:
- Set new **user** password:  (32 characters max)
- Repeat **user** password:


Apply

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


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

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

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

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

**Enable password protection:** Auf Wunsch kann der Passwort-Zugangsschutz aktiviert werden. In diesem Fall müssen ein Admin-Passwort und ein User-Passwort vergeben werden. Das Passwort darf maximal 31 Zeichen besitzen. 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 Änderungen am Gerät vorzunehmen. In der Passwordeingabemaske des Browsers sind für den Usernamen "admin" und "user" vorgesehen. Im Werkzustand ist als Default das Passwort für den Admin auf "admin" gesetzt, bzw. "user" für das User Passwort.

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

### 3.1.6.Console

Control Panel
Configuration
Maintenance
Logout

Power Ports
IP Address
IP ACL
HTTP
Console
Sensors
SNMP
Syslog
E-Mail

**Telnet Console**

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

**Serial console**

- Enable serial console:  yes  no
- Raw mode:  yes  no
- Activate echo:  yes  no
- Enable binary KVM protocol:  yes  no
- Require user login:  yes  no
  - Delay after 3 failed logins:  yes  no
- Username:
- Set new password:  (32 characters max)
- Repeat password:

**Enable Telnet:** Aktiviert die Telnet Konsole.

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

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

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

Active negotiation: Die IAC Aushandlung wird vom Server initiiert.

Require user login: Es werden Username und Passwort verlangt.

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

### 3.1.7.Sensors

Control Panel
Configuration
Maintenance
Logout

[Power Ports](#) · [IP Address](#) · [IP ACL](#) · [HTTP](#) · [Console](#) · [Sensors](#) · [SNMP](#) · [Syslog](#) · [E-Mail](#)

#### Internal Sensors

- Choose power meter:
- Power meter name:
- Generate AC current messages:  yes  no
  - Maximum value:  A
  - Minimum value:  A
  - Hysteresis:  A

#### External Sensors

- Choose sensor port:
- Sensor name:
- Generate messages:  yes  no
  - Maximum value:  °C
  - Minimum value:  °C
  - Hysteresis:  °C

#### Misc sensor options

- Min/Max measurement period:
- Default display:
- Enable beeper for AC alarms:  yes  no
- Enable beeper for sensor alarms:  yes  no

Choose power meter: Selektiert den Messkanal (nur einer bei der **MultiBox-pro LAN+**).

Power meter name: Der konfigurierbare Name, der auf der Übersichtsseite unter "Line Name" angezeigt wird.

Generate AC current messages: Schaltet die Überwachung von Strom-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.



Choose sensor port: 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 (z.B. 7002 für den Hybridsensor), ein Buchstabe für den Sensor-Untertyp und der einstellbare Sensorname. Als Sensor-Untertypen sind definiert: "T" = Temperatur, "H" = Luftfeuchtigkeit, "I" = Sensoreingang.

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.

Generate messages: Schaltet die Überwachung von Sensor-Grenzwerten ein.

Maximum/Minimum value: Einstellbare Grenzwerte, bei denen Meldungen per SNMP-Trap, Syslog oder E-Mail versendet werden sollen.

Hysteresis: Legt den Abstand fest, der nach einem Überschreiten eines Grenzwertes eines externen Sensors überschritten werden muss, um das Unterschreiten des Grenzwertes zu signalisieren.

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

Default Display: Wählt aus ob der Strom im LED-Display gezeigt wird (Current), oder der Wert eines Sensors.

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

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

## Hysterese Beispiel

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

### Beispiel:

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

...

49,1 °C - unterhalb der oberen Grenze, aber im Hysteresebereich  
49,0 °C - unterhalb der oberen Grenze, aber im Hysteresebereich  
48,9 °C - eine Meldung für das Überschreiten der oberen Grenze inklusive Hysteresebereich wird erzeugt

### 3.1.8.SNMP

Control Panel
Configuration
Maintenance
Logout

[Power Ports](#) · [IP Address](#) · [IP ACL](#) · [HTTP](#) · [Console](#) · [Sensors](#) · [SNMP](#) · [Syslog](#) · [E-Mail](#)

**SNMP**

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

**SNMP v2**

- Enable SNMP v2:  yes  no
- SNMP v2 public Community:  (16 char. max)
- SNMP v2 private Community:  (16 char. max)

**SNMP v3**

- Enable SNMP v3:  yes  no
- SNMP v3 Username:  (32 char. max)
- SNMP v3 Authorization Algorithm: 
  - Set new **Authorization** password:  (8 char. min, 32 char. max)
  - Repeat **Authorization** password:
- SNMP v3 Privacy Algorithm: 
  - Set new **Privacy** password:  (8 char. min, 32 char. max)
  - Repeat **Privacy** password:

**SNMP Traps**

- send SNMP Traps
- SNMP trap receiver 1 :


[MIB table](#)

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

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

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

Enable SNMP v2: Aktiviert SNMP v2.

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

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

SNMP v2 private Community: Das Passwort für die SNMP-set Arbeitsgruppe.

Enable SNMP v3: Aktiviert SNMP v3.

SNMP v3 Username: Der SNMP v3 Benutzername.

SNMP v3 Authorization Algorithm: Der ausgewählte Authentifizierungs Algorithmus.

SNMP v3 Privacy Algorithm: Die SNMP v3 Verschlüsselung.

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

**!** Die Berechnung der Passwort-Hashes ändert sich mit den eingestellten Algorithmen. Werden die Authentication oder Privacy Algorithmen geändert, müssen im Konfigurationsdialog die Passwörter wieder neu eingegeben werden. SHA-384" und "SHA-512" werden rein in Software berechnet. Wird auf der Konfigurationsseite "SHA-512" eingestellt, können einmalig bis zu ca. 45 Sekunden für die Schlüsselerzeugung vergehen.

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

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

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

### 3.1.9.Syslog

The screenshot shows a web interface with a navigation bar at the top containing 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. Below this is a breadcrumb trail: 'Power Ports · IP Address · IP ACL · HTTP · Console · Sensors · SNMP · Syslog · E-Mail'. The main content area is titled 'Syslog' and contains two configuration items: 'Enable Syslog:' with radio buttons for 'yes' (selected) and 'no', and 'Syslog server:' with an empty text input field. An 'Apply' button is located at the bottom center of the configuration area.

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.

### 3.1.10.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.

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): Authentifizierung des E-Mailservers.

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

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

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



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

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

## 4. Spezifikationen

### 4.1. IP ACL

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

Beispiele:

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



Sollten Sie sich hier aus Versehen „ausgesperrt“ haben, aktivieren Sie den Bootloader-Modus und setzen Sie das Gerät in den Werkszustand zurück.

### 4.2. IPv6

#### IPv6 Adressen

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

#### Adressnotation

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

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

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

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

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

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

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

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

## 4.3.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-Sniffen 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. Wird auf der Konfigurationsseite "SHA-512" eingestellt, können einmalig bis zu ca. 45 Sekunden für die Schlüsselerzeugung vergehen.

## Verschlüsselung

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

 Während bei der Einstellung "AES-192" und "AES-256" die Schlüssel nach "draft-blumenthal-aes-usm-04" berechnet werden, benutzen die Verfahren "AES-192-3DESKey" und "AES-256-3DESKey" eine Art der Schlüsselerzeugung, die auch beim "3DES" ("draft-reeder-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 "HMAC-SHA-96" mit "AES-128" als Authentifizierung und Verschlüsselung.

## NET-SNMP

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

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

bzw.

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

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

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

### NET-SNMP Beispiele

Power-Port 1 Schaltzustand abfragen:

```
snmpget -v2c -mALL -c public 192.168.1.232 epc1202PortState.1
```

Power-Port 1 einschalten:

```
snmpset -v2c -mALL -c private 192.168.1.232 epc1202PortState.1 integer 1
```

### 4.3.1. Geräte MIB

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" aus Platzgründen bei jedem Eintrag in der Tabelle weggelassen. Die komplette OID würde daher z.B. "1.3.6.1.4.1.28507.43.1.1.1.1" 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	OID	Type	Acc.
epc1202TrapCtrl	.43.1.1.1.1.0	Integer32	RW
0 = off 1 = Ver. 1 2 = Ver. 2c 3 = Ver. 3			
epc1202TrapIPIndex	.43.1.1.1.2.1.1.x	Integer32	RO
A unique value, greater than zero, for each receiver slot.			
epc1202TrapAddr	.43.1.1.1.2.1.2.x	OCTETS	RW
DNS name or IP address specifying one Trap receiver slot. A port can optionally be specified: 'name:port' An empty string disables this slot.			
epc1202portNumber	.43.1.3.1.1.0	Integer32	RO
The number of Relay Ports			
epc1202PortIndex	.43.1.3.1.2.1.1.x	Integer32	RO
A unique value, greater than zero, for each Relay Port.			
epc1202PortName	.43.1.3.1.2.1.2.x	OCTETS	RO
A textual string containing name of a Relay Port.			
epc1202PortState	.43.1.3.1.2.1.3.x	INTEGER	RW
current state a Relay Port			
epc1202PortSwitchCount	.43.1.3.1.2.1.4.x	Integer32	RO
The total number of switch actions occurred on a Relay Port. Does not count switch commands which will not switch the relay state, so just real relay switches are displayed here.			
epc1202PortStartupMode	.43.1.3.1.2.1.5.x	INTEGER	RW
set Mode of startup sequence (off, on , remember last state)			
epc1202PortStartupDelay	.43.1.3.1.2.1.6.x	Integer32	RW



Delay in sec for startup action			
epc1202PortRepowerTime	.43.1.3.1.2.1.7.x	Integer32	RW
Delay in sec for rePower-Port after switching off			
epc1202ActivePowerChan	.43.1.5.1.1.0	Unsigned32	RO
Number of supported Power Channels.			
epc1202PowerIndex	.43.1.5.1.2.1.1.x	Integer32	RO
Index of Power Channel entries			
epc1202ChanStatus	.43.1.5.1.2.1.2.x	Integer32	RO
0 = data not active, 1 = data valid			
epc1202AbsEnergyActive	.43.1.5.1.2.1.3.x	Gauge32	RO
Absolute Active Energy counter.			
epc1202PowerActive	.43.1.5.1.2.1.4.x	Integer32	RO
Active Power			
epc1202Current	.43.1.5.1.2.1.5.x	Gauge32	RO
Actual Current on Power Channel.			
epc1202Voltage	.43.1.5.1.2.1.6.x	Gauge32	RO
Actual Voltage on Power Channel			
epc1202Frequency	.43.1.5.1.2.1.7.x	Gauge32	RO
Frequency of Power Channel			
epc1202PowerFactor	.43.1.5.1.2.1.8.x	Integer32	RO
Power Factor of Channel between -1.0 and 1.00			
epc1202Pangle	.43.1.5.1.2.1.9.x	Integer32	RO
Phase Angle between Voltage and L Line Current between -180.0 and 180.0			
epc1202PowerApparent	.43.1.5.1.2.1.10.x	Integer32	RO
L Line Mean Apparent Power			
epc1202PowerReactive	.43.1.5.1.2.1.11.x	Integer32	RO
L Line Mean Reactive Power			
epc1202AbsEnergyReactive	.43.1.5.1.2.1.12.x	Gauge32	RO
Absolute Reactive Energy counter.			
epc1202AbsEnergyActiveResettable	.43.1.5.1.2.1.13.x	Gauge32	RW
Resettable Absolute Active Energy counter. Writing '0' resets all resettable counter.			
epc1202AbsEnergyReactiveResettable	.43.1.5.1.2.1.14.x	Gauge32	RO
Resettable Absolute Reactive Energy counter.			
epc1202ResetTime	.43.1.5.1.2.1.15.x	Gauge32	RO
Time in seconds since last Energy Counter reset.			
epc1202ForwEnergyActive	.43.1.5.1.2.1.16.x	Gauge32	RO
Forward Active Energy counter.			
epc1202ForwEnergyReactive	.43.1.5.1.2.1.17.x	Gauge32	RO
Forward Reactive Energy counter.			
epc1202ForwEnergyActiveResettable	.43.1.5.1.2.1.18.x	Gauge32	RO
Resettable Forward Active Energy counter.			
epc1202ForwEnergyReactiveResettable	.43.1.5.1.2.1.19.x	Gauge32	RO
Resettable Forward Reactive Energy counter.			
epc1202RevEnergyActive	.43.1.5.1.2.1.20.x	Gauge32	RO
Reverse Active Energy counter.			
epc1202RevEnergyReactive	.43.1.5.1.2.1.21.x	Gauge32	RO
Reverse Reactive Energy counter.			
epc1202RevEnergyActiveResettable	.43.1.5.1.2.1.22.x	Gauge32	RO
Resettable Reverse Active Energy counter.			

epc1202RevEnergyReactiveResettable	.43.1.5.1.2.1.23.x	Gauge32	RO
Resettable Reverse Reactive Energy counter.			
epc1202OVPIIndex	.43.1.5.2.1.1.x	Integer32	RO
None			
epc1202OVPSStatus	.43.1.5.2.1.2.x	INTEGER	RO
shows the status of the built-in Overvoltage Protection			
epc1202SensorIndex	.43.1.6.1.1.1.x	Integer32	RO
None			
epc1202TempSensor	.43.1.6.1.1.2.x	Integer32	RO
actual temperature, a value of -9999 indicates that data is not available			
epc1202HygroSensor	.43.1.6.1.1.3.x	Integer32	RO
actual humidity, a value of -9999 indicates that data is not available			
epc1202InputSensor	.43.1.6.1.1.4.x	INTEGER	RO
logical state of input sensor			

## 4.4.SSL

### TLS Standard

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

Die folgenden TLS Ciphersuites werden unterstützt:

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

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

## Erstellen eigener Zertifikate

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

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

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

Hier einige Beispiele zur Generierung mit OpenSSL:

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

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

### RSA 2048-Bit Zertifikat mit Sign Request:

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



Die Server Keys sollten mit "openssl genrsa" erzeugt werden. Wenn in der erzeugten Schlüsseldatei nicht "-----BEGIN RSA PRIVATE KEY-----" sondern nur "-----BEGIN PRIVATE KEY-----" steht, wird der Schlüssel nicht erkannt.

### ECC Zertifikat mit Sign Request:

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

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


### Linux:

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

### Windows:

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

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

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

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

 Nach einem Zurücksetzen in den [Werkszustand](#) bleibt ein hochgeladenes Zertifikat erhalten.

## Performance Betrachtungen

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

## 4.5 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 zur Verfügung. 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, das 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 wird im Kapitel "Cmd Overview" gegeben.

## 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

## 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

Möchte man 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
link, rechts	bewegt Cursor nach links oder rechts
Pos1, Ende	setzt den Cursor auf Anfang oder Ende der Zeile
Entf	löscht Zeichen unter dem Cursor
Rück	löscht Zeichen links vom Cursor
rauf, runter	Zeigt ältere Eingabezeilen (History)
Tab, Strg-Tab	vervollständigt das Wort am Cursor
Strg-C	löscht die Zeile

Führt ein Verkleinern des Terminalfensters dazu, dass sich die Eingabezeile über mehrere Bildschirmzeilen erstreckt, so funktionieren die Editierfunktionen nicht zuverlässig.

### 4.5.1 Konsole Cmd 1202

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

console telnet echo show	shows if echo enabled
console telnet activeneg set {OFF=0 ON=1}	enables telnet active negotiation (IAC) on/off
console telnet activeneg show	shows if active negotiation enabled
console telnet login set {OFF=0 ON=1}	enables login on/off
console telnet login show	shows if login enabled
console telnet login delay set {OFF=0 ON=1}	enables delay (after 3 login fails) on/off
console telnet login delay show	shows if login delay enabled
console telnet user set "{username}"	sets login user name
console telnet user show	shows login user name
console telnet passwd set "{passwd}"	sets login password
console telnet passwd hash set "{passwd}"	sets login hashed password
<b>email</b>	
email	enters cmd group "email"
email enabled set {OFF=0 ON=1}	enables email on/off
email enabled show	shows if email is enabled
email sender set "{email_addr}"	sets email sender address
email sender show	shows email sender address
email recipient set "{email_addr}"	sets email recipient address
email recipient show	shows email recipient address
email server set "{dns_name}"	sets email SMTP server address
email server show	shows email SMTP server address
email port set {ip_port}	sets email SMTP port
email port show	shows email SMTP port
email security set {NONE=0 STARTTLS=1 SSL=2}	sets SMTP connection security
email security show	shows SMTP connection security
email auth set {NONE=0 PLAIN=1 LOGIN=2}	sets email authentication
email auth show	show email authentication
email user set "{username}"	sets SMTP username
email user show	shows SMTP username
email passwd set "{passwd}"	sets SMTP password
email passwd hash set "{passwd}"	sets crypted SMTP password
email testmail	send test email
<b>ethernet</b>	
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
<b>extsensor</b>	
extsensor	enters cmd group "extsensor"
extsensor {port_num} {TEMP=0 HYGRO=1} value show	shows sensor value
extsensor {port_num} {TEMP=0 HYGRO=1} label set "{name}"	sets sensor name to label
extsensor {port_num} {TEMP=0 HYGRO=1} label show	shows label of sensor
extsensor {port_num} name show	shows type of sensor
extsensor {port_num} {TEMP=0 HYGRO=1} events set {off=0 on=1}	enables sensor events on/off
extsensor {port_num} {TEMP=0 HYGRO=1} events show	shows if sensor events are enabled
extsensor {port_num} {TEMP=0 HYGRO=1} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SM S=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	enables different event types
extsensor {port_num} {TEMP=0 HYGRO=1} events type show	shows what event types are enabled
extsensor {port_num} {TEMP=0 HYGRO=1} maxval set {num}	sets maximum value for sensor
extsensor {port_num} {TEMP=0 HYGRO=1} maxval show	shows maximum value for sensor
extsensor {port_num} {TEMP=0 HYGRO=1} minval set {num}	sets minimum value for sensor
extsensor {port_num} {TEMP=0 HYGRO=1} minval show	shows minimum value for sensor
extsensor {port_num} {TEMP=0 HYGRO=1} hyst set {num}	sets hysteresis value for sensor
extsensor {port_num} {TEMP=0 HYGRO=1} hyst show	shows hysteresis value for sensor
extsensor {port_num} {TEMP=0 HYGRO=1} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port set {port_num}	sets Port for Power Port Switching actions

extsensor {port_num} {TEMP=0 HYGRO=1} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} port show	shows Port for Power Port Switching actions	
extsensor {port_num} {TEMP=0 HYGRO=1} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} state set {OFF=0 ON=1 DISABLED=2}	sets Port state for Power Port Switching actions	
extsensor {port_num} {TEMP=0 HYGRO=1} {BELOWMIN=0 ABOVEMIN=1 ABOVEMAX=2 BELOWMAX=3} state show	shows Port state for Power Port Switching actions	
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 display set {CURRENT=0 TEMP1=1 HYGRO1=2 TEMP2=3 HYGRO2=4}	sets default display	
extsensor display show	shows state of default display	
extsensor beeper set {OFF=0 ON=1}	enables beeper sensor alarms	
extsensor beeper show	shows if beeper sensor alarms are enabled	
<hr/>		
http	enters cmd group "http"	
http server set {HTTP_BOTH=0 HTTPS_ONLY=1 HTTP_ONLY=2}	sets connection types the webservice accepts	
http server show	shows webservice accepting connection types	
http port set {ip_port}	sets http port	
http port show	shows http port	
http portssl set {ip_port}	sets https port	
http portssl show	shows https port	
http ajax enabled set {OFF=0 ON=1}	enables ajax autorefresh on/off	
http ajax enabled show	shows if ajax autorefresh enabled	
http passwd enabled set {OFF=0 ON=1}	enables http password on/off	
http passwd enabled show	shows if http password enabled	
http passwd user set "{passwd}"	sets http user password	
http passwd admin set "{passwd}"	sets http admin password	
http passwd hash user set "{passwd}"	sets hashed http user password	
http passwd hash admin set "{passwd}"	sets hashed http admin password	
<hr/>		
ip4	enters cmd group "ip4"	
ip4 hostname set "{name}"	sets device hostname	
ip4 hostname show	shows device hostname	2
ip4 address set "{ip_address}"	sets IPv4 address	
ip4 address show	shows IPv4 address	2
ip4 netmask set "{ip_address}"	sets IPv4 netmask	
ip4 netmask show	shows IPv4 netmask	2
ip4 gateway set "{ip_address}"	sets IPv4 gateway address	
ip4 gateway show	shows IPv4 gateway address	2
ip4 dns set "{ip_address}"	sets IPv4 DNS server address	
ip4 dns show	shows IPv4 DNS server address	2
ip4 dhcp enabled set {OFF=0 ON=1}	enables IPv4 DHCP on/off	
ip4 dhcp enabled show	shows IPv4 DHCP state	2
<hr/>		
ip6	enters cmd group "ip6"	
ip6 enabled set {OFF=0 ON=1}	enables IPv6 on/off	
ip6 enabled show	shows if IPv6 is enabled	2
ip6 routadv enabled set {OFF=0 ON=1}	enables IPv6 router advertisement	
ip6 routadv enabled show	shows IPv6 router advertisement state	2
ip6 dhcp enabled set {OFF=0 ON=1}	enables IPv6 DHCP on/off	
ip6 dhcp enabled show	shows if IPv6 DHCP is enabled	2
ip6 address show	show all IPv6 addresses	3
ip6 gateway show	show all IPv6 gateways	3
ip6 dns show	show all IPv6 DNS server	3
ip6 manual enabled set {OFF=0 ON=1}	enables manual IPv6 addresses	
ip6 manual enabled show	shows if manual IPv6 addresses are enabled	2
ip6 manual address {1..4} set "{ip_address}"	sets manual IPv6 address	
ip6 manual address {1..4} show	shows manual IPv6 address	2
ip6 manual gateway set "{ip_address}"	sets manual IPv6 gateway address	
ip6 manual gateway show	shows manual IPv6 gateway address	2
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	2



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}
<hr/>	
linesensor	enters cmd group "linesensor"
linesensor {line_num} {energy_sensor} value show	shows energy sensor of given line 4
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} events set {OFF=0 ON=1}	enables events on/off
linesensor {line_num} events show	shows if events are enabled
linesensor {line_num} events type set "{EVT_SYSLOG=0,EVT_SNMP=1,EVT_EMAIL=2,EVT_SM S=3,EVT_GSMEMAIL=4,EVT_BEEPER=5}"	enables different event types
linesensor {line_num} events type show	shows what event types are enabled
linesensor {line_num} maxval set {float}	sets maximum value for line meter
linesensor {line_num} maxval show	shows maximum value for line meter
linesensor {line_num} minval set {float}	sets minimum value for line meter
linesensor {line_num} minval show	shows minimum value for line meter
linesensor {line_num} hyst set {float}	sets hysteresis value for line meter
linesensor {line_num} hyst show	shows hysteresis value for line meter
linesensor {line_num} {BELOWMIN=0 ABOVEMIN=1  ABOVMAX=2 BELOWMAX=3} port set {port_num}	sets Port for Power Port Switching actions
linesensor {line_num} {BELOWMIN=0 ABOVEMIN=1  ABOVMAX=2 BELOWMAX=3} port show	shows Port for Power Port Switching actions
linesensor {line_num} {BELOWMIN=0 ABOVEMIN=1  ABOVMAX=2 BELOWMAX=3} state set {OFF=0 ON=1  DISABLED=2}	sets Port state for Power Port Switching actions
linesensor {line_num} {BELOWMIN=0 ABOVEMIN=1  ABOVMAX=2 BELOWMAX=3} state show	shows Port state for Power Port Switching actions
linesensor beeper set {OFF=0 ON=1}	enables beeper for line meter alarms
linesensor beeper show	shows if beeper for line meter alarms is enabled
<hr/>	
port	enters cmd group "port"
port {port_num} state set {OFF=0 ON=1}	sets port to new state
port {port_num} state show	shows port state
port {port_num} reset	start reset sequence for port
port {port_num} toggle	toggles port
port {port_num} batch set {OFF=0 ON=1} wait {num_secs} {OFF=0 ON=1}	starts batch mode for port
port {port_num} batch cancel	cancels batch mode
port {port_num} label set "{name}"	sets port label name
port {port_num} label show	shows port label name
port {port_num} initstate coldstart set {OFF=0 ON=1  REMEMBER=2}	sets port coldstart initialization
port {port_num} initstate coldstart show	shows port coldstart initialization
port {port_num} initstate delay set {num}	sets port init delay
port {port_num} initstate delay show	shows port init delay
port {port_num} repowerdelay set {num}	sets port repower delay
port {port_num} repowerdelay show	shows port repower delay
port {port_num} resettime set {num}	sets port reset duration
port {port_num} resettime show	shows port reset duration
port {port_num} watchdog enabled set {OFF=0 ON=1}	sets port watchdog to on/off
port {port_num} watchdog enabled show	shows port watchdog state
port {port_num} watchdog mode set {OFF=0  PORT_RESET=1 IP_MS=2 IP_MS_INV=3}	sets port watchdog mode
port {port_num} watchdog mode show	shows port watchdog mode
port {port_num} watchdog type set {WD_ICMP=0  WD_TCP=1}	sets port watchdog type
port {port_num} watchdog type show	shows port watchdog type
port {port_num} watchdog host set "{dns_name}"	sets port watchdog host target
port {port_num} watchdog host show	shows port watchdog host target

port {port_num} watchdog port set {ip_port}	sets port watchdog TCP port
port {port_num} watchdog port show	shows port watchdog TCP port
port {port_num} watchdog pinginterval set {num}	sets port watchdog ping interval
port {port_num} watchdog pinginterval show	shows port watchdog ping interval
port {port_num} watchdog pingretries set {num}	sets port watchdog ping retries
port {port_num} watchdog pingretries show	shows port watchdog ping retries
port {port_num} watchdog retrybooting set {OFF=0 ON=1}	sets port watchdog retry booting to on/off
port {port_num} watchdog retrybooting show	shows port watchdog retry booting state
port {port_num} watchdog bootretries set {num}	sets port watchdog retry boot timeout
port {port_num} watchdog bootretries show	shows port watchdog retry boot timeout
snmp	enters cmd group "snmp"
snmp port set {ip_port}	sets SNMP UDP port
snmp port show	shows SNMP UDP port
snmp snmpget enabled set {OFF=0 ON=1}	enables SNMP GET cmds on/off
snmp snmpget enabled show	show if SNMP GET cmds are enabled
snmp snmpset enabled set {OFF=0 ON=1}	enables SNMP SET cmds on/off
snmp snmpset enabled show	show if SNMP SET cmds are enabled
snmp snmpv2 enabled set {OFF=0 ON=1}	enables SNMP v2 on/off
snmp snmpv2 enabled show	show if SNMP v2 is enabled
snmp snmpv2 public set "{text}"	enables SNMP v3 on/off
snmp snmpv2 public show	show if SNMP v3 is enabled
snmp snmpv2 private set "{text}"	sets SNMP v2 public community
snmp snmpv2 private show	shows SNMP v2 public community
snmp snmpv3 enabled set {OFF=0 ON=1}	sets SNMP v2 private community
snmp snmpv3 enabled show	shows SNMP v2 private community
snmp snmpv3 username set "{text}"	sets SNMP v3 username
snmp snmpv3 username show	shows SNMP v3 username
snmp snmpv3 authalg set {NONE=0 MD5=1 SHA1=2 SHA256=3 SHA384=4 SHA512=5}	sets SNMP v3 authentication
snmp snmpv3 authalg show	show SNMP v3 authentication algorithm
snmp snmpv3 privalg set {NONE=0 DES=1 3DES=2 AES128=3 AES192=4 AES256=5 AES192*=6 AES256*=7}	sets SNMP v3 privacy algorithm
snmp snmpv3 privalg show	show SNMP v3 privacy algorithm
snmp snmpv3 authpasswd set "{passwd}"	sets SNMP v3 authentication password
snmp snmpv3 privpasswd set "{passwd}"	sets SNMP v3 privacy password
snmp snmpv3 authpasswd hash set "{passwd}"	sets SNMP v3 authentication hashed password
snmp snmpv3 privpasswd hash set "{passwd}"	sets SNMP v3 privacy hashed password
snmp trap type set {NONE=0 V1=1 V2=2 V3=3}	sets type of SNMP traps
snmp trap type show	show SNMP trap type
snmp trap receiver {trap_num} set "{dns_name}"	sets address and port of SNMP trap receiver {trap_num}
snmp trap receiver {trap_num} show	show address and port of SNMP trap receiver {trap_num}
syslog	enters cmd group "syslog"
syslog enabled set {OFF=0 ON=1}	enables syslog msgs on/off
syslog enabled show	show if syslog enabled
syslog server set "{dns_name}"	sets address of syslog server
syslog server show	shows address of syslog server
system	enters cmd group "system"
system restart	restarts device
system fabsettings	restore fab settings and restart device
system bootloader	enters bootloader mode
system flushdns	flush DNS cache
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. Befehl kann auf allen Ebenen ausgeführt werden
2. Die Ausgabe kann 2 Zeilen umfassen - die erste Zeile zeigt den aktuellen Zustand, die zweite Zeile den Status nach einem Neustart
3. Die Ausgabe kann mehrere Zeilen umfassen
4. Bitte die Energie Sensor Tabelle konsultieren, um den richtigen Index zu finden

## Energie Sensor Tabelle

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

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

## 4.6 Nachrichten

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

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

### 4.6.1.E-Mail

Bei folgenden Ereignissen werden E-Mail Benachrichtigungen ausgelöst:

- Schalten der Power-Ports
- Überschreiten von Max/Min Werten der Sensoren
- Änderung des Sensor Digitaleingangs
- Überschreiten von Max/Min Werten der gemessenen Stromaufnahme
- Statusänderung des Überspannungsschutzes

### 4.6.2.SNMP Traps

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

- Schalten der Power-Ports
- Überschreiten von Max/Min Werten der Sensoren
- Änderung des Sensor Digitaleingangs
- Überschreiten von Max/Min Werten der gemessenen Stromaufnahme
- Statusänderung des Überspannungsschutzes

### 4.6.3.Syslog

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

- Einschalten des Geräts
- Ein- bzw. Ausschalten von Syslog in der Konfiguration
- Schalten der Power-Ports
- Überschreiten von Max/Min Werten der Sensoren
- Änderung des Sensor Digitaleingangs
- Überschreiten von Max/Min Werten der gemessenen Stromaufnahme
- Statusänderung des Überspannungsschutzes

## 5. Support

### 5.1. Datensicherheit

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

- HTTP Passwort einschalten
- Nicht das Default HTTP Passwort verwenden
- Den Zugriff auf HTTP nur über SSL erlauben
- In SNMPv3 Authentifizierung und Verschlüsselung einschalten
- SNMP v2 abschalten
- In der E-Mail Konfiguration STARTTLS bzw. SSL einschalten
- In der IP ACL nur die Geräte eintragen, die Zugriff auf HTTP oder SNMP benötigen

### 5.2. Kontakt

Bei weiteren Fragen zu Installation oder Betrieb des Geräts wenden Sie sich bitte an unser Support-Team.

ANTRAX Datentechnik GmbH  
Hasenbrink 4  
32052 Herford

Telefon: 05221 929 66-0  
Fax: 05221 929 66-28  
E-Mail: [info@antrax.de](mailto:info@antrax.de)  
Internet: [www.antrax.de](http://www.antrax.de)

USt-IdNr.: DE812964730  
eingetragen im Handelsregister des Amtsgerichtes Bad Oeynhausen  
Handelsregisternummer HRB HRB 5275

WEEE-Reg.-Nr. DE 69438430

### 5.3. FAQ

#### 4. 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 verbindet 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.