

LINDY®

CONNECTION PERFECTION

IPower Strip 4

Benutzerhandbuch

Deutsch

No. 32661

www.lindy.com



1.	Gerätebeschreibung	3
1.1.	Sicherheitserklärung	3
1.2.	Lieferumfang	3
1.3.	Beschreibung	4
1.4.	Anschluss und Inbetriebnahme	5
1.5.	Überspannungsschutz	6
1.6.	Status LED	6
1.7.	Bootloader-Modus	6
1.8.	Firmware-Update	8
1.9.	Technische Daten	8
1.9.1.	Elektrische Meßgrößen	9
1.10.	Sensoren	9
2.	Bedienung	10
2.1.	Bedienung am Gerät	10
2.2.	Control Panel	11
2.3.	Maintenance Funktionen	13
3.	Konfiguration	14
3.1.	Netzwerkkonfiguration per Software	14
3.2.	Konfiguration per Webinterface	15
3.2.1.	Power Ports	15
3.2.2.	Watchdog	16
3.2.3.	IP Address	18
3.2.4.	IP ACL	19
3.2.5.	HTTP	20
3.2.6.	Sensors	21
3.2.7.	SNMP	23
3.2.8.	Syslog	24
3.2.9.	E-Mail	25
4.	Spezifikationen	26
4.1.	IP ACL	26
4.2.	IPv6	26
4.3.	SNMP	27
4.3.1.	Geräte MIB	29
4.4.	SSL	30
4.5.	Nachrichten	32
4.5.1.	E-Mail	32
4.5.2.	SNMP Traps	33
4.5.3.	Syslog	33
5.	Support	33

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, Styroporsteile 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:

- **LINDY IPower Strip 4**
- Schnellstart-Anleitung
- CD-ROM mit Anleitung und Softwaretools

1.3. Beschreibung

Der **LINDY IPower Strip 4** kann 4 verschiedene Lastausgänge (Schuko-Steckdosen (CEE 7/3), max. 16A) schalten.

Das Gerät hat folgende Features:

- Schalten von 4 Lastausgängen.
- Energiemessung des Netzanschlusses sowie Messung der Größen Spannung, Strom, Wirkleistung, Blindleistung, Scheinleistung, Frequenz, Phasenwinkel und Powerfaktor.
- Anschluss eines optionalen externen Sensors zur Ermittlung der Temperatur und Luftfeuchtigkeit, oder eines Schalteingangs.
- Eine dreistellige 7-Segment LED-Anzeigen (für Stromanzeige oder Temperatur/Luftfeuchtigkeit der externen Sensoren).
- Getrennter Überspannungsschutz (Overvoltage Protection).
- Einzeln parametrisierbare Einschaltverzögerung aller Lastausgänge.
- Für jeden Lastausgang individuell einstellbarer Watchdog, der in Abhängigkeit der Erreichbarkeit (Netzwerk-Ping) schaltet.
- Dual TCP/IP Stack mit IPv4 und IPv6 Unterstützung.
- Steuerung und Überwachung des Geräts über Ethernet mit einem integrierten Webserver mit SSL Verschlüsselung und SNMP (v1, v2c und v3).
- 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.
- Verschlüsselte E-mails.

LINDY-Control: Unsere IPower-Produkte lassen sich auch bequem per App bedienen. Laden Sie sich hierfür einfach die entsprechende App „LINDY-Control“ vom PlayStore oder AppStore auf Ihr Smartphone oder Tablet.

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 Netzwerkkabel in die Ethernetbuchse (RJ45).
- Schließen Sie den externen Sensor (optional) an.

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

Die Konfiguration mit GBL_Conf.exe ist nur möglich, wenn sich das Gerät im Bootloader-Modus befindet.

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 Software: (nur wenn vorher "Enable FW to BL" in GBL_Conf.exe aktiviert wurde)

- Starten Sie GBL_Conf.exe
- Führen Sie mit "Search" eine Netzwerksuche aus
- Aktivieren Sie unter "Program Device" den Menüpunkt "Enter Bootloader"

per Webinterface:

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

Ob sich das Gerät im Bootloader-Modus befindet, erkennen Sie am Blinken der Status LED, oder in GBL_Conf.exe bei einer erneuten Gerätesuche an dem Zusatz „BOOT-LDR“ hinter dem Gerätenamen. Im Bootloader-Modus lassen sich mit Hilfe des Programms GBL_Conf.exe das Passwort und die IP ACL deaktivieren, ein Firmware-Update durchführen sowie der Werkzustand wieder herstellen.



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

per Software:

- Starten Sie GBL_Conf.exe
- Führen Sie mit "Search" eine Netzwerksuche aus
- Aktivieren Sie unter "Program Device" den Menüpunkt "Enter Firmware"

Werkzustand

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

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 Software:

- Aktivieren Sie dazu den Bootloader-Modus des Geräts
- Starten Sie 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)

per Webinterface:

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

1.8. Firmware-Update

Ein Firmware-Update kann über das Webinterface oder durch Gbl_Conf.exe erfolgen:

per Webinterface:

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

per Software:

- Aktivieren Sie den Bootloader-Modus (siehe Kapitel Bootloader-Modus).
- Starten Sie Gbl_Conf.exe.
- Markieren Sie im linken Feld das Gerät, für das ein Firmware-Update durchgeführt werden soll.
- Klicken Sie dann unter "*Program Device*" auf den Eintrag "*Firmware Update*"
- Geben Sie die zu übertragende Firmwaredatei an

Nach Abschluss des Update-Vorgangs mit Gbl_Conf.exe starten Sie bitte die Firmware des Geräts neu. Dazu verlassen Sie einfach den Bootloader-Modus.

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. Bei Bedarf korrigieren Sie im Bootloader Modus die Einträge in Gbl_Conf.exe und speichern mit "*Save Config*" ab.



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	1 x Ethernetanschluss (RJ45) 1 x Netzanschluss (Schukostecker, max. 16A), Länge ca. 2m 4 x Lastausgänge (Schukosteckdose, max. 16 A) 1 x Mini-DIN für externen Sensor
Netzwerkanbindung	10/100 MBit/s 10baseT Ethernet
Protokolle	TCP/IP, HTTP/HTTPS, SNMP v1/v2c/v3, SNMP traps, Syslog, E-Mail (SMTP)
Spannungsversorgung	internes Netzteil (230V AC / -15% / +10%)
Überspannungsschutz <ul style="list-style-type: none"> • Maximale Betriebsspannung • einmal. Spitzenstrom für 20/80us Puls • Max. Begrenzungsspannung 20/80us Puls, I_{pk}=100A 	Varistor 20 mm/190J Scheibe 300 VACrms 10000 A 710 V
Umgebung <ul style="list-style-type: none"> • Betriebstemperatur • Lagertemperatur • Luftfeuchtigkeit 	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

Elektrische Messgrößen				
Messwert	Bereich	Einheit	Auflösung	Ungenauigkeit (typisch)
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%
Energiezähler				
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

Am **LINDY IPower Strip 4** kann ein externer Sensor der Firma LINDY angeschlossen werden. Aktuell sind folgende Sensoren verfügbar



Temperatursensor 32638 / 32649	
Kabellänge	≈ 2m
Anschluss	Mini-DIN
Temperaturbereich	-20°C bis +80°C bei ±2°C (maximal) und ±1°C (typisch)



Feuchte/Tempsensor (auf Anfrage)	
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	Reset min/max

Port	Name	Humidity	24h min	24h max	
1: 7002	Humidity	32,3 %	31,3 %	33,6 %	Reset min/max

2. Bedienung

2.1. Bedienung am Gerät

Schalten

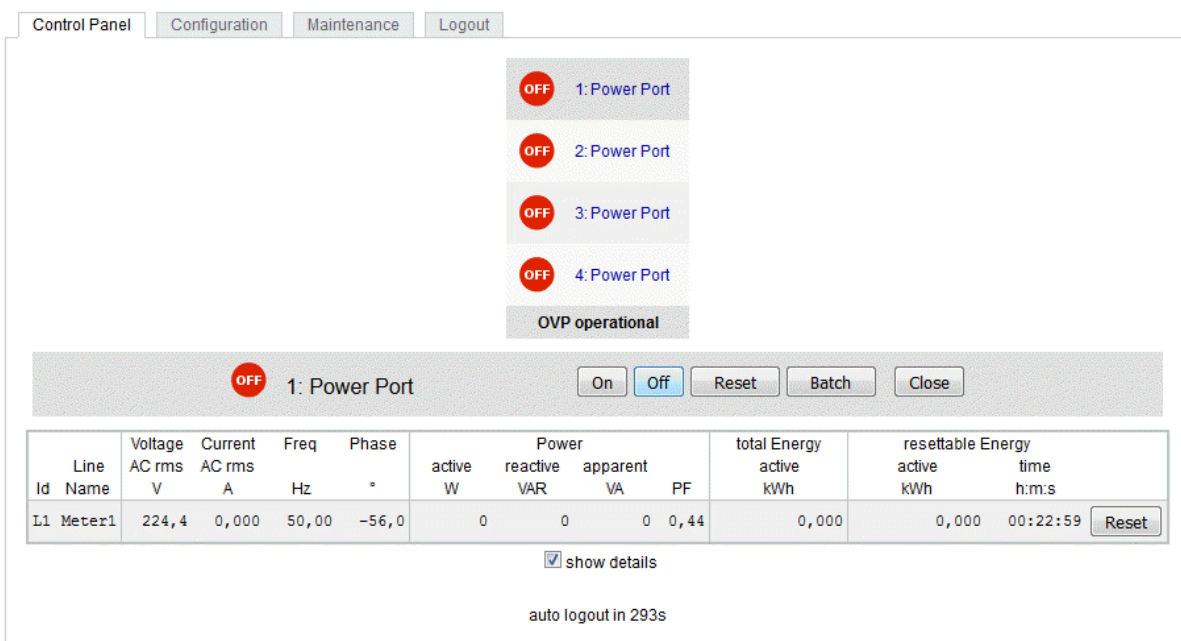
Den aktuellen Schaltzustand des Ausgangs erkennt man an den dazugehörigen Klartext-Anzeigen (Port-LEDs). Leuchtet die grüne "on" LED, ist der Port eingeschaltet, leuchtet die rote "off" LED ist der Ausgangsport ausgeschaltet. Am Gerät befinden sich die Taster „Select“ und „Ok“. Wenn Sie „select“ drücken, 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

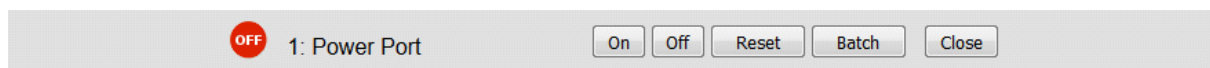
Ist kein Port manuell selektiert, werden durch wiederholtes Drücken des "Ok" Tasters nacheinander die IP-Adresse und die Werte der externen Sensoren im Display (7-Segment Anzeige) dargestellt.

2.2. Control Panel

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



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.

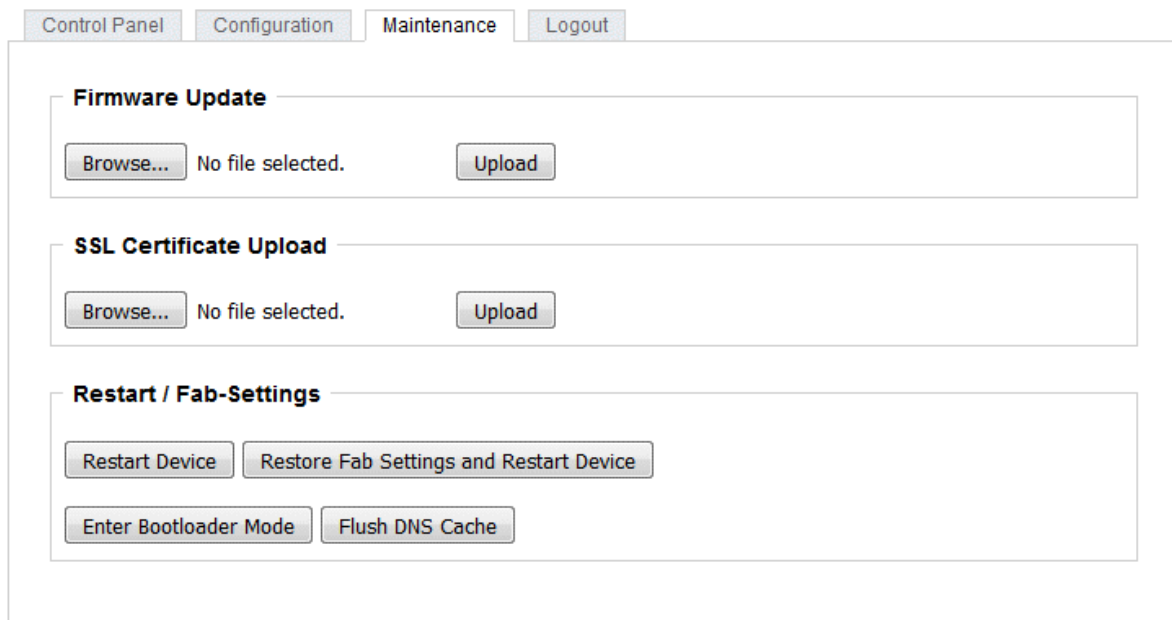
Möchte man den Zustand des Ports für eine festgelegte Zeitspanne ändern, kann man mit Hilfe der Dropdown-Werte die Schaltvorgänge ("switch on" bzw. "switch off") sowie die Wartezeit dazwischen (in Sekunden, Minuten oder Stunden) auswählen.



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.



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.

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 dem mit Gbl_Conf.exe Einstellungen vorgenommen werden können.

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

3. Konfiguration

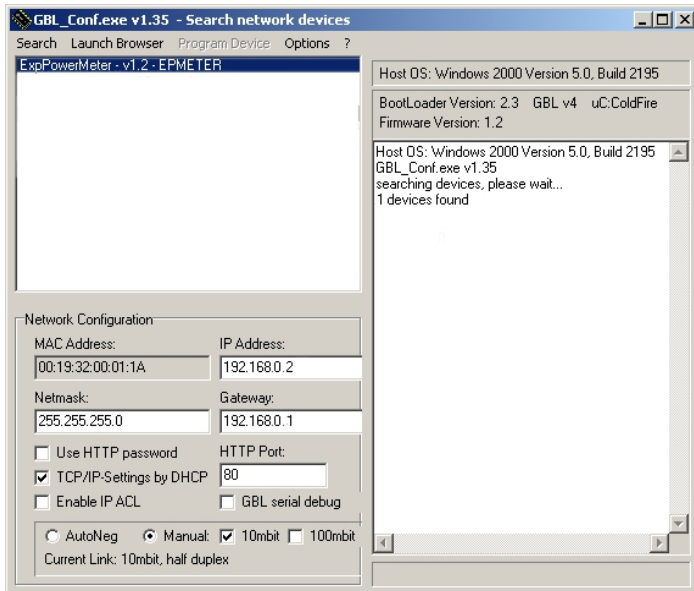
Automatische Konfiguration per DHCP

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. Netzwerkkonfiguration per Software

Zur Ansicht und Veränderung der Netzwerkeinstellungen können Sie das Programm GBL_Conf.exe nutzen. Das Programm ist kostenlos auf unserer Webseite www.lindy.de erhältlich und befindet sich auch auf der beiliegenden CD-ROM. Sie können mit dem Programm GBL_Conf.exe auch Firmware-Updates einspielen und ein Zurücksetzen auf die [Werkseinstellungen](#) auslösen.



Oberfläche GBL_Conf.exe

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

- Aktivieren Sie den Bootloader-Modus (siehe Kapitel Bootloader Modus) und wählen Sie in "Search" den Punkt "Bootloader-Mode Devices only".

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

Die neue Netzwerkkonfiguration wird jetzt angezeigt.

3.2. 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.

3.2.1. Power Ports

The screenshot shows a web interface with a navigation bar at the top containing 'Control Panel', 'Configuration', 'Maintenance', and 'Logout'. Below the navigation bar is a breadcrumb trail: 'Power Ports · IP Address · IP ACL · HTTP · Sensors · SNMP · Syslog · E-Mail'. The main content area is titled 'Power Ports' and contains the following configuration options:

- Choose Power Port to configure: 1: Power Port (dropdown menu)
- Label: Power Port (text input)
- Initialization status (coldstart): on off remember last state
- Initialization delay: 0 s (text input)
- Repower delay: 0 s (text input)
- Reset duration: 10 s (text input)
- Enable watchdog: yes no

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

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, dass die Initialisierung ausgeschaltet ist.

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

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

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

3.2.2. Watchdog

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:	<input checked="" type="radio"/> yes <input type="radio"/> no
• Watchdog action:	<input checked="" type="radio"/> reset <input type="radio"/> off
• Watchdog type:	<input checked="" type="radio"/> ICMP <input type="radio"/> TCP
• Hostname:	<input type="text"/>
• Ping interval:	<input type="text" value="10"/> s
• Ping retries:	<input type="text" value="6"/>
• retry BOOTING after RESET failure:	<input type="radio"/> no <input checked="" type="radio"/> yes
• retry Boot after N ping timeouts:	<input type="text" value="10"/>

3.2.3. IP Address

Control Panel
Configuration
Maintenance
Logout

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

Configuration - IP

- 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 Neighbor Discovery + SLAAC: yes no
- Use DHCP v6: yes no
- Current IPv6 address(es):

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 Address: Die IP Adresse des Gerätes.

Netmask: Die Netzmaske im verwendeten Netz.

Gateway address: IP Adresse des Gateway.

Use 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 Neighbor Discovery + SLAAC: Die "Stateless Address Autoconfiguration" kommuniziert mit dem Router, um die globale IPv6-Adresse zugänglich zu machen.

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

Current IPv6 adresse(s): Zeigt die IPv6 Adressen, über die das Gerät erreichbar ist.



Für IP Änderungen ist ein Neustart der Firmware notwendig. Dies kann im Maintenance Bereich vorgenommen werden.

3.2.4. IP ACL

Control Panel Configuration Maintenance Logout

Power Ports · IP Address · **IP ACL** · HTTP · 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:f124	Delete	Add
2. Grant IP access to host/net:	192.168.1.84	Delete	Add
3. Grant IP access to host/net:	mypc.locdom	Delete	Add
4. Grant IP access to host/net:	192.168.1.0/24	Delete	Add
5. Grant IP access to host/net:	1234:4ef0:eec1:0::/64	Delete	Add

Apply

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

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

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

 Sollten Sie sich hier aus Versehen „ausgesperrt“ haben, aktivieren Sie den Bootloader-Modus und deaktivieren Sie mit Hilfe der GBL_Conf.exe die IP ACL. Als Alternative können Sie das Gerät in den Werkszustand zurücksetzen.

3.2.5. HTTP

Control Panel
Configuration
Maintenance
Logout

[Power Ports](#) · [IP Address](#) · [IP ACL](#) · [HTTP](#) · [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:

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


HTTP port: 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 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 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.

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

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

3.2.6. Sensors

Control Panel
Configuration
Maintenance
Logout

Power Ports
IP Address
IP ACL
HTTP
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
- Min/Max measurement period:

Display

- Default display:

Choose power meter: Selektiert den Messkanal (nur einer beim **LINDY IPower Strip 4**).

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.

Enable alarm with beeper: Schaltet den Summer bei Unter-/Überschreiten der Strom-Grenzwerte 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 Buchstaben 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.

Enable alarm with beeper: Schaltet den Summer bei Unter-/Überschreiten der Sensor Grenzwerte ein.

Maximum/Minimum value: Einstellbare Grenzwerte, bei denen Meldungen per SNMP-Trap, Syslog oder Email 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.

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

3.2.7. SNMP

Control Panel
Configuration
Maintenance
Logout

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

SNMP

• Enable SNMP options: SNMP get SNMP set

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.

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: Dass 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.

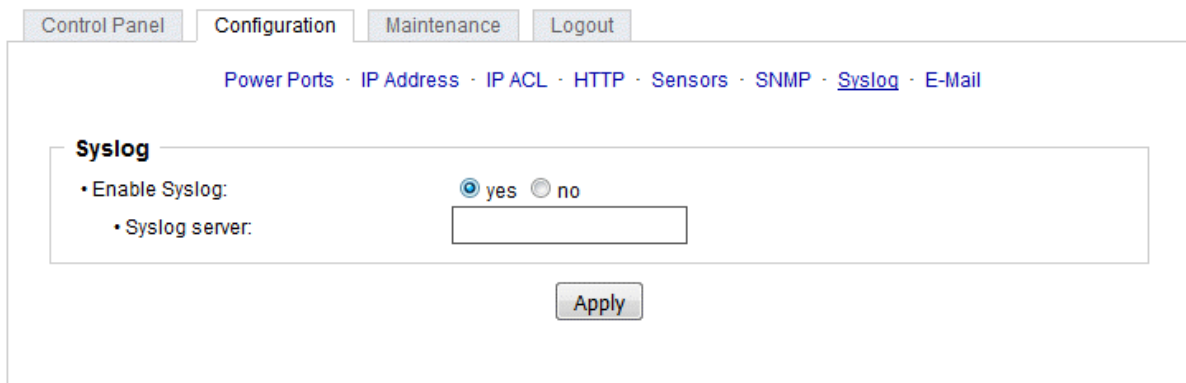
 Die Berechnung der Passwort Hashes ändert sich mit den eingestellten Algorithmen. Werden die Authentication oder Privacy Algorithmen geändert, müssen im Konfigurationsdialog die Passwörter wieder neu eingegeben werden.

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

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.

3.2.8. Syslog



Control Panel Configuration Maintenance Logout

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

Syslog

- Enable Syslog: yes no
- Syslog server:

Apply

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

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

3.2.9. E-Mail

Control Panel Configuration Maintenance Logout

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

E-Mail

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

Authentication

- SMTP Authentication (password): ▼
- Username:
- Set new password:
- Repeat password:

Apply

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 Authentication (password): Authentifizierung des E-Mailservers.

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

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

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

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

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


4. Spezifikationen

4.1. IP ACL

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

Beispiele:

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

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

4.2. IPv6

IPv6 Adressen

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

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. Da RFC7630 sehr neu ist, existieren aber noch keine Clients, mit der die "HMAC-SHA-2" Implementierung ausreichend getestet werden konnte.

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.

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.
- 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 Prefix "1.3.6.1.4.1.28507" zur Gude Enterprise OID aus Platzgründen bei jedem Eintrag in der Tabelle weggelassen. Die komplette OID würde daher z.B. "1.3.6.1.4.1.28507.43.1.1.1.1" 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			
epc1202OVPStatus	.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 Zertifikat

```
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
```

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. 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

4.5.1. E-Mail

Bei folgenden Ereignissen werden Email Benachrichtigungen ausgelöst:

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

- Statusänderung des Überspannungsschutzes

4.5.2. 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

4.5.3. 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

Auf unseren Internetseiten unter www.lindy.de 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.

CE Statement

CE Certification

This equipment complies with the requirements relating to Electromagnetic Compatibility Standards EN55022/EN55024 and the further standards cited therein. It must be used with shielded cables only. It has been manufactured under the scope of RoHS compliance.

CE Konformitätserklärung

Dieses Produkt entspricht den einschlägigen EMV Richtlinien der EU für IT-Equipment und darf nur zusammen mit abgeschirmten Kabeln verwendet werden.

Diese Geräte wurden unter Berücksichtigung der RoHS Vorgaben hergestellt.

Die formelle Konformitätserklärung können wir Ihnen auf Anforderung zur Verfügung stellen

LINDY Herstellergarantie – Hinweis für Kunden in Deutschland

LINDY gewährt für dieses Produkt über die gesetzliche Regelung in Deutschland hinaus eine zweijährige Herstellergarantie ab Kaufdatum. Die detaillierten Bedingungen dieser Garantie finden Sie auf der LINDY Website aufgelistet bei den AGBs.

Hersteller / Manufacturer (EU):

LINDY-Elektronik GmbH

Markircher Str. 20

68229 Mannheim

GERMANY

Email: info@lindy.com , T: 0049 (0)621 470050

LINDY Electronics Ltd.

Sadler Forster Way

Teesside Industrial Estate, Thornaby

Stockton-on-Tees, TS17 9JY

United Kingdom

postmaster@lindy.co.uk , T: +44 (0) 1642 754000

Recycling Information



WEEE (Waste of Electrical and Electronic Equipment), Recycling of Electronic Products

Europe, United Kingdom

In 2006 the European Union introduced regulations (WEEE) for the collection and recycling of all waste electrical and electronic equipment. It is no longer allowable to simply throw away electrical and electronic equipment. Instead, these products must enter the recycling process.

Each individual EU member state has implemented the WEEE regulations into national law in slightly different ways. Please follow your national law when you want to dispose of any electrical or electronic products. More details can be obtained from your national WEEE recycling agency.

Germany / Deutschland

Die Europäische Union hat mit der WEEE Richtlinie Regelungen für die Verschrottung und das Recycling von Elektro- und Elektronikprodukten geschaffen. Diese wurden im Elektro- und Elektronikgerätegesetz – ElektroG in deutsches Recht umgesetzt. Dieses Gesetz verbietet das Entsorgen von entsprechenden, auch alten, Elektro- und Elektronikgeräten über die Hausmülltonne! Diese Geräte müssen den lokalen Sammelsystemen bzw. örtlichen Sammelstellen zugeführt werden! Dort werden sie kostenlos entgegen genommen. Die Kosten für den weiteren Recyclingprozess übernimmt die Gesamtheit der Gerätehersteller.

France

En 2006, l'union Européenne a introduit la nouvelle réglementation (DEEE) pour le recyclage de tout équipement électrique et électronique.

Chaque Etat membre de l' Union Européenne a mis en application la nouvelle réglementation DEEE de manières légèrement différentes. Veuillez suivre le décret d'application correspondant à l'élimination des déchets électriques ou électroniques de votre pays.

Italy

Nel 2006 l'unione europea ha introdotto regolamentazioni (WEEE) per la raccolta e il riciclo di apparecchi elettrici ed elettronici. Non è più consentito semplicemente gettare queste apparecchiature, devono essere riciclate. Ogni stato membro dell' EU ha tramutato le direttive WEEE in leggi statali in varie misure. Fare riferimento alle leggi del proprio Stato quando si dispone di un apparecchio elettrico o elettronico.

Per ulteriori dettagli fare riferimento alla direttiva WEEE sul riciclaggio del proprio Stato.



LINDY No 32661

1st Edition, FEB 2016

www.lindy.com