Industrie-4G-LTE-Router YZWK001 (YZWK001WS-4G)

Bedienungs- und Installationsanleitung, Version 2.0

4G LTE Cat-1 · WLAN 2,4 GHz · 1 × LAN 10/100 · RS485/RS232 · Modbus RTU/TCP · MQTT · VPN (WireGuard, ZeroTier, OpenVPN, IPsec, L2TP) · 9–35 V DC · Hutschiene

Stand: 10/2026 · Grundlage: Herstellerdatenblatt V1.1, Weboberfläche Firmware R_01.01_STD (Web-UI 0.0.386), praktische Inbetriebnahme. Bitte lesen Sie diese Anleitung vor der Installation vollständig durch und bewahren Sie sie auf.

> **So benutzen Sie diese Anleitung.** Der Router wird im Werkszustand geliefert. Kapitel 1 bis 11 gelten für alle Anwender. Danach wählen Sie Ihr Zielbild: **Zielbild 1 „Anlage ohne Festnetz"** (Kapitel 12): Der Router sendet Modbus-Werte über Mobilfunk an einen MQTT-Broker im Internet, Fernzugriff per VPN. **Zielbild 2 „Anlage im Heimnetz mit Home Assistant"** (Kapitel 13): Der Router hängt im Heimnetz, Home Assistant liest die Werte lokal. Jeder Schritt nennt den Menüpfad der Weboberfläche und einen **Kontrollpunkt**, an dem Sie erkennen, dass der Schritt gelungen ist.



Abb. 01: Router YZWK001 mit 4G-Antenne

Inhalt

1. Sicherheitshinweise
2. Bestimmungsgemäße Verwendung und Zielbilder
3. Lieferumfang und Typenschild
4. Gerätebeschreibung: Anschlüsse, LEDs, Taste, Klemmenbelegung
5. Technische Daten
6. Montage und Platzbedarf
7. Elektrischer Anschluss: Versorgung und RS485
8. Inbetriebnahme: SIM, Antenne, Zugang zur Weboberfläche
9. Grundkonfiguration: Pflichtschritte nach der ersten Anmeldung
10. Die Weboberfläche im Überblick
11. RS485/Modbus einrichten: Modbus-TCP-Gateway oder Modbus Collect mit MQTT
12. Zielbild 1: Anlage ohne Festnetz (Mobilfunk, Cloud-MQTT, VPN)
13. Zielbild 2: Anlage im Heimnetz mit Home Assistant
14. Fernzugriff per VPN
15. Service: Zugang zu einem Router, der bereits in einem fremden Netz steckt
16. Neustart, Sicherung, Werkseinstellungen, Firmware-Update
17. Fehlerbehebung
18. Wartung, Entsorgung, Hinweise

- Anhang A: Schnellstart in 5 Schritten (Kundenblatt)
- Anhang B: Werkswerte und Menüreferenz
- Anhang C: Praxisbeispiel Temperaturregler AiFUZZY/Yudian
- Anhang D: Abbildungsverzeichnis

---

1 Sicherheitshinweise

Achtung: nur Schutzkleinspannung. Das Gerät wird ausschließlich mit 9–35 V DC betrieben. Niemals 230 V AC an die Klemmen anschließen. Das Netzteil muss eine sicher getrennte Kleinspannung (SELV/PELV) liefern. Arbeiten im Schaltschrank mit Netzspannung dürfen nur von einer Elektrofachkraft ausgeführt werden. Anlage vorher spannungsfrei schalten und gegen Wiedereinschalten sichern.

- Nur in trockenen Innenräumen oder im geschlossenen Schaltschrank betreiben. Betauung vermeiden, Luftfeuchte unter 95 % nicht kondensierend.
- Zulässiger Temperaturbereich −30 °C bis +75 °C. Nicht direkt über wärmeabgebenden Bauteilen (Netzteile, Schütze, Frequenzumrichter) montieren.
- Gerät nicht öffnen. Keine vom Anwender zu wartenden Teile.
- SIM-Karte nur im spannungslosen Zustand einsetzen oder entnehmen.
- Antenne mit mindestens 20 cm Abstand zu Personen betreiben. Nur die mitgelieferte oder eine gleichwertige Antenne verwenden.
- **Werkseitige Passwörter (WLAN und Weboberfläche) bei der Inbetriebnahme immer ändern.** Das Gerät ist über Mobilfunk mit dem Internet verbunden. Im Werkszustand ist die Weboberfläche auch aus dem Mobilfunknetz erreichbar (Kapitel 9.3).

- Das Gerät ist nicht für sicherheitsrelevante Steuerungsaufgaben (Not-Aus, Sicherheitsabschaltungen von Wärmeerzeugern) vorgesehen. Sicherheitsfunktionen müssen unabhängig vom Router wirken.

2 Bestimmungsgemäße Verwendung und Zielbilder

Der YZWK001 ist ein kompakter Mobilfunk-Router für die Hutschiene. Er stellt eine Internetverbindung über 4G LTE bereit, verteilt sie per LAN und WLAN und fragt als Modbus-Master über RS485 Geräte wie Energiezähler, Wechselrichter, Wärmepumpen- oder Heizungsregler ab. Die Messwerte sendet er per MQTT an einen Server oder stellt sie als Modbus-TCP-Gateway bereit. Über VPN ist ein sicherer Fernzugriff auf die Anlage möglich.

Typische Einsatzorte: Heizungs- und Technikräume, PV- und Speicheranlagen, Zählerschränke, Unterverteilungen, Ferienhäuser und Baustellen ohne Festnetz-Internet.

Wichtig zum Netzwerk-Konzept: Der Router ist im Werkszustand ein **eigenständiges Netz** (192.168.8.x) mit eigenem DHCP-Server. Er ist nicht dafür gedacht, einfach in den Switch oder die Fritzbox eines bestehenden Heimnetzes gesteckt zu werden. Für die Einrichtung verbinden Sie sich direkt mit dem Router (Kapitel 8). Soll der Router dauerhaft im Heimnetz hängen, folgen Sie Kapitel 13.

Zielbild	Internet	Datenweg	Zugriff aus der Ferne
1 Anlage ohne Festnetz	Mobilfunk (SIM)	Router pollt Modbus, sendet per MQTT an Broker im Internet	VPN (WireGuard oder ZeroTier)
2 Anlage im Heimnetz	Mobilfunk (SIM); Heimnetz nur lokal	Home Assistant liest per Modbus TCP oder MQTT im Heimnetz	über das Heimnetz, optional VPN

Zielbild 1: Anlage ohne Festnetz

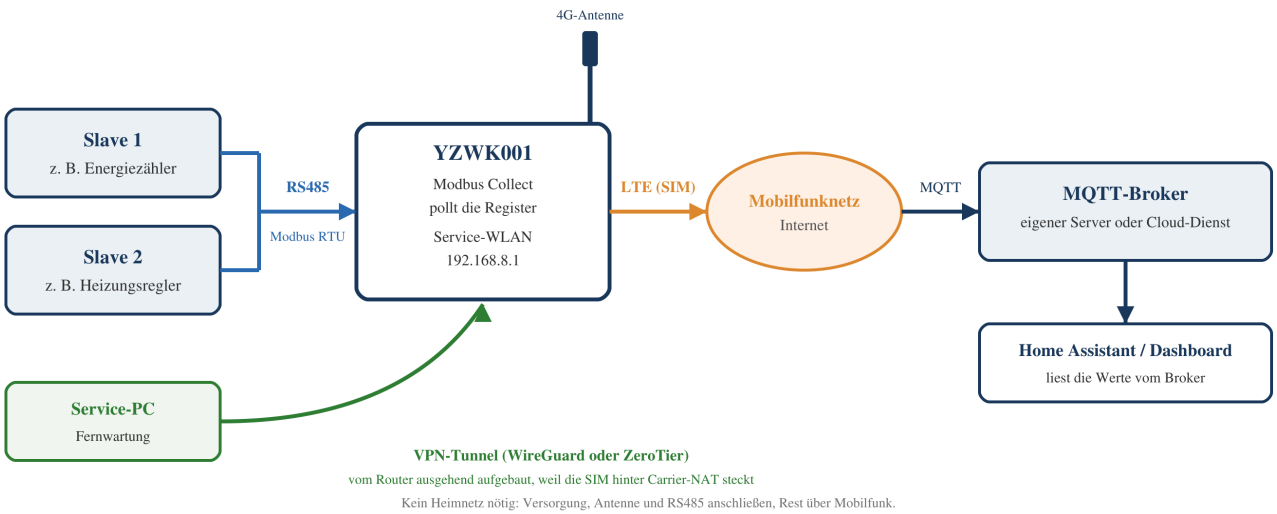


Abb. 02: Zielbild 1: Anlage ohne Festnetz, Werte per Mobilfunk an einen MQTT-Broker, Fernwartung per VPN

Zielbild 2: Anlage im Heimnetz mit Home Assistant

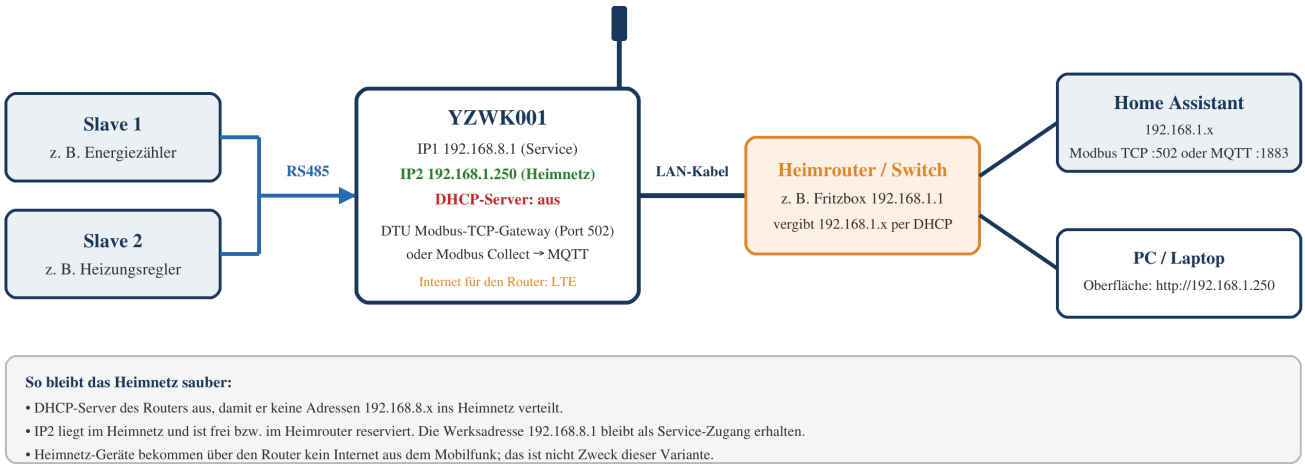


Abb. 03: Zielbild 2: Router im Heimnetz, Home Assistant liest lokal

3 Lieferumfang und Typenschild

Menge	Teil
1	Router YZWK001
1	4G-Flachantenne, SMA-Stecker, 5 dBi
1	Netzwerkkabel, 1 m
1	4-polige Steckklemme 3,5 mm (Versorgung und RS485)
1	Hutschienen-Clip

			
Router YZWK001	Netzwerkkabel 1 m	4-polige Steckklemme	Hutschienen-Clip

Nicht im Lieferumfang: Netzteil (12 V DC empfohlen, Kapitel 7), SIM-Karte (Nano-SIM mit Datentarif). WLAN arbeitet über eine interne Antenne.

Typenschild. Auf dem Gerät finden Sie: Seriennummer (Format ZWK001Q…), WLAN-Name (SSID) nach dem Schema `Wireless-2G-` plus letzte sechs Stellen der Seriennummer, WLAN-Passwort, Benutzername und Passwort der Weboberfläche. **Notieren Sie diese Daten, bevor Sie das Gerät im Schaltschrank montieren.**

[Abb. 04: Typenschild mit Markierung von Seriennummer, SSID, WLAN-Passwort und Login]

Ihre Gerätedaten	
Seriennummer	_____
WLAN-Name (SSID)	Wireless-2G-_____
WLAN-Passwort (Werk)	_____
Login Weboberfläche (Werk)	admin / _____
Neues Admin-Passwort (Kapitel 9.2)	_____

4 Gerätebeschreibung

Front: SIM-Schacht (Nano-SIM, 1,8 V / 3 V), LEDs, Taste RST.

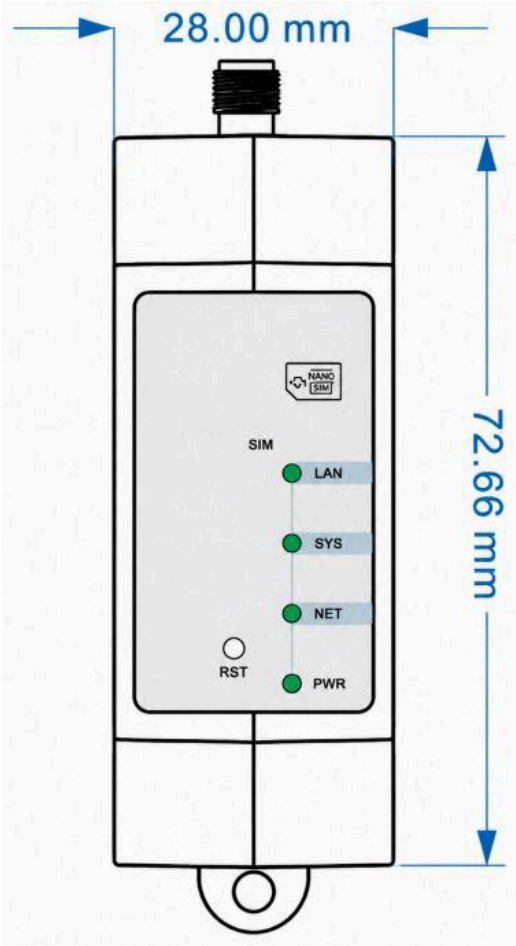


Abb. 05: Frontansicht mit SIM-Schacht, LEDs und Taste RST (Breite 28 mm, Höhe 72,7 mm)

LED	Bedeutung
PWR	Betriebsspannung liegt an
NET	Mobilfunk-Netzstatus (Einbuchung, Datenverbindung)
SIG	Mobilfunk-Signalanzeige
LAN	Ethernet-Anschluss (Verbindung, Datenverkehr)

Taste RST: kurz drücken = Neustart; gedrückt halten, bis die LEDs einen Neustart anzeigen = Werkseinstellungen (Kapitel 16).

Oberseite: ANT, SMA-Buchse für die 4G-Antenne. **Unterseite:** LAN (RJ45, 10/100 Mbit/s, Auto-MDI/MDIX) und 4-polige Steckklemme.

Klemmenbelegung (Blick von unten)

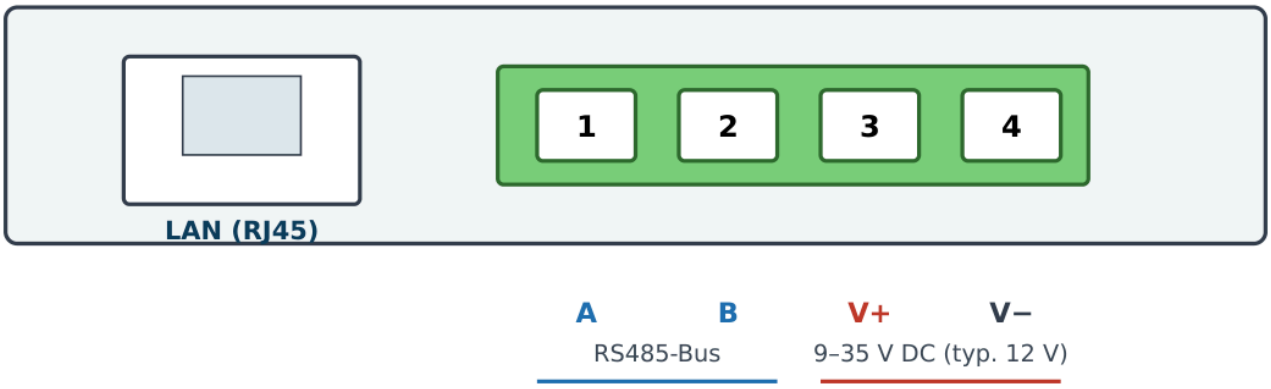


Abb. 06: Unterseite mit LAN (RJ45) und 4-poliger Steckklemme, Blick von unten

Klemme	1	2	3	4
Funktion	RS485 A (+)	RS485 B (−)	V+ (9–35 V DC)	V− (Masse, zugleich Bezugspotenzial RS485)

Die serielle Schnittstelle ist per Software zwischen **RS485 und RS232** umschaltbar (Kapitel 11.1). Werkseinstellung ist **RS232**. Für Modbus RTU muss **RS485** gewählt werden. Ein Abschlusswiderstand ist im Gerät nicht per Schalter vorhanden; bei Bedarf extern 120 Ω zwischen A und B (Kapitel 7.2).

5 Technische Daten

Mobilfunk	
Standard	4G LTE Cat-1, kein 2G/3G-Fallback; Modul Quectel EG800K (EU)
Datenrate	LTE-FDD bis 10 Mbit/s Download, 5 Mbit/s Upload
Frequenzbänder (EU)	LTE-FDD B1, B3, B5, B7, B8, B20, B28
SIM	1 × Nano-SIM, 1,8 V / 3 V
APN	Auto-APN oder manuell; Statuswerte Signal (dBm), Netztyp, Betreiber, ICCID, IMSI, IMEI
Antenne	698–960 / 1710–2690 MHz, 50 Ω, 5 dBi, SMA

WLAN / LAN	
WLAN	2,4 GHz, IEEE 802.11 b/g/n, Access Point **oder** Station (Client), nicht gleichzeitig; interne Antenne
WLAN-Sicherheit	WPA2-PSK/WPA-PSK, AES/TKIP, SSID versteckbar, AP-Isolation, bis 50 Clients
Ethernet	1 × RJ45, 10/100 Mbit/s, Auto-MDI/MDIX, **nur LAN** (kein WAN-Modus in dieser Firmware)
LAN-Adressen	bis zu drei IPv4-Adressen (IP1 Management, IP2/IP3 Sekundär), DHCP-Server abschaltbar

Netzwerk und Sicherheit	
Uplinks / Failover	Mobilfunk; WLAN-Station als zweiter Uplink; Link Priority mit ICMP-Überwachung
Firewall	Fernzugriffs-Matrix (PING/WEB/SSH/TELNET je LAN/WAN/VPN), SPI-Filter (DDoS, Portscan, IP-Spoofing, SYN-Flood), Adress- und Domainfilter, DNAT/SNAT/DMZ, statische Routen
VPN	WireGuard, ZeroTier, OpenVPN (Client/Server), IPsec IKEv1/v2 (bis 10 Tunnel), L2TP (Client/Server), Hersteller-Cloud m2mCloud (werkseitig **ein**, Kapitel 9.4)
Verwaltung	Weboberfläche HTTP (Port 80) und HTTPS; CLI per Telnet oder SSH (umschaltbar, Kapitel 9.3); Konfigurations-Backup/-Restore; Firmware-Update; System-, Kernel- und Modem-Log; SNMP v2/v3
Sonstiges	Zeitgesteuerte Aktionen (Timer), ICMP-Watchdog, Ping/Traceroute-Werkzeug, LoRaWAN-Endknoten (SX1262, optional)

Serielle Schnittstelle / Modbus	
Schnittstelle	1 × seriell, per Software RS485 oder RS232; 300–230 400 Baud, Parität none/even/odd, 5–8 Datenbits, 1–2 Stoppbits
Betriebsart A „DTU"	transparente Brücke seriell ↔ TCP/UDP/MQTT; Modbus-Umsetzer RTU/ASCII ↔ TCP (Router als Modbus-TCP-Server oder -Client); AT-Durchleitung
Betriebsart B „Modbus Collect"	Router als Modbus-Master (RTU oder TCP), Reporting per MQTT, TCP, UDP oder IEC 60870-5-104
Funktionscodes (Modbus Collect)	01 Coils, 02 Discrete Inputs, 03 Holding Register, 04 Input Register; Schreiben über Datenpunkte mit „Writable" und MQTT-Subscribe
Datentypen	Signed/Unsigned 16 Bit, Signed/Unsigned 32 Bit und Float 32 Bit jeweils in den Wortfolgen ABCD, CDAB, BADC, DCBA
Abfrageintervall	30 ms bis 120 s je Datenpunkt

Hardware / Allgemein	
Prozessor / Speicher	MediaTek MT7628, 128 MB DDR2 RAM, 16 MB Flash
Betriebssystem	OpenWrt-basiertes Linux mit herstellereigener Weboberfläche (englisch)
Versorgung	9–35 V DC (typ. 12 V), verpolungsgeschützt, Steckklemme 3,5 mm
Leistungsaufnahme	< 3 W
Gehäuse	ABS, Hutschiene TS 35; 28 × 72,7 × 65,8 mm, Höhe mit SMA-Buchse ca. 88,7 mm; 60 g
Umgebung	−30 °C bis +75 °C, < 95 % r. F. nicht kondensierend

6 Montage und Platzbedarf

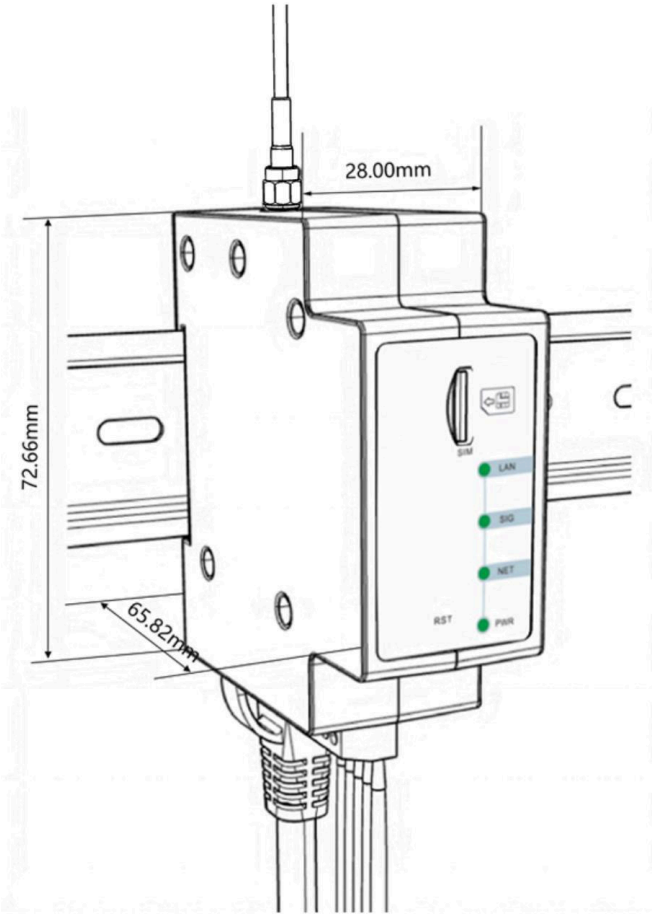


Abb. 07a: Platzbedarf mit Antenne und Kabeln (Breite 28 mm, Höhe 72,7 mm)

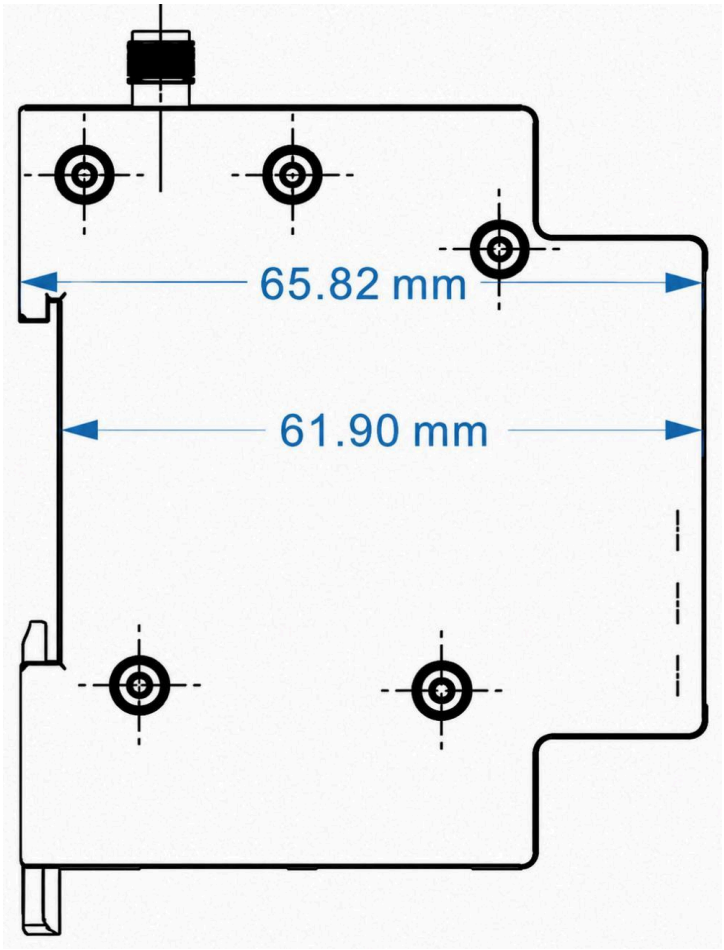


Abb. 07b: Seitenansicht, Tiefe 65,8 mm, Hutschienenaufnahme 61,9 mm

1. Hutschienen-Clip auf der Geräterückseite befestigen, falls nicht vormontiert.
2. Gerät oben in die 35-mm-Hutschiene einhängen und unten einrasten.
3. Platz einplanen: oben mindestens 30 mm für Antennenbuchse und Kabel, unten mindestens 40 mm für Netzwerkkabel und Steckklemme.

Antennenposition. Metallische Schaltschränke und Stahlbetonkeller dämpfen das Mobilfunksignal stark. Die Antenne im Metallschrank nicht innen montieren, sondern über ein SMA-Verlängerungskabel außerhalb des Schranks anbringen. Die Signalqualität prüfen Sie in der Weboberfläche (Kapitel 9.6).

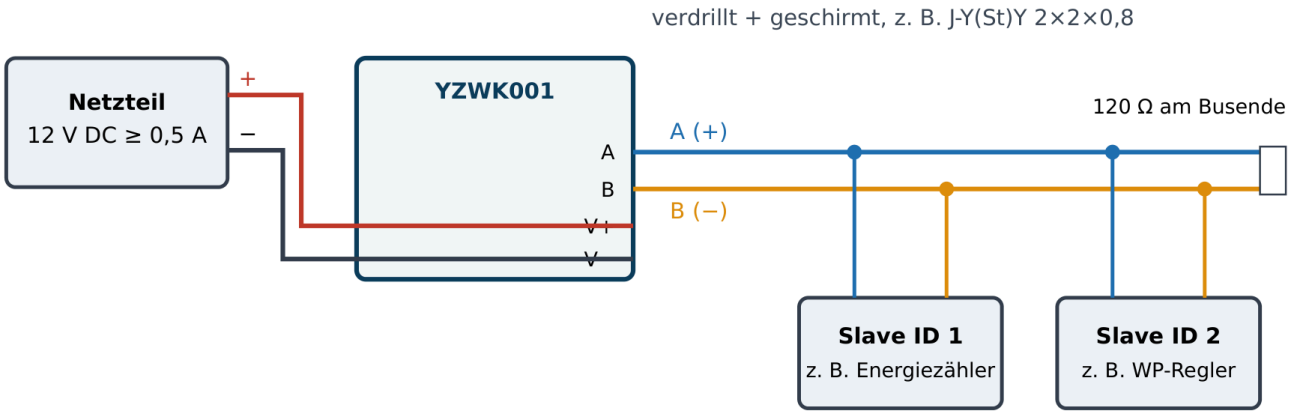
7 Elektrischer Anschluss

7.1 Spannungsversorgung

Empfohlen wird ein Hutschienen-Netzteil 12 V DC mit mindestens 0,5 A. Der Router nimmt unter 3 W auf, beim Senden im Mobilfunknetz treten kurze Stromspitzen auf. Alternativ 24-V-Anlagennetz, zulässig ist der gesamte Bereich 9–35 V DC.

- Plus an V+ (Klemme 3), Minus an V− (Klemme 4). Der Eingang ist verpolungsgeschützt.
- Leiterquerschnitt 0,5–1,5 mm², Aderendhülsen verwenden.
- Die Steckklemme erst nach vollständiger Verdrahtung auf das Gerät stecken.

7.2 RS485 / Modbus RTU



- Bus als Linie verdrahten, keine Sterntopologie · Abschluss 120 Ω zwischen A und B an beiden Busenden
- Schirm einseitig auf PE/Funktionserde auflegen

Anschlussbeispiel: Versorgung und RS485-Bus mit zwei Modbus-Teilnehmern

Abb. 08: Anschlussbeispiel Versorgung und RS485-Bus mit zwei Modbus-Teilnehmern

- A (Klemme 1) an A bzw. D+ des Feldgeräts, B (Klemme 2) an B bzw. D−. Manche Hersteller bezeichnen die Adern anders oder haben A/B vertauscht. **Kommt keine Kommunikation zustande, zuerst A und B tauschen.**
- Verdrilltes, geschirmtes Kabel verwenden, zum Beispiel J-Y(St)Y 2×2×0,8. Schirm einseitig auf PE/Funktionserde.
- Bus als Linie verdrahten, keine Sterntopologie. Abschluss 120 Ω zwischen A und B an beiden Busenden; bei kurzen Leitungen unter 10 m und wenigen Teilnehmern meist entbehrlich.
- Bei langen Leitungen oder Teilnehmern mit eigener Versorgung eine Bezugsleitung von V− (Klemme 4) zum GND/COM des Feldgeräts führen.
- Jeder Teilnehmer braucht eine eindeutige Slave-ID (1–247). Baudrate, Datenbits, Parität und Stoppbits müssen bei allen Geräten gleich sein, zum Beispiel 9600 8N1.

8 Inbetriebnahme

8.1 SIM-Karte, Antenne, Spannung

1. **SIM vorbereiten.** Nano-SIM mit Datentarif. Empfehlung: SIM-PIN vorher in einem Smartphone deaktivieren. Bei IoT-/M2M-Karten den APN aus den Vertragsunterlagen bereitlegen.
2. **SIM einsetzen** im spannungslosen Zustand: Schutzabdeckung entfernen, Karte in den Schacht schieben, bis sie einrastet.
3. **Antenne** handfest an die SMA-Buchse ANT schrauben.
4. **Versorgung** nach Kapitel 7 verdrahten, Steckklemme aufstecken. **Kontrollpunkt:** LED PWR leuchtet. Nach etwa einer Minute ist der Router betriebsbereit.

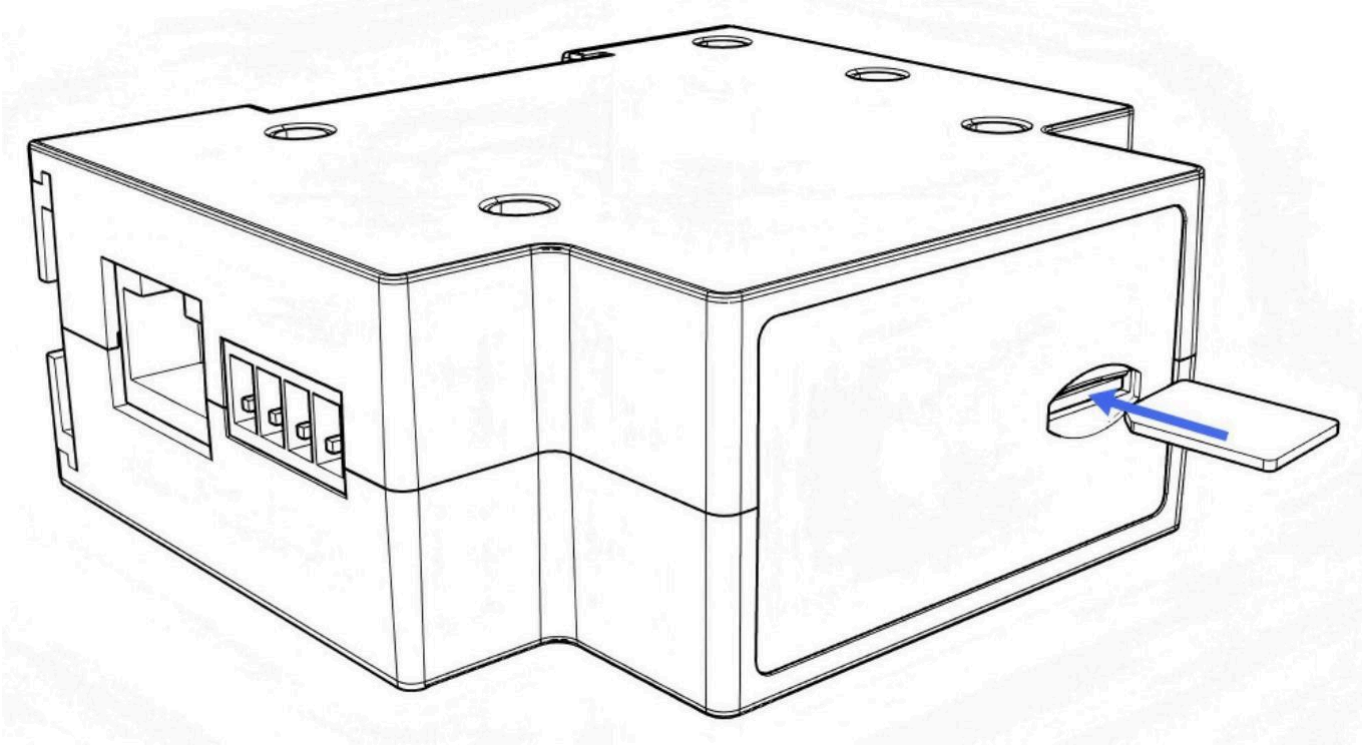


Abb. 09: Nano-SIM in den Schacht auf der Front schieben, bis sie einrastet

8.2 Zugang zur Weboberfläche

> **Den Router für die Einrichtung direkt verbinden, nicht über das Heimnetz.** Der Router hat sein eigenes Netz 192.168.8.x. Steckt er im Switch einer Fritzbox oder eines anderen Routers, ist er von dort aus nicht erreichbar, und sein DHCP-Server stört das Heimnetz. Was zu tun ist, wenn das bereits passiert ist, steht in Kapitel 15.



Abb. 10: Zugang für die Einrichtung: direkt am Router, nicht über das Heimnetz

Weg A: über das WLAN des Routers (empfohlen). Am Laptop oder Smartphone das WLAN `Wireless-2G-xxxxxx` vom Typenschild wählen und das WLAN-Passwort "**qwertyuiop**" eingeben. Es ist normal, dass das Gerät „kein Internet" meldet, solange die SIM noch nicht eingerichtet ist.

Weg B: über das Netzwerkkabel, direkt zum PC. Mitgeliefertes Kabel vom LAN-Anschluss des Routers direkt in den PC. Der PC muss auf „IP-Adresse automatisch beziehen" stehen (Windows-Standard). Nach

einigen Sekunden erhält der PC eine Adresse 192.168.8.x.

Kontrollpunkt: Eingabeaufforderung öffnen, `ipconfig` eingeben. Beim verwendeten Adapter steht eine IPv4-Adresse, die mit `192.168.8.` beginnt. Fehlt sie, siehe Kapitel 17.

8.3 Anmeldung

1. Browser öffnen und **`http://192.168.8.1`** eingeben, mit ausgeschriebenem `http://`. Manche Browser machen aus der bloßen Zahl eine Suchanfrage.
2. Mit Benutzername und Passwort vom Typenschild anmelden (Benutzer `admin`).
3. **Kontrollpunkt:** Die Startseite „Overview" erscheint mit Device Model `YZWK001WS-4G`, Seriennummer, Software Version und dem Block „Modem Information".

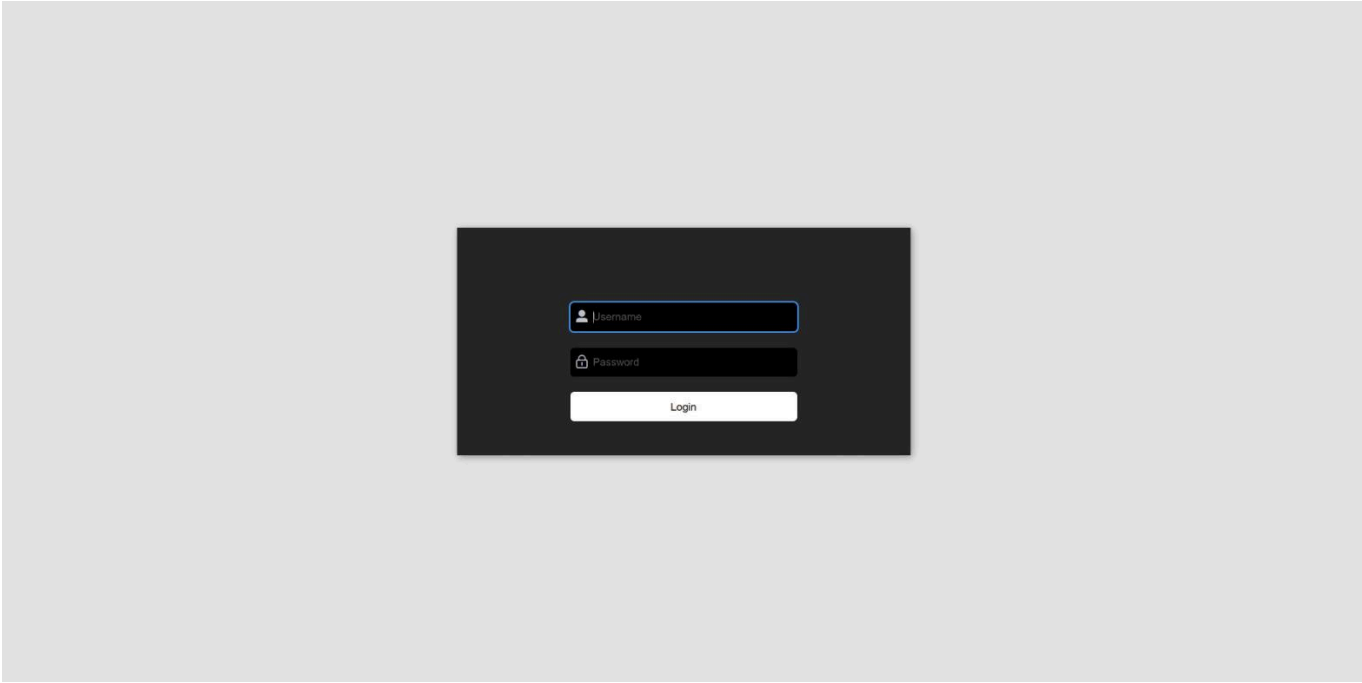


Abb. 11: Anmeldeseite der Weboberfläche

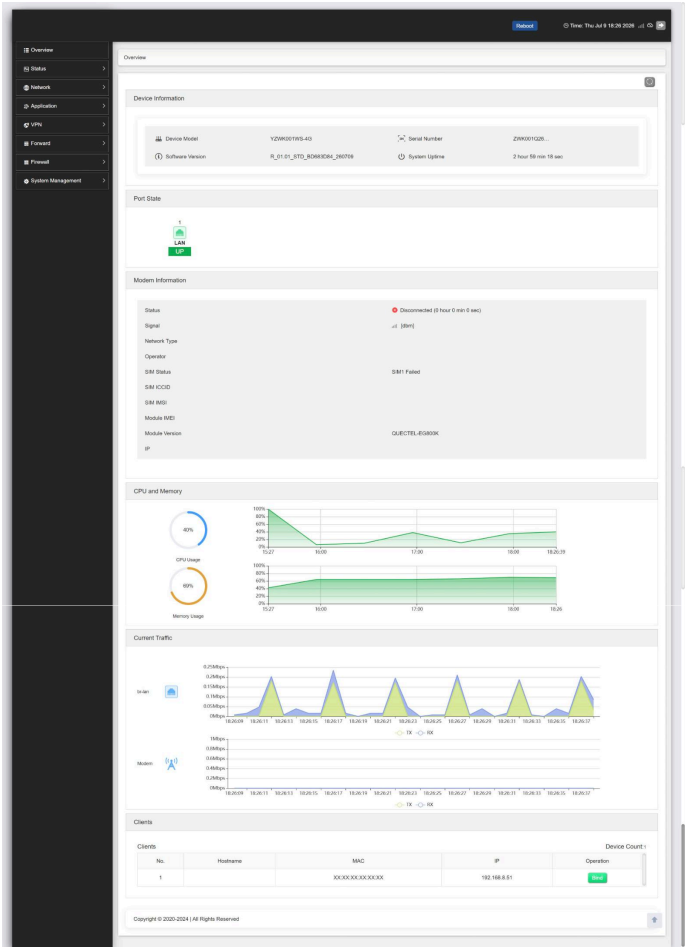


Abb. 12: Startseite Overview (hier noch ohne Mobilfunkverbindung, Status Disconnected)

Nach dreimaliger Falscheingabe sperrt die Anmeldung vorübergehend; die Wartezeit wird angezeigt.

9 Grundkonfiguration: Pflichtschritte nach der ersten Anmeldung

Die Oberfläche ist englisch. Jede Seite hat unten links **Save**; Änderungen gelten erst nach Save. Einige Schalter wirken sofort (NTP, Account-Enable, MASQ). Das Fragezeichen oben rechts öffnet den Hilfetext des Herstellers.

9.1 Sicherung des Werkszustands

System Management → Config Management → Backup. Die Datei auf dem PC ablegen. **Kontrollpunkt:** Download einer Konfigurationsdatei.

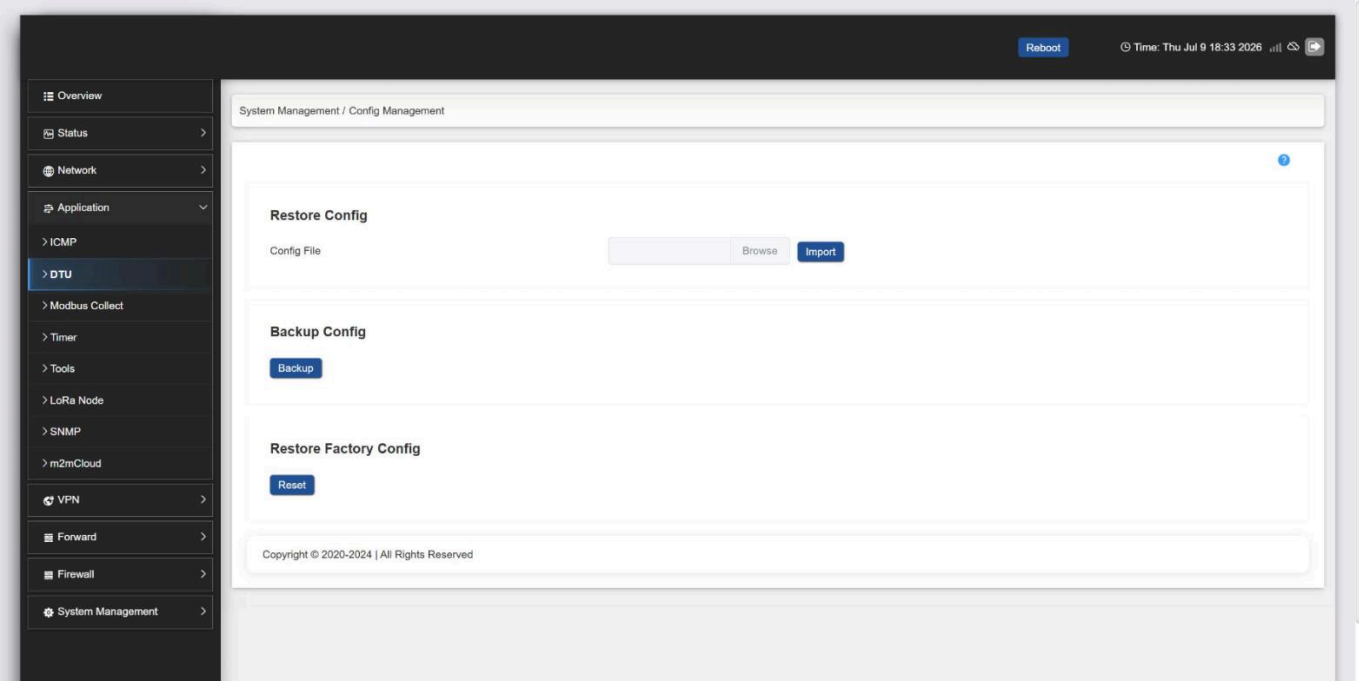


Abb. 29: System Management → Config Management: Import, Backup, Reset

9.2 Admin-Passwort ändern

System Management → **Account**, Zeile `admin` aufklappen, Password Change: altes Passwort, neues Passwort (mindestens 12 Zeichen; erlaubt sind Buchstaben, Ziffern und `@ . - _ :`), Bestätigung, Save. Optional den Schalter „Webpage idle exit (10 min)" einschalten (automatische Abmeldung). Neues Passwort in die Tabelle in Kapitel 3 eintragen.

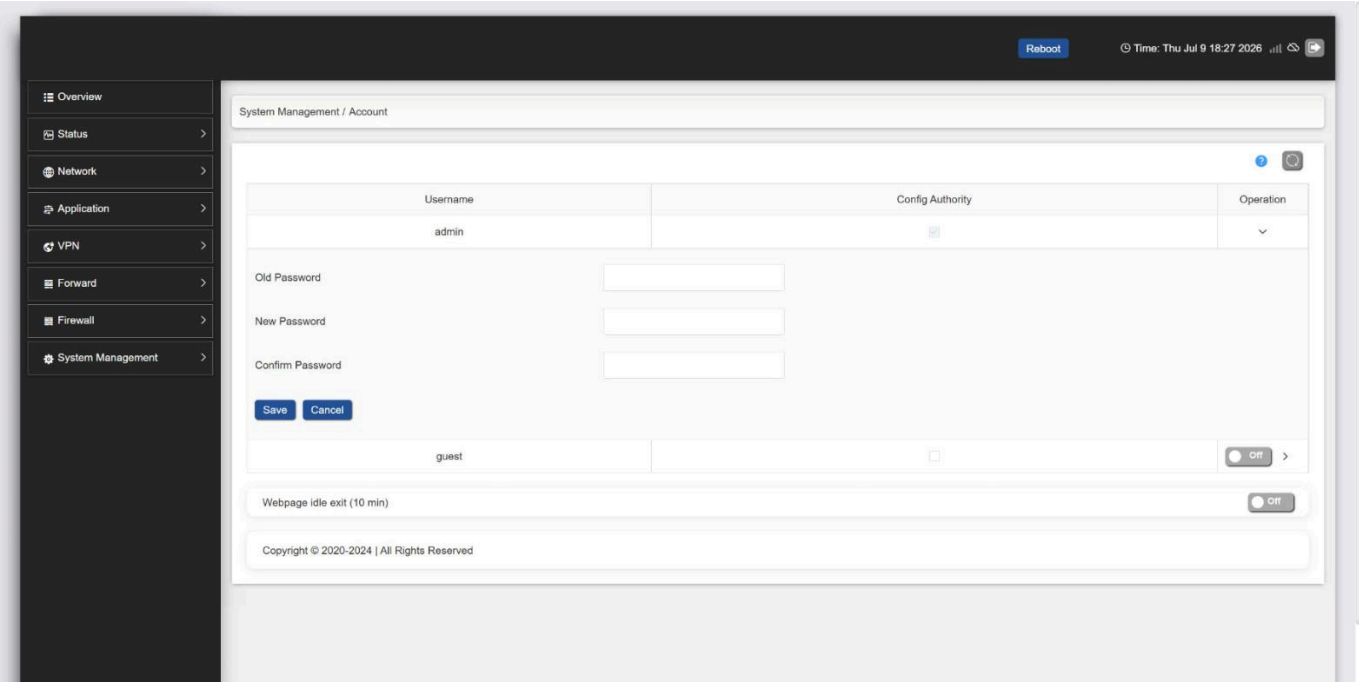


Abb. 13: System Management → Account, Zeile admin aufgeklappt

9.3 Fernzugriff auf die Oberfläche einschränken

Firewall → **Port Setting** → **Reiter Remote Access.** Im Werkszustand sind PING, WEB, SSH und CLI(TELNET) für LAN, **WAN** und VPN alle freigegeben. Damit wäre die Oberfläche aus dem Mobilfunknetz erreichbar. In der Spalte **WAN** die Häkchen bei **WEB, SSH und CLI** entfernen; PING kann bleiben. Save. Im

Reiter Port Setting bei Bedarf CLI Mode von `telnet` auf `ssh` stellen. **Kontrollpunkt:** Die Matrix zeigt in der WAN-Spalte nur noch PING.

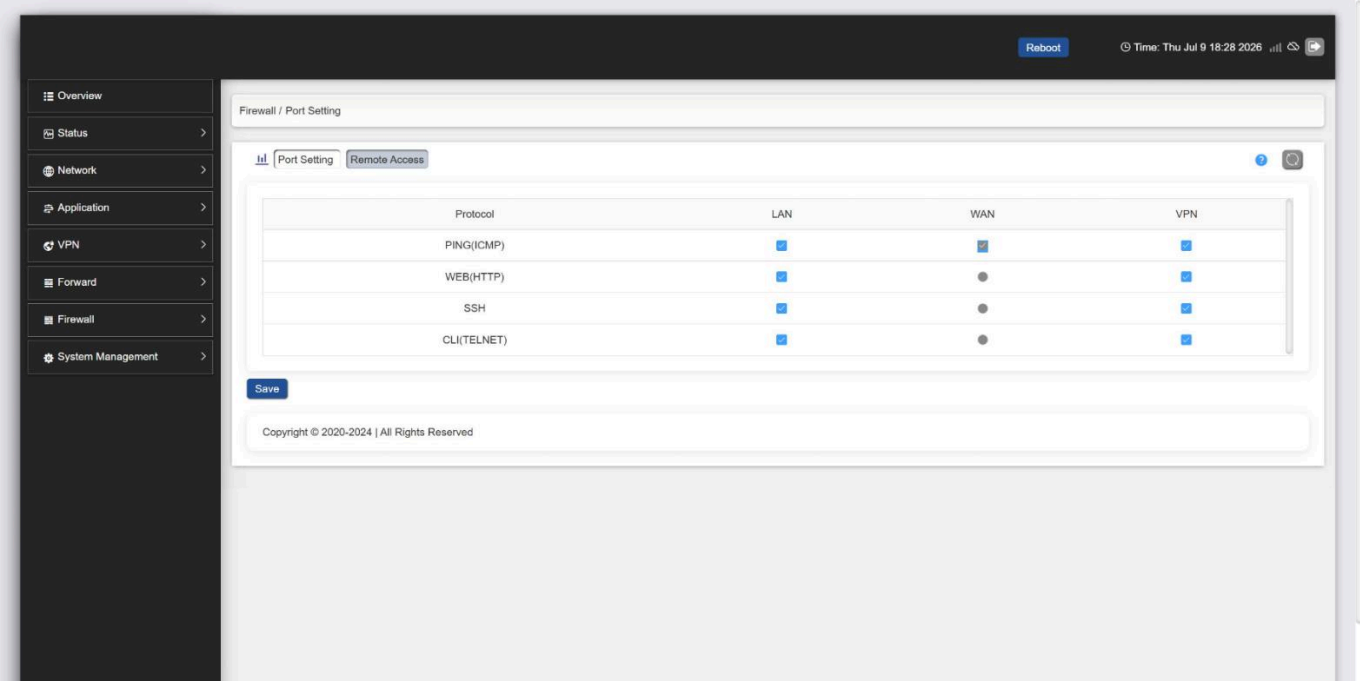


Abb. 14: Firewall → Port Setting → Remote Access im Zielzustand; abgewählte Felder zeigt die Oberfläche als graue Punkte

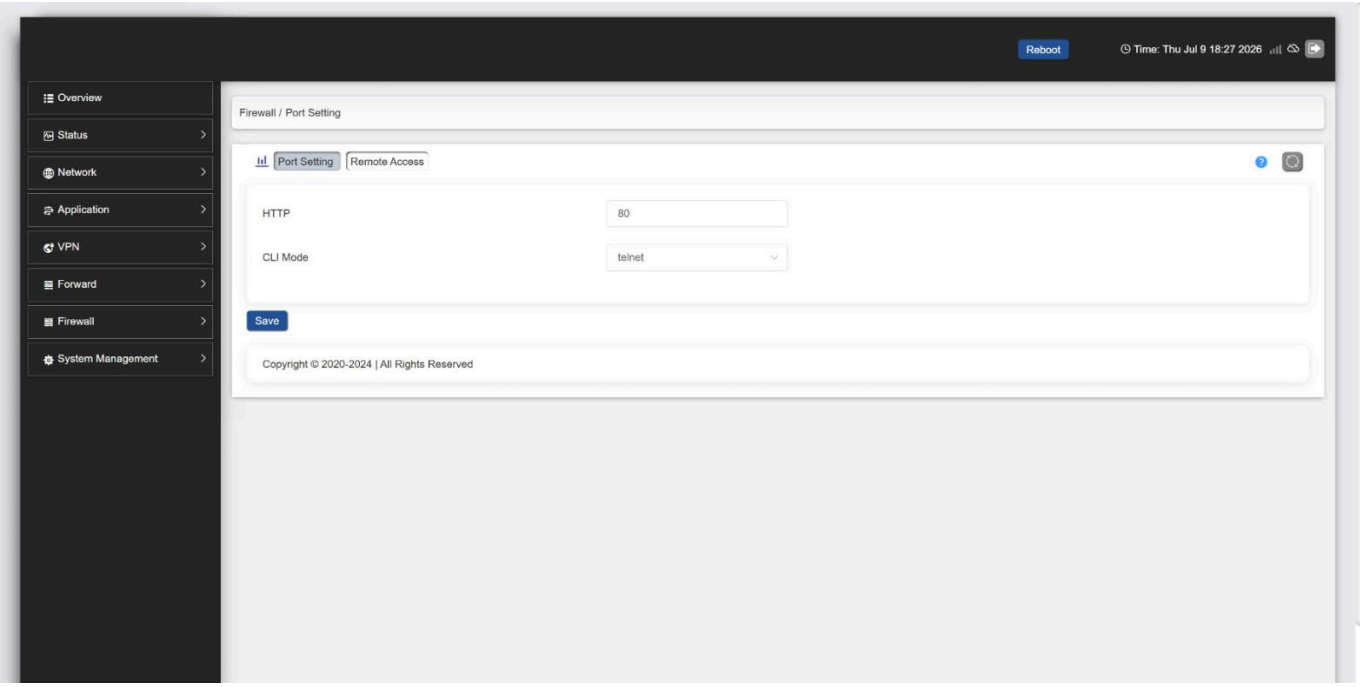


Abb. 14b: Reiter Port Setting mit HTTP-Port und CLI Mode

9.4 Hersteller-Cloud abschalten

Application → m2mCloud. Der Dienst ist werkseitig **On** und versucht dauerhaft, einen Server in Hongkong (`hk.ezulink.com`) zu erreichen. Wird er nicht ausdrücklich benötigt: Schalter oben rechts auf **Off**, Save. **Kontrollpunkt:** Im Log (System Management → Log, syslog) erscheinen keine neuen Meldungen „MQTT connect to server fail" mehr.

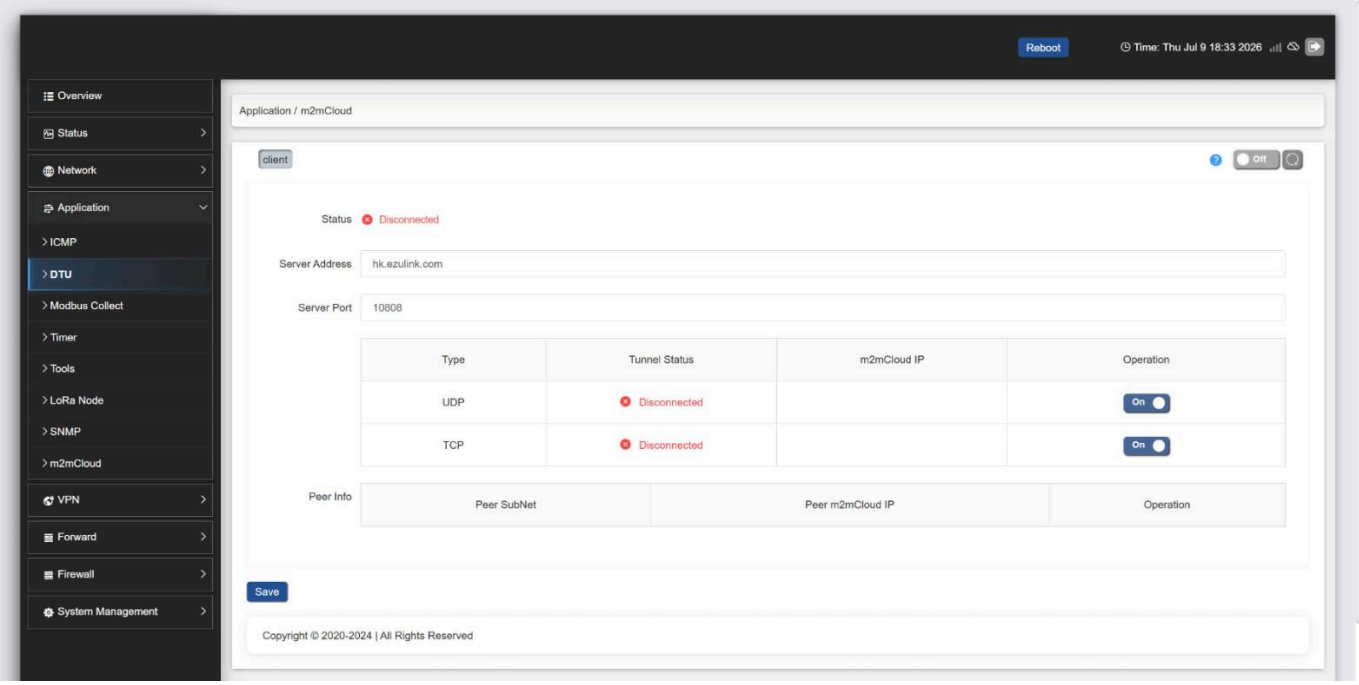


Abb. 28: Application → m2mCloud, Hauptschalter im Zielzustand Off

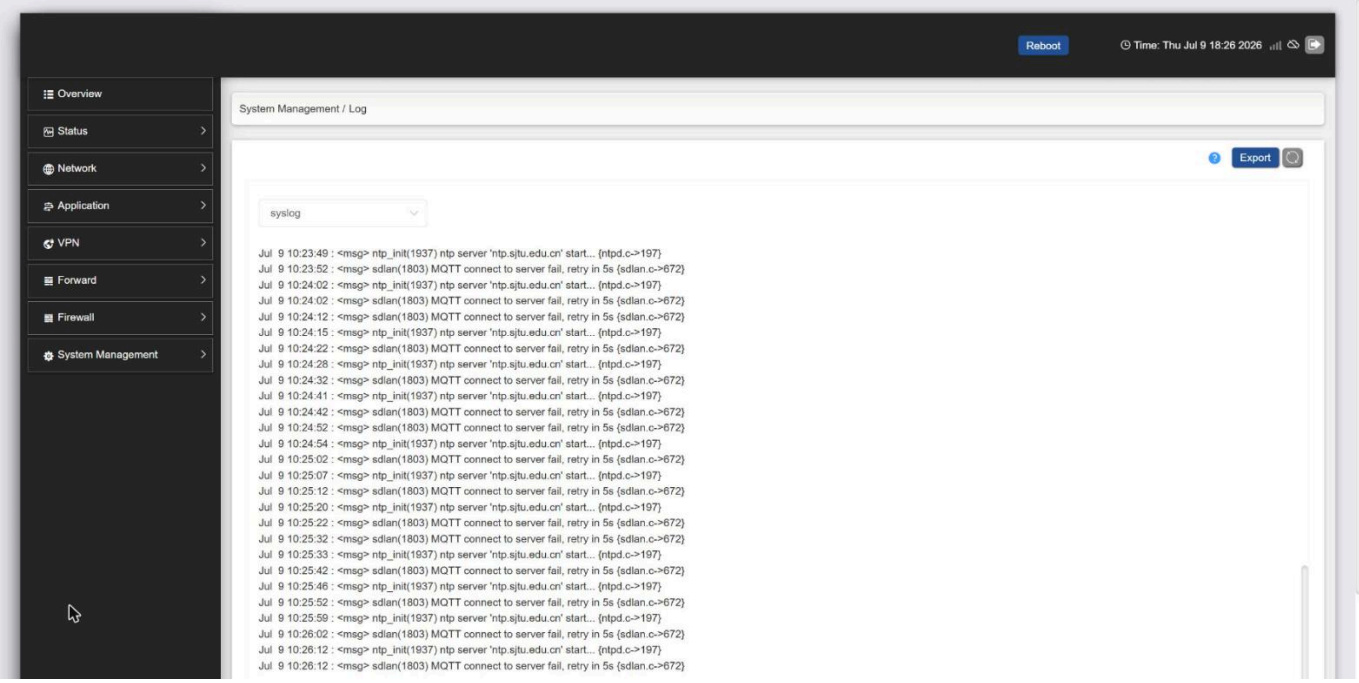


Abb. 30: System Management → Log mit Auswahl syslog/dmesg/modem

9.5 Uhrzeit und Zeitzone

System Management → System Time. Time Zone auf **„(UTC+01:00) Amsterdam/Paris/Berlin"**. Bei Main Server das Häkchen **Manual** setzen und `de.pool.ntp.org` eintragen, Backup Server `ptbtime1.ptb.de`, Interval 86400. NTP-Schalter On, Save. **Hinweis:** Die Firmware kennt keine automatische Sommerzeit. Zeitgesteuerte Aktionen (Timer) laufen im Sommer eine Stunde versetzt, sofern die Zeitzone nicht manuell auf UTC+2 umgestellt wird. **Kontrollpunkt:** State wechselt auf „Connected", sobald Mobilfunk steht (Kapitel 9.6). Die Uhrzeit in der Kopfzeile stimmt.

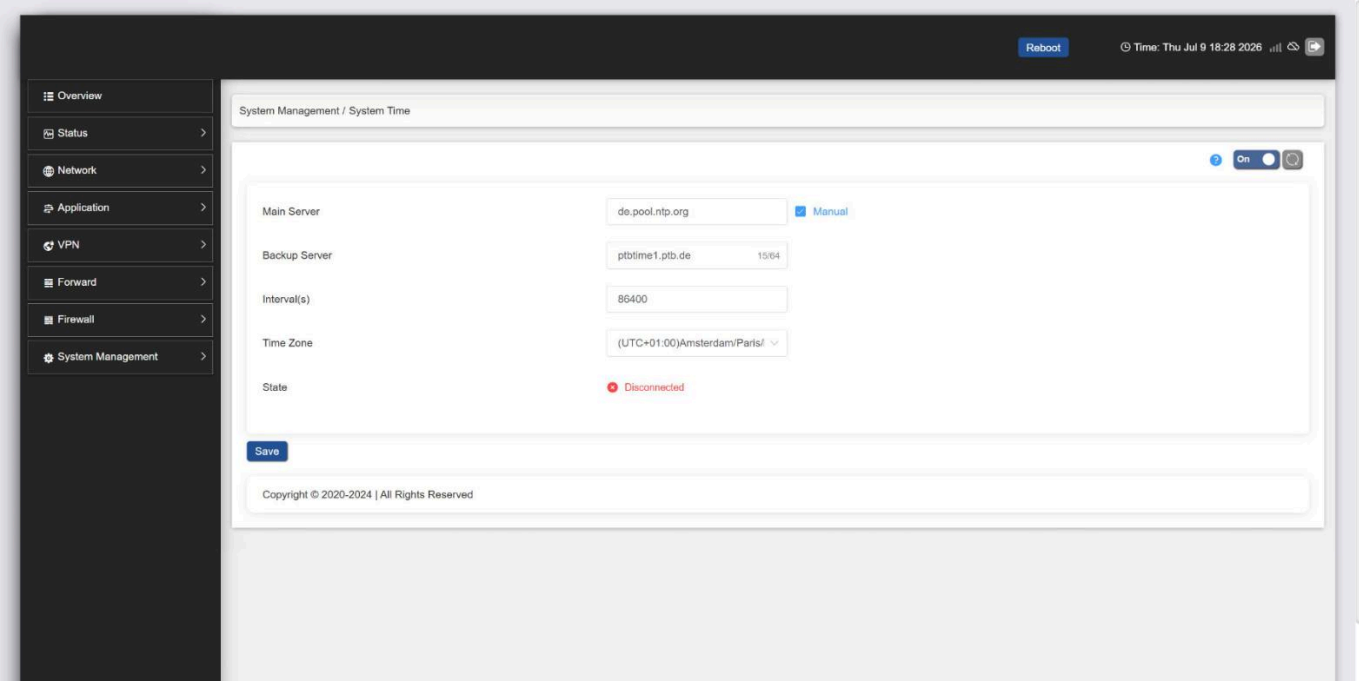


Abb. 15: System Time mit Zeitzone Berlin und manuellem NTP-Server

9.6 Mobilfunk und APN

Network → **Modem** → **Reiter Modem1**, in der Tabelle „PDP Setting" Regel 1 über den Pfeil aufklappen.

Feld	Eintrag
APN	leer lassen für Auto-APN; funktioniert das nicht, den APN des Anbieters eintragen (Beispiele: Telekom `internet.telekom`, Vodafone `web.vodafone.de`, o2 `internet`, 1NCE `iot.1nce.net`; immer mit den Vertragsunterlagen abgleichen)
Username / Password	nur wenn der Anbieter es verlangt
PIN	nur wenn die SIM-PIN noch aktiv ist
Auth	NONE oder PAP+CHAP
Protocol	IPv4
Network Type	AUTO oder 4G

OK, dann Save. Der Schalter in der Spalte Operation muss **On** sein. „False Link Detection" (600 s) eingeschaltet lassen.

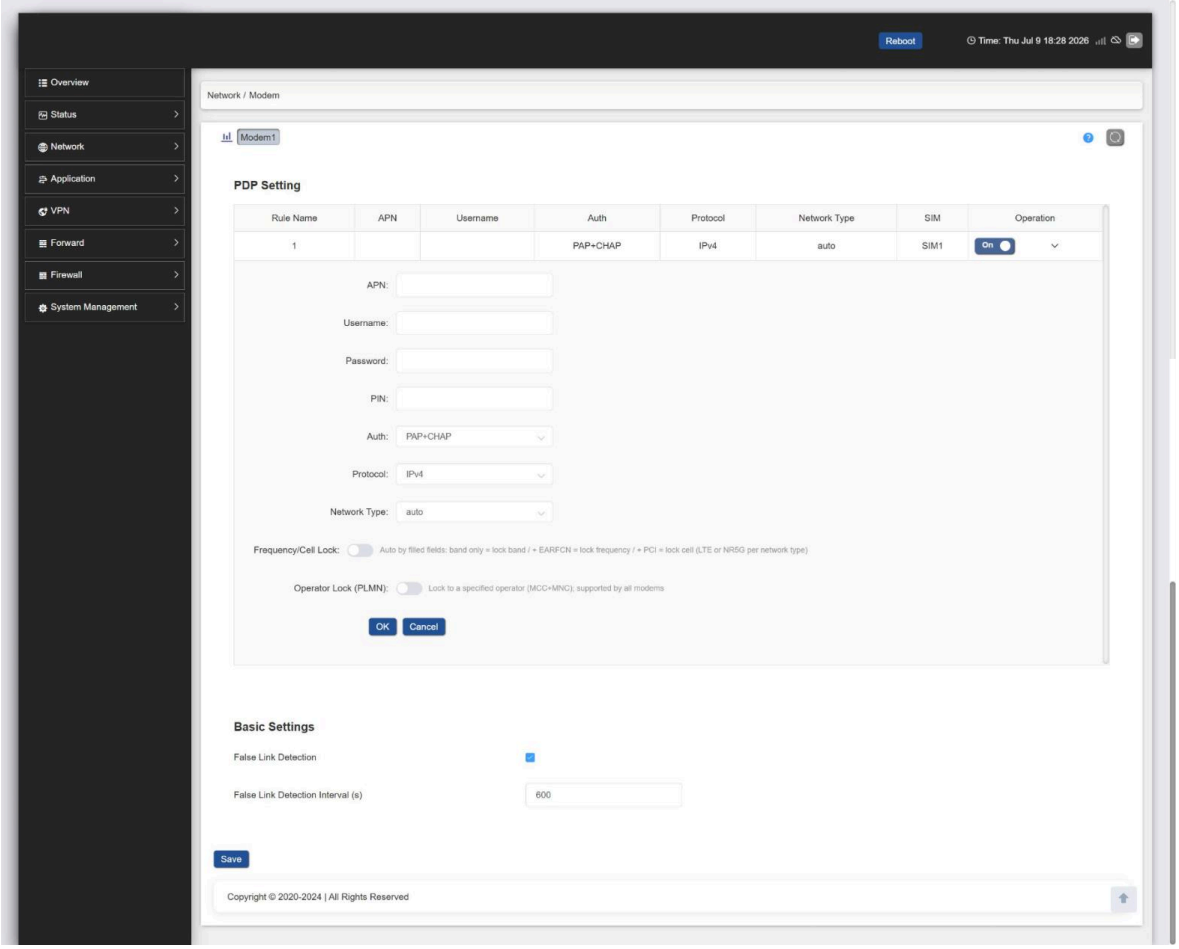


Abb. 16: Network → Modem, PDP-Profil 1 aufgeklappt

Kontrollpunkt: Unter **Overview** → **Modem Information** steht nach ein bis zwei Minuten Status **Connected**, Network Type LTE, SIM Status Ready, eine Signalstärke in dBm und eine IP-Adresse. Die LED NET zeigt Datenverbindung.

Signal (dBm)	Bewertung
besser als −85	gut
−85 bis −100	ausreichend
schlechter als −100	schwach, Antenne versetzen oder verlängern

9.7 Verbindungsüberwachung auf europäische Ziele stellen

Network → **Link Priority:** Das ICMP-Ziel steht werkseitig auf `223.5.5.5` (China). Auf `1.1.1.1` oder `8.8.8.8` ändern, Interval 10, Retry 2, Save. **Application** → **ICMP** (Watchdog für unbeaufsichtigten Betrieb): Add, Destination `8.8.8.8`, Backup `1.1.1.1`, Interval 60, Retry 5, Source Interface `Modem`, Action `Modem-reset`, Save. Der Watchdog startet 180 s nach dem Booten. **Kontrollpunkt:** Unter Link Priority zeigt der Status des Modems grün.

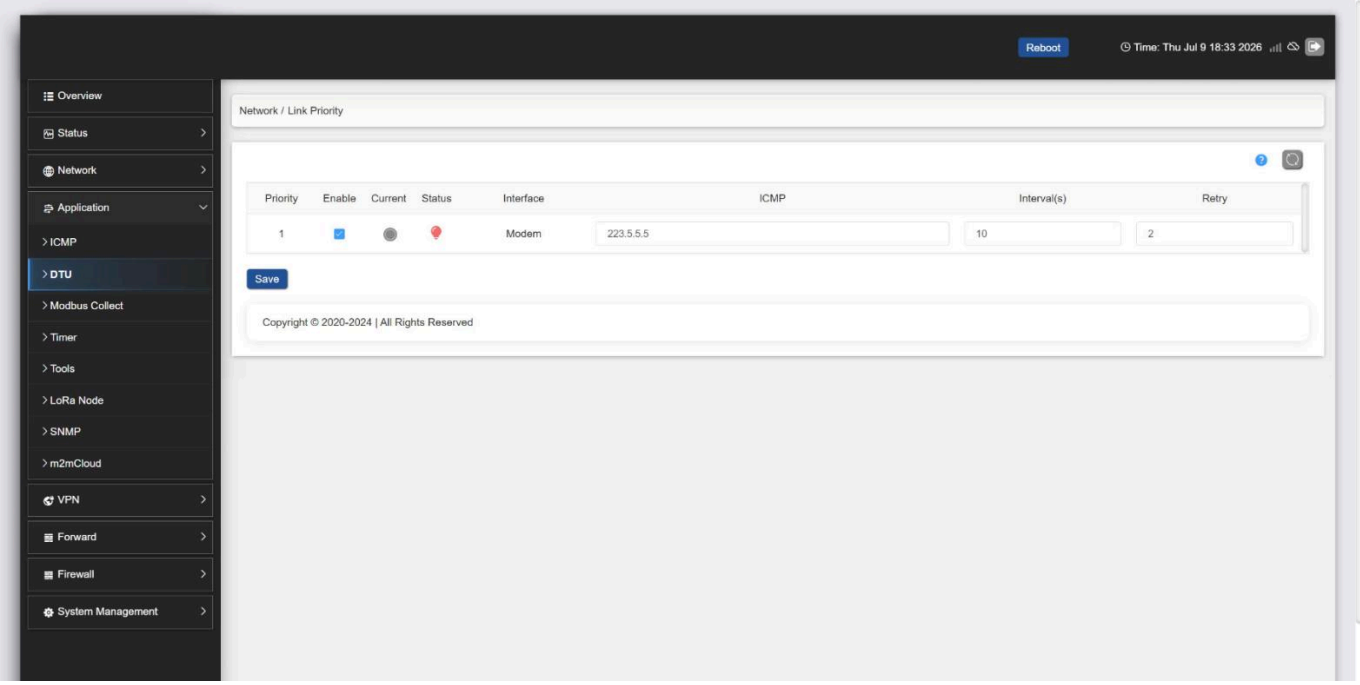


Abb. 26: Network → Link Priority (Werkszustand mit ICMP-Ziel 223.5.5.5, Status rot ohne Mobilfunk)

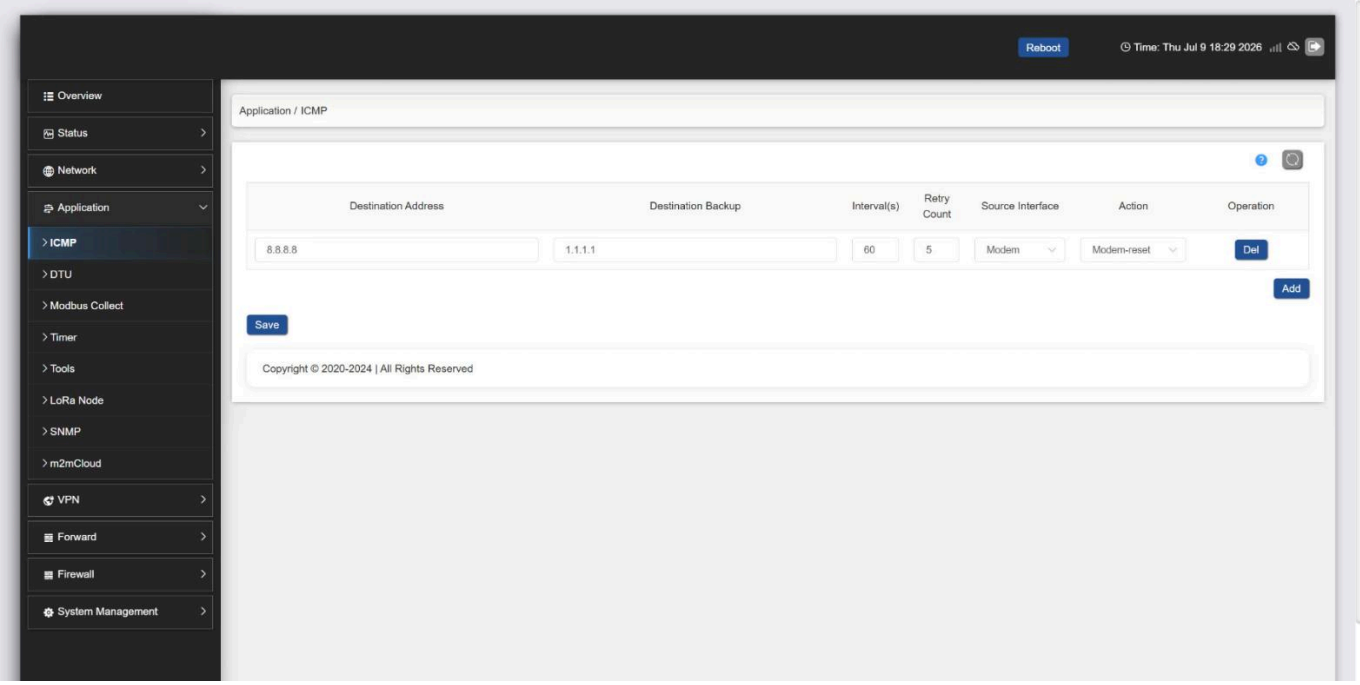


Abb. 27: Application → ICMP, Watchdog-Regel mit Modem-reset

9.8 WLAN absichern

Network → WIFI2.4G. Eigene SSID und ein neues Passwort (8–32 Zeichen) vergeben, Security Mode WPA2, Cipher AES, Save. Wer das WLAN nicht braucht, schaltet es nach Abschluss aller Einstellungen mit dem Schalter oben rechts auf Off. **Achtung:** Nach dem Speichern bricht die WLAN-Verbindung ab. Mit der neuen SSID neu verbinden. Mode bleibt **AP**; der Modus **Station** schaltet das eigene WLAN ab (Kapitel 13.3).

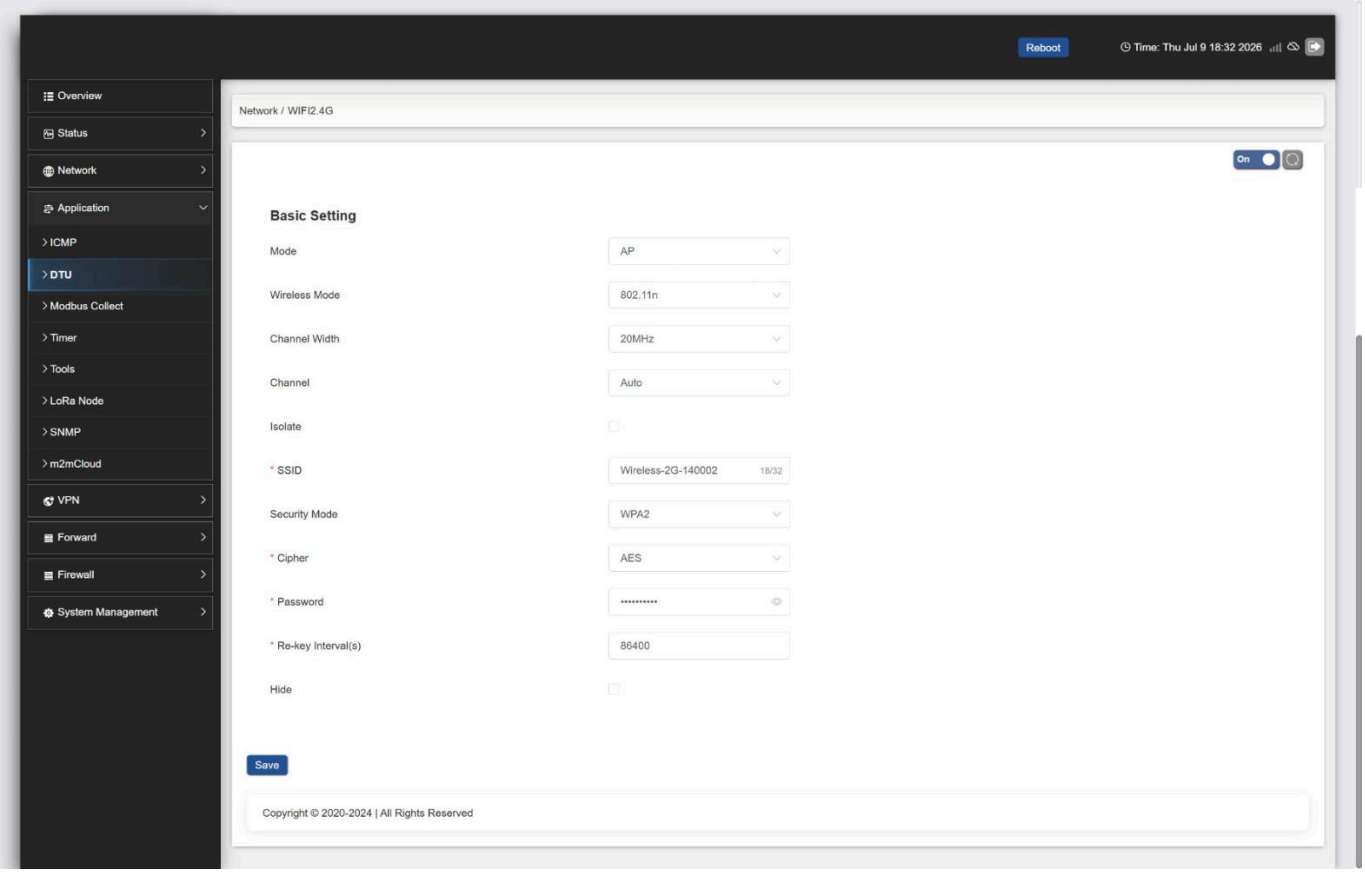


Abb. 25: Network → WIFI2.4G im AP-Modus

9.9 Erneut sichern

Backup nach Kapitel 9.1 wiederholen. Damit ist die Grundkonfiguration abgeschlossen. Weiter mit Kapitel 11 (RS485) und dem gewählten Zielbild.

10 Die Weboberfläche im Überblick

```
Overview            Startseite: Gerät, Port-Status, Modem, CPU/RAM, Datenverkehr,
verbundene Clients
Status              LAN | WIFI2.4G | Modem | Route Table
Network             LAN | WIFI2.4G | Modem | DHCP | Link Priority
Application         ICMP | DTU | Modbus Collect | Timer | Tools | LoRa Node | SNMP |
m2mCloud
VPN                 WireGuard | ZeroTier | IPsec | L2TP Client | L2TP Server | OPENVPN
Client | OPENVPN Server
Forward             NAT | Static Route | MASQ
Firewall            Port Setting | SPI Filter | Address Filter | Domain Filter
System Management   Log | System Time | Account | Config Management | Upgrade
```

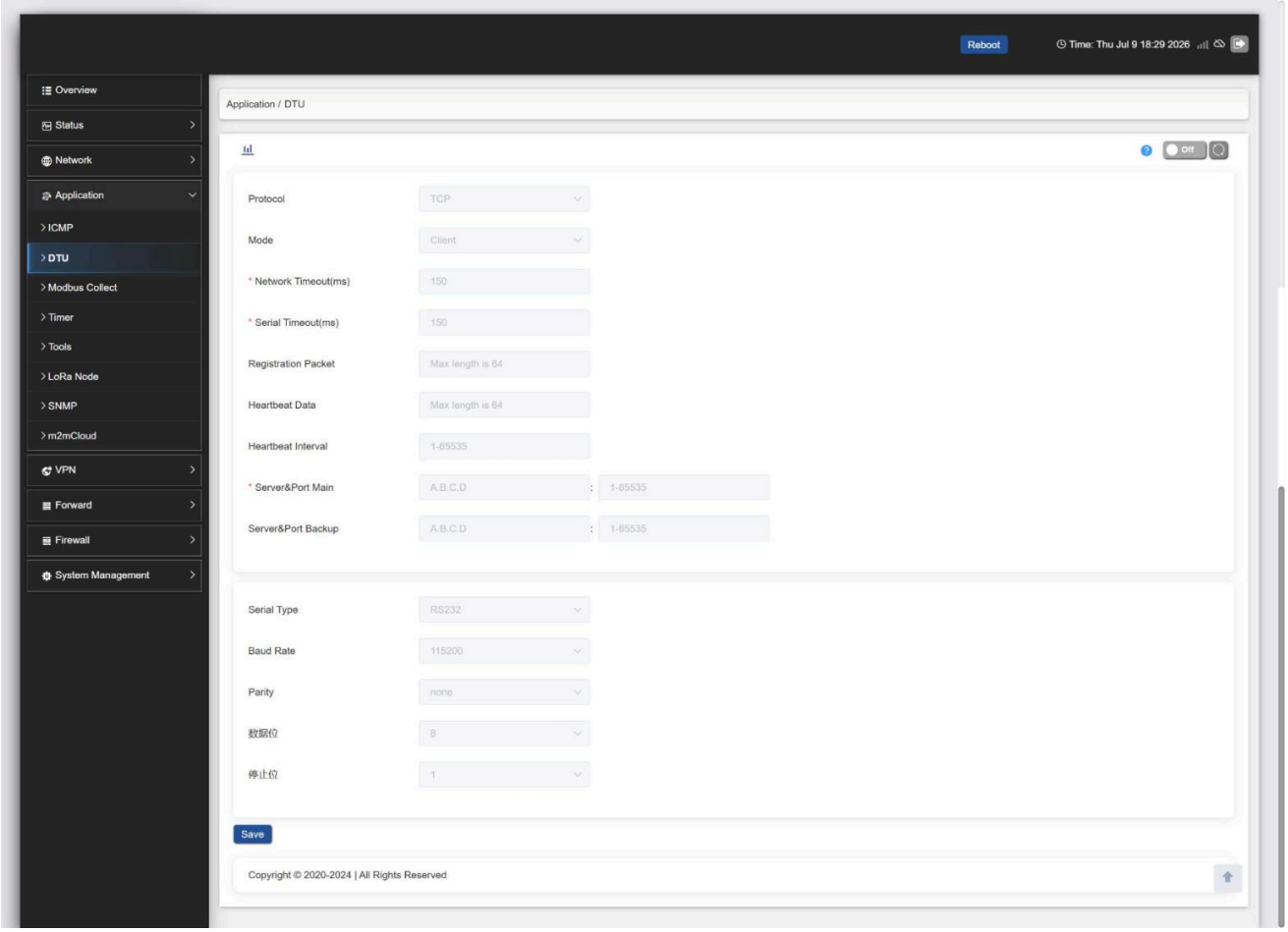


Abb. 17: Aufbau einer Dienstseite: Menü links, Hauptschalter und Fragezeichen oben rechts, Save unten links

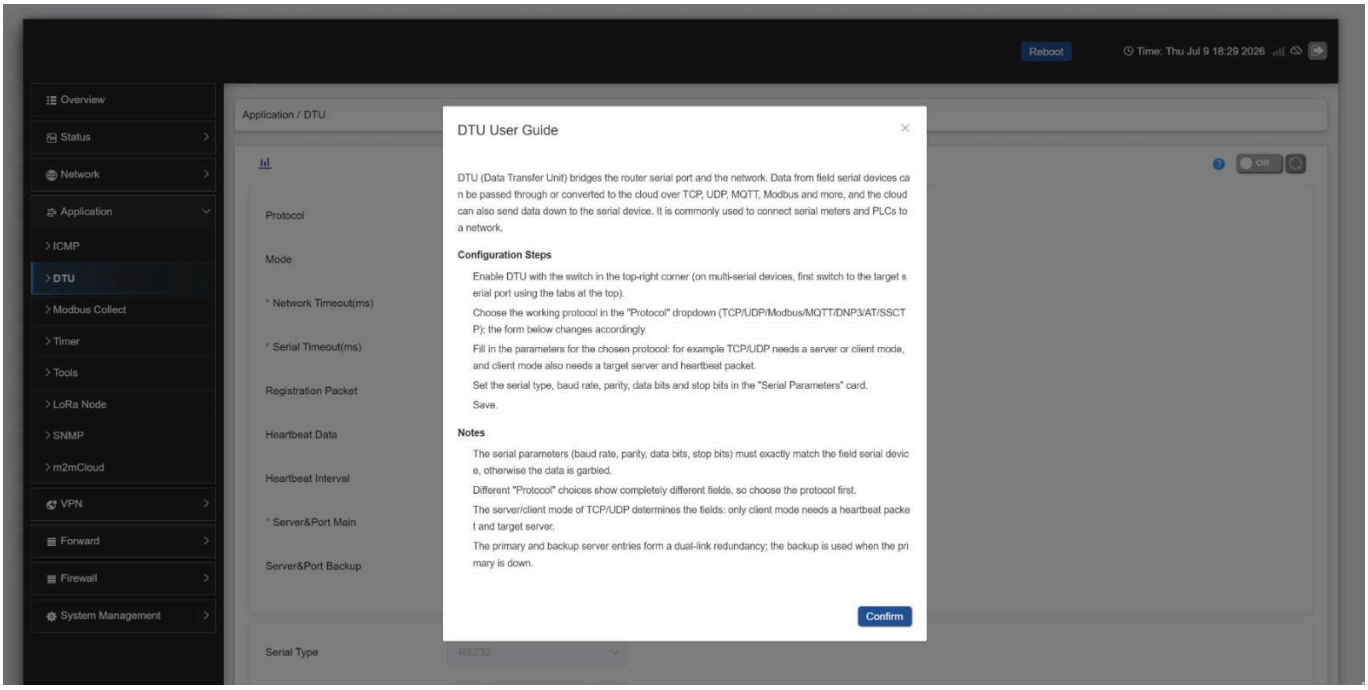


Abb. 17b: Hilfetext des Herstellers nach Klick auf das Fragezeichen

Bedienlogik: Linke Menüleiste, immer nur ein Hauptmenü geöffnet. Dienste haben oben rechts einen On/Off-Hauptschalter; bei Off sind die Felder ausgegraut. Seiten können per Direktlink aufgerufen werden, zum Beispiel `http://192.168.8.1/#/Application/ModbusCollect`. Oben rechts in der Kopfzeile: Reboot, Uhrzeit, Signalbalken. Zwei Beschriftungen auf den Seriell-Seiten sind nicht übersetzt: **数据位 = Datenbits, 停止位 = Stoppbits.**

11 RS485/Modbus einrichten

11.1 Betriebsart wählen

Die serielle Schnittstelle kann nur von **einem** Dienst benutzt werden: entweder **DTU** oder **Modbus Collect**. Beide gleichzeitig ist nicht möglich.

Sie wollen …	Betriebsart	Kapitel
Home Assistant, Node-RED oder eine Leitstelle sollen die RS485-Geräte **selbst per Modbus TCP** abfragen	**A: DTU, Modbus-TCP-Gateway**	11.2
Der Router soll die Register **selbst abfragen** und die Werte per **MQTT** senden; keine Modbus-Konfiguration im Zielsystem	**B: Modbus Collect, MQTT**	11.3
Rohdaten eines seriellen Geräts (kein Modbus) an einen Server tunneln	DTU, TCP/UDP Client	Herstellerhilfe
Leitsystem mit IEC 60870-5-104	Modbus Collect, IEC104	Herstellerhilfe

Für Zielbild 1 (Cloud-MQTT) ist **B** die passende Betriebsart. Für Zielbild 2 (Home Assistant) funktionieren A und B; A ist einfacher, wenn Sie Modbus-Registerlisten in Home Assistant pflegen wollen, B ist einfacher, wenn Sie lieber MQTT-Sensoren anlegen.

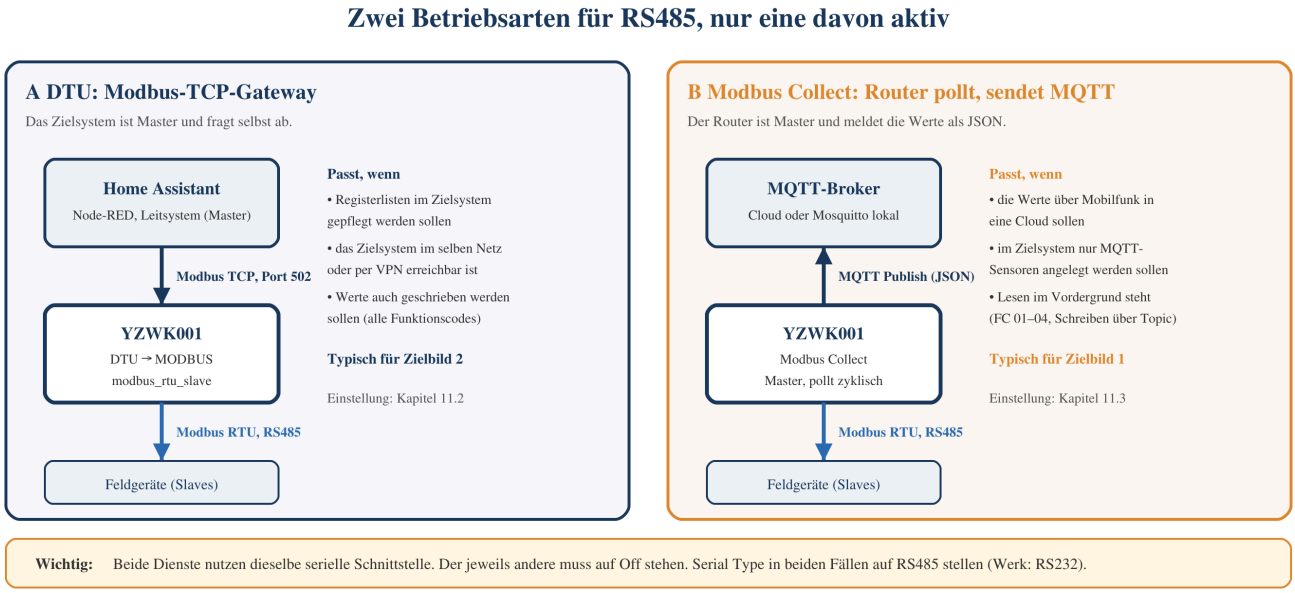


Abb. 18: Zwei Betriebsarten für RS485: DTU als Modbus-TCP-Gateway oder Modbus Collect mit MQTT

11.2 Betriebsart A: Modbus-TCP-Gateway (DTU)

Der Router nimmt Modbus-TCP-Anfragen aus dem Netz an und gibt sie als Modbus RTU auf den RS485-Bus. Die RS485-Geräte sind Slaves, das Zielsystem ist Master.

Application → DTU:

1. Protocol: **MODBUS**.
2. Serial Modbus Working Mode: **modbus_rtu_slave** (Router ist Modbus-TCP-Server).
3. Modbus Local Port: **502**.
4. Network Timeout und Serial Timeout: 150 ms belassen; bei langsamen Geräten Serial Timeout auf 300–500 ms erhöhen.

5. Serial Parameters: Serial Type **RS485**, Baud Rate, Parity, Datenbits (数据位), Stoppbits (停止位) exakt wie am Feldgerät, zum Beispiel 9600 / none / 8 / 1.
6. Hauptschalter oben rechts **On**, Save.

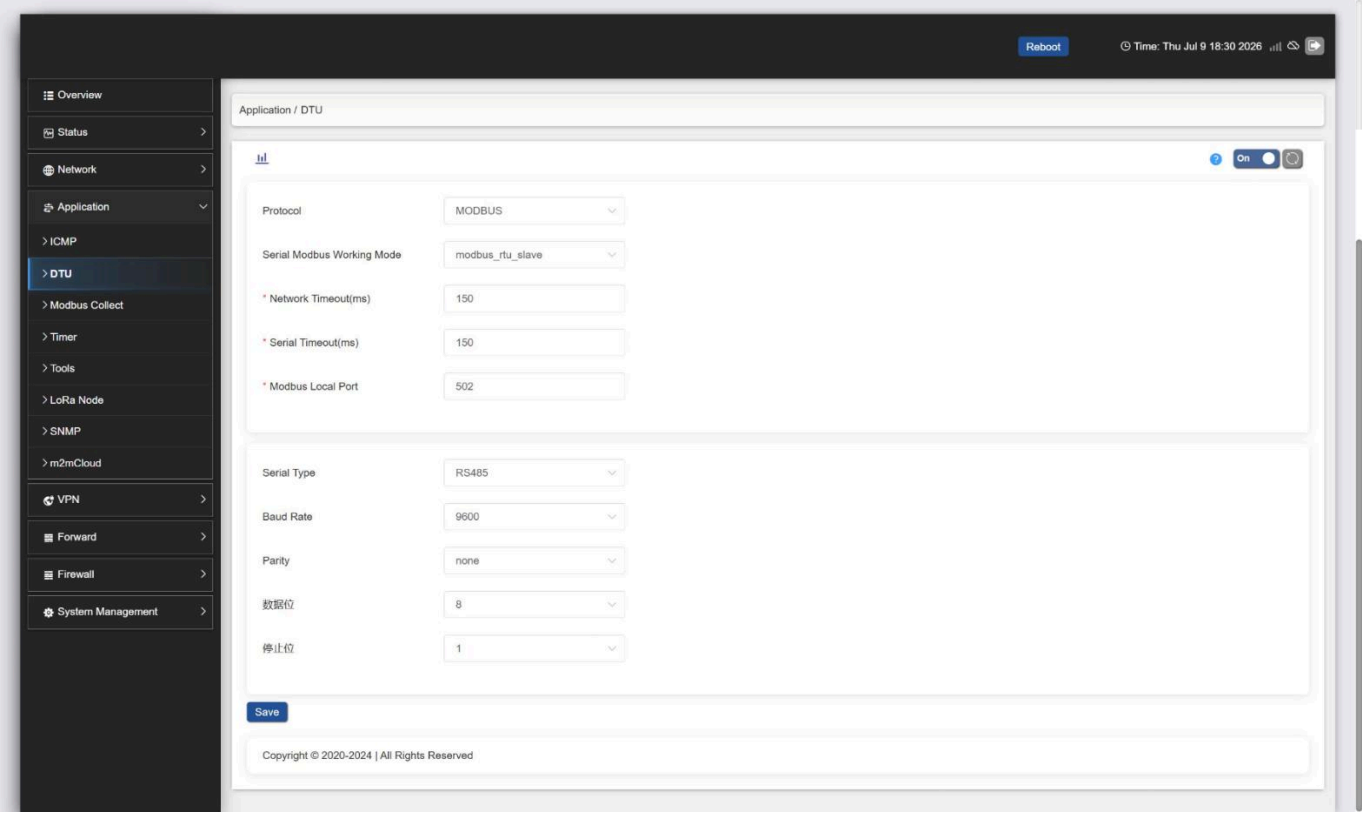


Abb. 19: Application → DTU als Modbus-TCP-Gateway: MODBUS, modbus_rtu_slave, Port 502, RS485 9600 8N1

Kontrollpunkt: Von einem PC im selben Netz mit einem Modbus-Testprogramm (zum Beispiel „Modbus Poll", „QModMaster" oder „mbpoll") eine Verbindung zu `192.168.8.1:502`, Unit-ID = Slave-ID des Geräts, Funktion 03, Register lesen. Es kommen plausible Werte. Timeout oder Fehler: Kapitel 17, Abschnitt Modbus.

Bei Modbus Collect muss der Hauptschalter **Off** sein, sonst ist die Schnittstelle belegt.

11.3 Betriebsart B: Modbus Collect mit MQTT

Der Router fragt die Register selbst zyklisch ab und sendet die Werte als JSON an einen MQTT-Broker.

Application → Modbus Collect:

Schritt 1, Global Config:

Feld	Eintrag
Report Method	MQTT
MQTT Server : Port	Adresse und Port des Brokers (Zielbild 1: Broker im Internet, Zielbild 2: Mosquitto im Heimnetz), Port 1883; mit TLS 8883 und Zertifikat (Feld MQTT CA)
Username / Password	MQTT-Zugangsdaten
Report Rate (s)	Sendeintervall, praxisgerecht 10–60 s (kürzer erhöht Datenvolumen)
Response Timeout (ms)	1000

Schritt 2, Gerät anlegen: Add Device.

Feld	Eintrag
Connection	RTU (Serial)
Serial	RS485
Baud / Parity / Data Bits / Stop Bits	wie am Feldgerät, zum Beispiel 9600 / none / 8 / 1
Publish Topic	zum Beispiel `anlage/heizraum/regler`
Subscribe Topic	zum Beispiel `anlage/heizraum/regler/set` (nur für Schreibbefehle)

Schritt 3, Datenpunkte anlegen: im Gerätedialog Add Command, je Register ein Eintrag.

Feld	Eintrag
Command Name	Name des Werts, erscheint als Schlüssel im JSON, zum Beispiel `istwert`
Slave Address	Slave-ID des Geräts
Function Code	03 Holding Register oder 04 Input Register (laut Registerliste des Herstellers)
Register Start	Registeradresse 0-basiert. Nennt die Herstellerliste „40003" oder „Register 3 (1-basiert)", hier 2 eintragen
Register Quantity	1 bei 16-Bit-Werten, 2 bei 32-Bit-Werten
Data Type	Unsigned 16bit, Signed 16bit, Float ABCD usw. Falsche Wortfolge erzeugt unsinnige Werte, dann CDAB oder DCBA probieren
Writable	Yes nur, wenn der Wert per MQTT geschrieben werden soll
Poll Interval (ms)	1000–10000

OK, Save im Gerätedialog, dann Hauptschalter oben rechts **On**, Save.

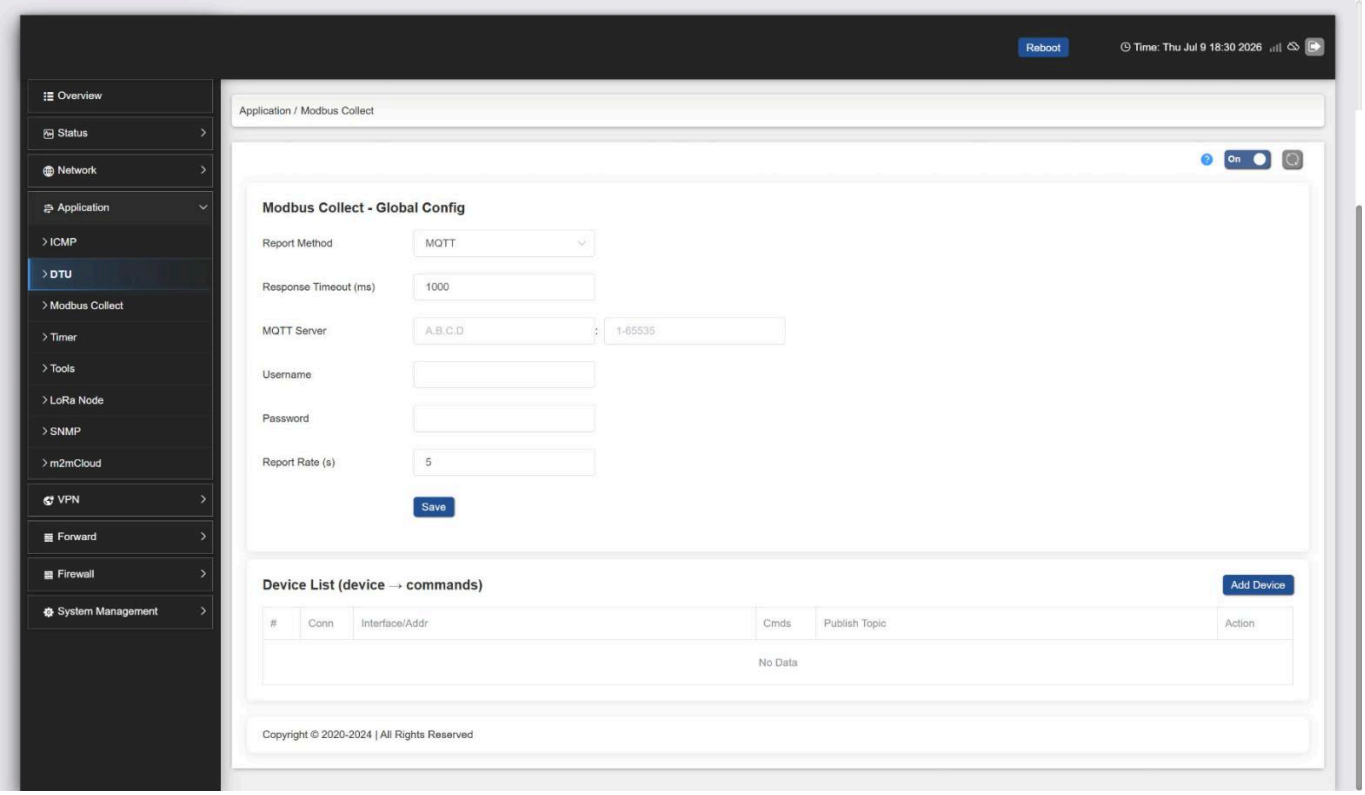


Abb. 20: Application → Modbus Collect, Global Config mit Report Method MQTT

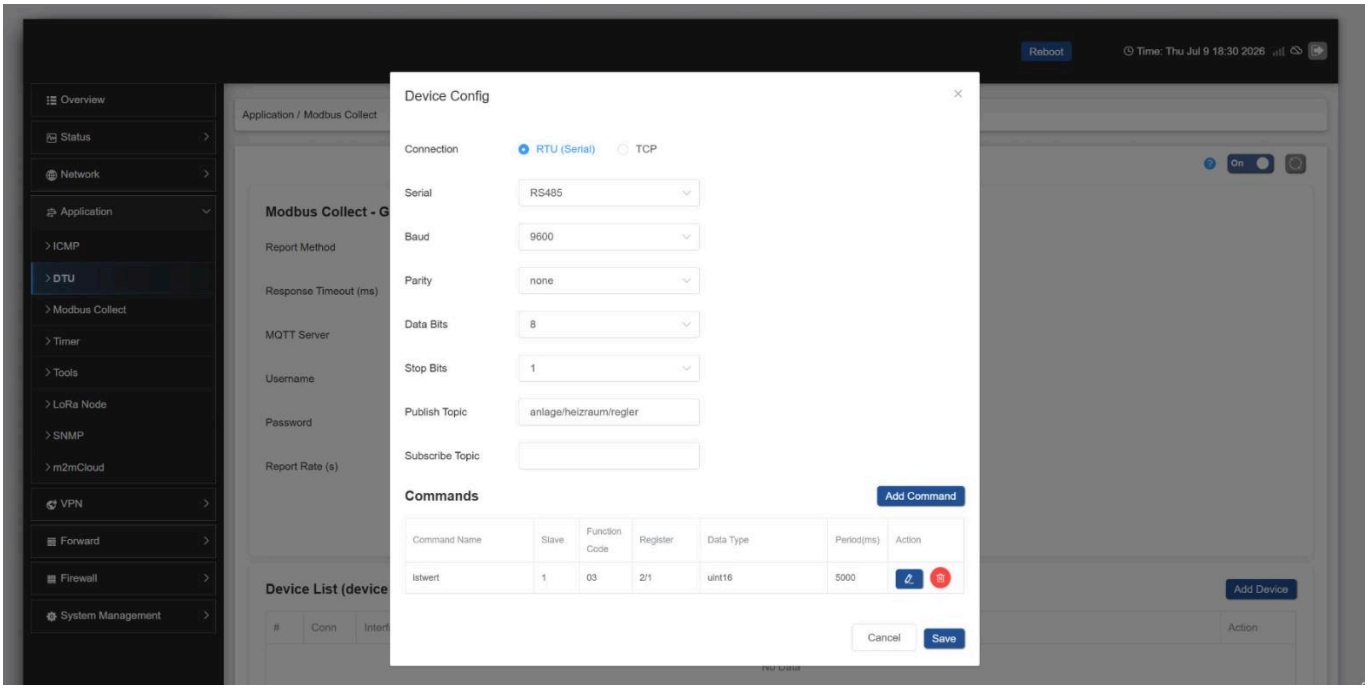


Abb. 21: Dialog Device Config mit Beispiel-Datenpunkt istwert

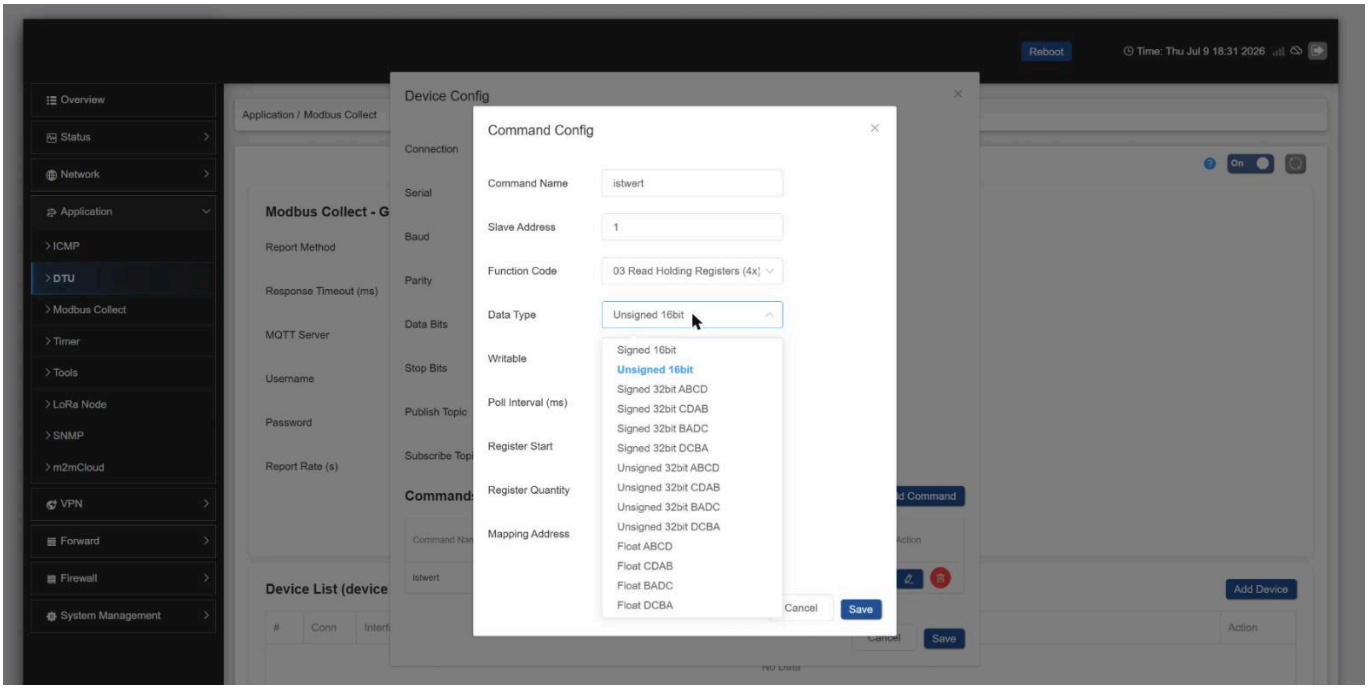


Abb. 21b: Dialog Command Config mit den wählbaren Datentypen und Wortfolgen

Kontrollpunkt: Mit einem MQTT-Programm (zum Beispiel „MQTT Explorer") am Broker anmelden und das Publish Topic abonnieren. Alle Report-Rate-Sekunden erscheint ein JSON mit den Command Names als Schlüsseln. Das genaue Format übernehmen Sie für die Sensor-Definitionen (Kapitel 12.3 und 13.5).

Bei DTU muss der Hauptschalter **Off** sein.

11.4 Registerangaben richtig lesen

- Modbus zählt Register ab 0. Hersteller schreiben oft 1-basiert oder mit Präfix (30001 = Input Register 0, 40001 = Holding Register 0). Im Zweifel beide Varianten testen.
- 32-Bit-Werte belegen zwei Register. Die Reihenfolge der Worte (ABCD, CDAB) ist herstellerabhängig.
- Ein Wert von 32767 oder 65535 bedeutet bei vielen Geräten „Fühler offen" oder „ungültig".
- Herstellertabellen passen nicht immer zur gelieferten Firmware des Feldgeräts. Werte am Gerätedisplay gegenprüfen (Anhang C).

12 Zielbild 1: Anlage ohne Festnetz

Der Router hängt nur an Mobilfunk. Die Modbus-Werte gehen per MQTT an einen Broker im Internet. Der Fernzugriff läuft über VPN, weil Mobilfunk-SIM-Karten in der Regel eine private Adresse hinter dem Netz des Anbieters erhalten (Carrier-Grade-NAT) und von außen nicht direkt erreichbar sind.

12.1 Voraussetzungen

- Kapitel 8, 9 und 11.3 abgeschlossen, Modem „Connected".
- Ein MQTT-Broker, der aus dem Internet erreichbar ist: eigener Server (Mosquitto), ein Cloud-Dienst oder ein Home Assistant, der über VPN erreichbar ist. Zugangsdaten und, bei TLS, das CA-Zertifikat bereithalten.

12.2 Datenweg einrichten

1. Modbus Collect nach Kapitel 11.3 mit der Broker-Adresse im Internet, Port 1883 oder 8883 (TLS).

2. Report Rate 30–60 s wählen, um Datenvolumen zu sparen. Richtwert: ein Gerät mit zehn Datenpunkten alle 30 s erzeugt etwa 30–60 MB pro Monat.
3. **Kontrollpunkt:** MQTT-Programm am Broker zeigt die Werte.

12.3 Werte in Home Assistant anzeigen (Broker erreichbar)

Beispiel für `configuration.yaml`, Schlüssel an das tatsächliche JSON anpassen:

```
mqtt:
  sensor:
    - name: "Regler Istwert"
      unique_id: yzwk001_regler_istwert
      state_topic: "anlage/heizraum/regler"
      value_template: "{{ value_json.istwert | float(0) / 10 }}"
      unit_of_measurement: "°C"
      device_class: temperature
      state_class: measurement
```

Teiler und Einheit laut Registerliste des Feldgeräts (viele Regler liefern Zehntelgrad).

12.4 Fernzugriff

Nach Kapitel 14 WireGuard oder ZeroTier einrichten. Danach sind Weboberfläche (`http://192.168.8.1`) und, bei Betriebsart A, das Modbus-TCP-Gateway (Port 502) über den Tunnel erreichbar.

12.5 Betriebssicherheit

- ICMP-Watchdog (Kapitel 9.7) aktiv.
- Optional **Application** → **Timer**: wöchentlicher Neustart, zum Beispiel Sonntag 03:00, Event reboot (setzt NTP-Sync voraus).
- Backup der fertigen Konfiguration (Kapitel 16.2).

13 Zielbild 2: Anlage im Heimnetz mit Home Assistant

Der Router hängt per Netzwerkkabel dauerhaft im Heimnetz (Fritzbox, Speedport oder ähnliches). Home Assistant liest die Werte lokal, ohne Cloud. Das Internet des Routers kommt weiterhin aus dem Mobilfunk; das Heimnetz nutzt er nur lokal.

13.1 Das Problem und die Lösung

Der Router bringt sein eigenes Netz 192.168.8.x und einen DHCP-Server mit. Im Heimnetz (zum Beispiel 192.168.1.x oder 192.168.178.x) ist er damit unsichtbar und stört die Adressvergabe. Die Firmware hat keinen WAN-Modus für den Ethernet-Port. Die saubere Lösung: Der Router bekommt eine **zweite, feste Adresse im Heimnetz** und sein **DHCP-Server wird abgeschaltet**. Die Werksadresse 192.168.8.1 bleibt als Service-Zugang bestehen.

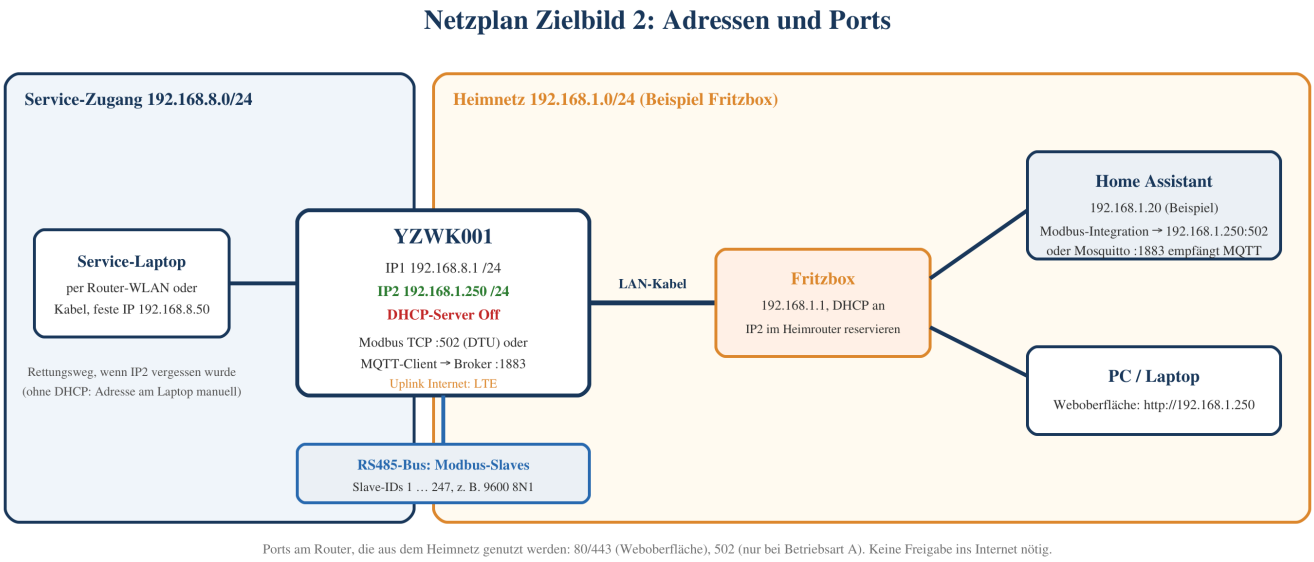


Abb. 22: Netzplan Zielbild 2 mit Adressen und Ports

13.2 Einrichtung

Alle Schritte noch **direkt am Router** (WLAN oder Direktkabel, Kapitel 8.2), bevor er ins Heimnetz gesteckt wird.

1. **Freie Adresse im Heimnetz festlegen.** Im Heimrouter (Fritzbox: Heimnetz → Netzwerk) den DHCP-Bereich ansehen und eine Adresse außerhalb wählen, zum Beispiel `192.168.1.250`. Alternativ im Heimrouter diese Adresse für die LAN-MAC des Routers reservieren (steht unter Status → LAN).
2. **DHCP-Server abschalten:** Network → DHCP → Schalter oben rechts **Off**, Save.
3. **Zweite Adresse eintragen:** Network → LAN → **IP2** = gewählte Adresse, Netmask 255.255.255.0, Save. IP1 bleibt 192.168.8.1.
4. Router per Kabel in den Heimnetz-Switch stecken.
5. **Kontrollpunkt:** Von einem PC im Heimnetz `http://192.168.1.250` (Ihre Adresse) öffnen. Die Anmeldeseite erscheint. Der Router taucht in der Geräteliste des Heimrouters auf.

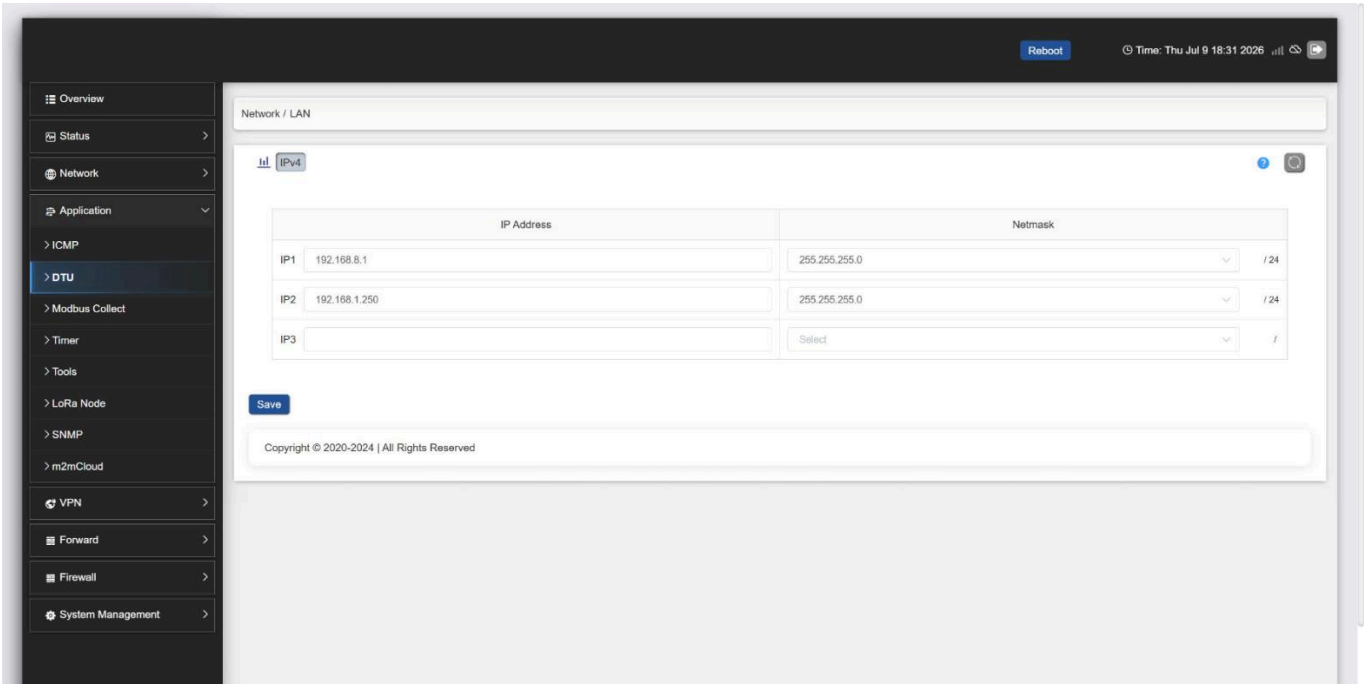


Abb. 22a: Network → LAN mit IP1 192.168.8.1 und IP2 192.168.1.250

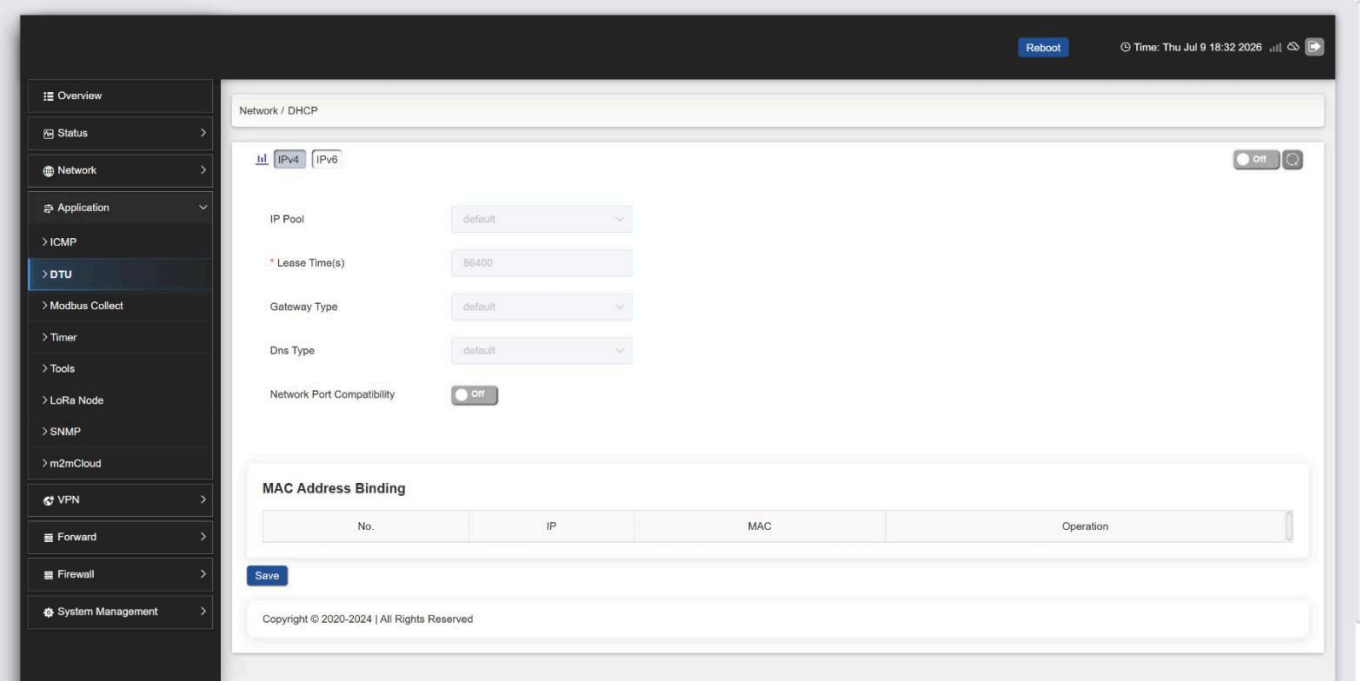


Abb. 22b: Network → DHCP mit abgeschaltetem Server

Hinweise: - Ohne DHCP-Server gibt der Router bei einer Direktverbindung (Kabel direkt zum PC) keine Adresse mehr aus. Für den Service-Zugang über 192.168.8.1 dann am PC eine feste Adresse 192.168.8.50/24 setzen (Kapitel 15) oder das Router-WLAN nutzen, solange es im Heimnetz steckt (dort vergibt die Fritzbox die Adresse). - Verwenden Sie **nicht** den WLAN-Station-Modus, nur um ins Heimnetz zu kommen; siehe 13.3. - Heimnetz-Geräte erhalten über den Router **kein** Internet aus dem Mobilfunk. Dafür wäre eine Routing-Konfiguration im Heimrouter nötig, die diese Anleitung nicht abdeckt.

13.3 Alternative ohne Kabel: WLAN-Station

Network → WIFI2.4G → Mode **Station**, Heim-WLAN aus der Scan-Liste übernehmen, Passwort eintragen, Save. Der Router bucht sich ins Heim-WLAN ein und erhält dort eine Adresse per DHCP (unter Status → WIFI2.4G ablesen oder in der Geräteliste des Heimrouters). **Warnung:** Im Station-Modus sendet der Router **kein eigenes WLAN** mehr. Ist das WLAN-Passwort falsch, bleibt nur der Zugang per Direktkabel (mit DHCP-Server an: PC automatisch; mit DHCP aus: feste PC-Adresse) oder der Werksreset. Daher: Station-Modus erst einrichten, wenn das Kabel als Rückweg bereitliegt.

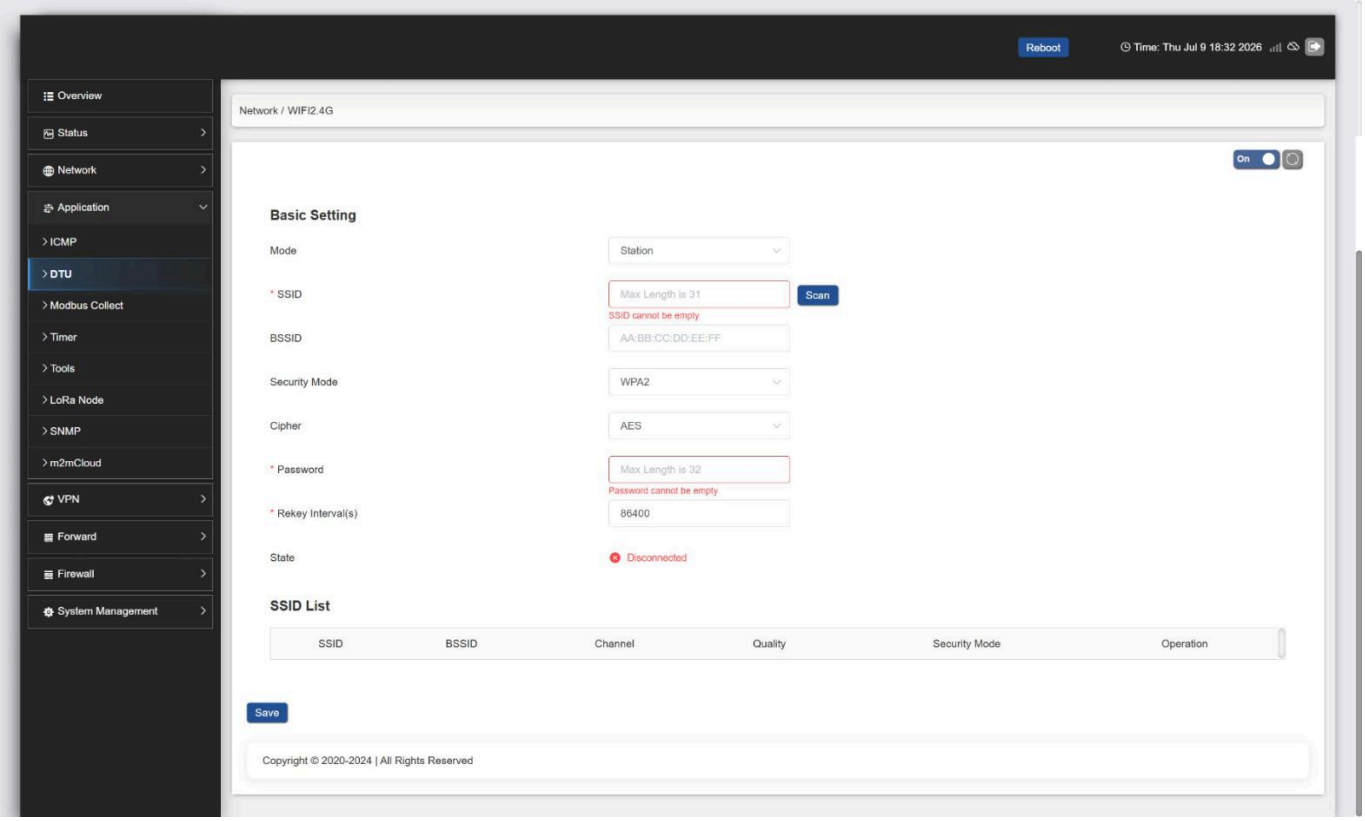


Abb. 25b: Network → WIFI2.4G im Station-Modus mit Scan-Liste

13.4 Variante A: Home Assistant liest per Modbus TCP

Router nach Kapitel 11.2 als Modbus-TCP-Gateway. In Home Assistant `configuration.yaml`:

```
modbus:
  - name: yzwk001
    type: tcp
    host: 192.168.1.250
    port: 502
    sensors:
      - name: "Regler Istwert"
        unique_id: yzwk001_regler_istwert
        slave: 1
        address: 2
        input_type: holding
        data_type: uint16
        scale: 0.1
        precision: 1
        unit_of_measurement: "°C"
        device_class: temperature
        state_class: measurement
        scan_interval: 10
```

`host` ist die IP2 des Routers, `slave` die Slave-ID am RS485-Bus, `address` das 0-basierte Register. Konfiguration prüfen und Home Assistant neu starten. **Kontrollpunkt:** Der Sensor zeigt einen Wert, keine „unavailable"-Anzeige.

13.5 Variante B: Home Assistant liest per MQTT

1. In Home Assistant das Add-on **Mosquitto broker** und die Integration **MQTT** einrichten; einen eigenen Benutzer für den Router anlegen.
2. Router nach Kapitel 11.3, MQTT Server = IP von Home Assistant, Port 1883, Benutzer/Passwort aus Schritt 1.
3. Mit MQTT Explorer das Topic prüfen und die Sensoren wie in Kapitel 12.3 anlegen. **Kontrollpunkt:** Unter Einstellungen → Geräte & Dienste → MQTT erscheinen die Werte.

13.6 Fernzugriff bei Zielbild 2

Über das Heimnetz, zum Beispiel VPN der Fritzbox (WireGuard ab FRITZ!OS 7.50), oder über den Router selbst nach Kapitel 14.

14 Fernzugriff per VPN

Mobilfunk-SIM-Karten erhalten in der Regel eine private Adresse hinter dem Netz des Anbieters. Portweiterleitungen von außen funktionieren dann nicht. Der Router baut deshalb selbst eine ausgehende VPN-Verbindung auf.

Verfahren	Empfohlen für
WireGuard	erste Wahl: schnell, schlank, stabil; Gegenstelle eigener Server, Fritzbox ab FRITZ!OS 7.50 oder Home-Assistant-Add-on
ZeroTier	einfachste Einrichtung ohne eigenen Server
OpenVPN	vorhandene OpenVPN-Infrastruktur; Zertifikate einzeln hochladen, kein .ovpn-Import
IPsec / L2TP	Anbindung an Firmen-Firewalls

Grundsatz: Weboberfläche, SSH und Modbus TCP niemals direkt ins Internet freigeben (Kapitel 9.3), sondern nur über den Tunnel.

14.1 WireGuard

VPN → WireGuard: 1. Interface Settings: **Generate Key**. Den angezeigten Public Key mit **Copy Public Key** kopieren; er wird auf der Gegenstelle als Peer eingetragen. 2. IP Address: Tunnel-Adresse des Routers, zum Beispiel `10.0.0.2/24`; Listen Port 51820; MTU 1420. 3. Peer Settings → Add: Public Key der Gegenstelle, optional Preshared Key, Endpoint Host und Port der Gegenstelle (öffentliche Adresse oder DynDNS), Allowed IPs (Tunnelnetz und das Netz hinter der Gegenstelle, zum Beispiel `10.0.0.0/24, 192.168.1.0/24`), **Persistent Keepalive 25** (wichtig hinter Carrier-Grade-NAT). 4. Interface Status On, Save. 5. Auf der Gegenstelle den Router als Peer mit seinem Public Key und Allowed IPs `10.0.0.2/32, 192.168.8.0/24` eintragen. **Kontrollpunkt:** Tabelle „WireGuard Tunnel Status" zeigt einen aktuellen „Latest Handshake". Von der Gegenstelle ist `http://192.168.8.1` erreichbar.

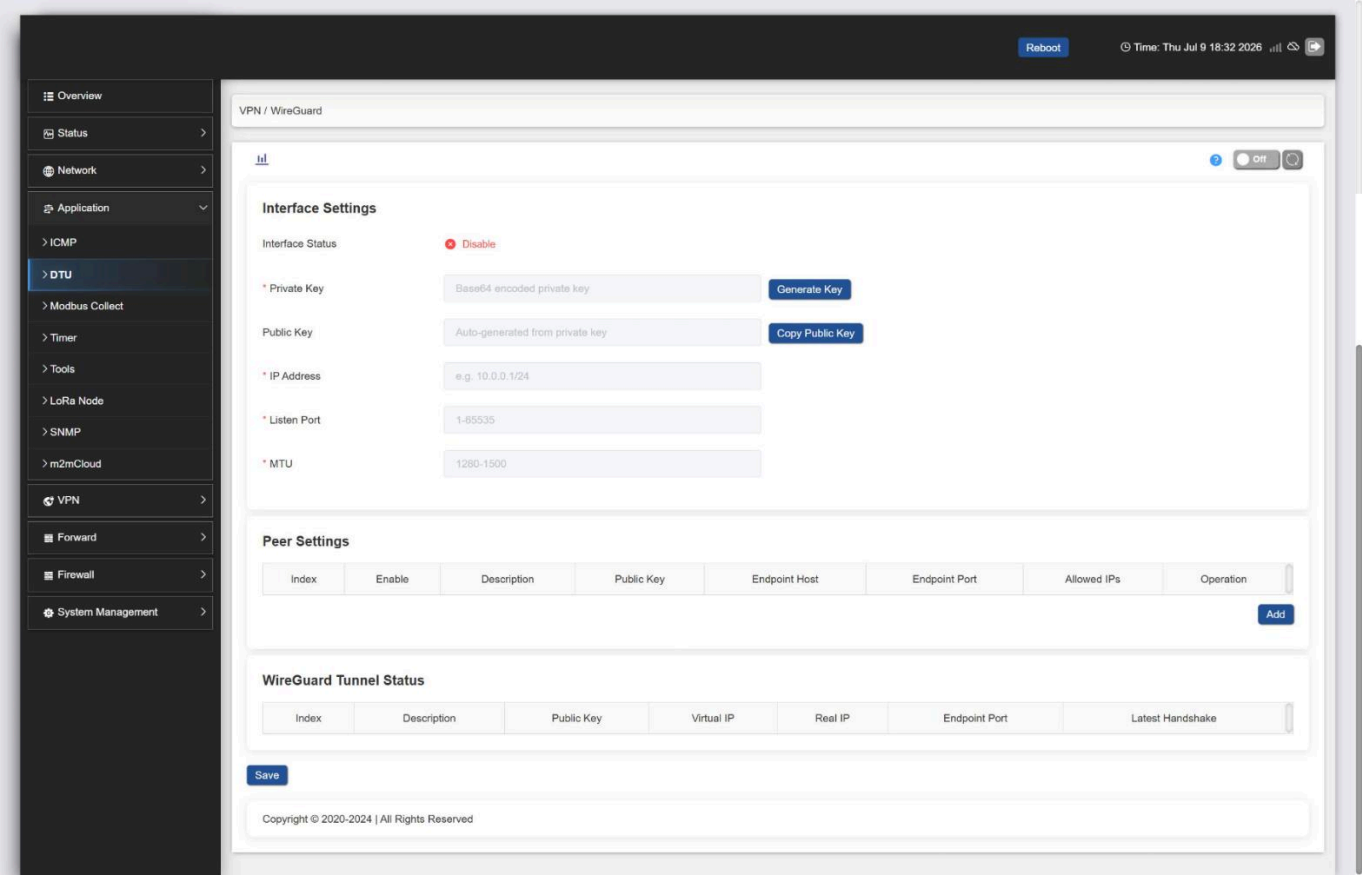


Abb. 23: VPN → WireGuard: Interface Settings, Peer Settings, Tunnel Status

14.2 ZeroTier

1. Auf my.zerotier.com ein Netzwerk anlegen, Network ID (16 Zeichen) notieren.
2. **VPN** → **ZeroTier** → Network Config → Add: Network ID eintragen, Allow Managed IPs/Routes an, Save, Schalter On.
3. Im ZeroTier-Portal das neue Mitglied (Node Address wie auf der Router-Seite) autorisieren.
4. Auf dem Zugriffs-PC den ZeroTier-Client installieren und demselben Netzwerk beitreten.
   Kontrollpunkt: „Network Live Status" zeigt Status OK und eine Assigned IP; über diese IP ist die Weboberfläche erreichbar. Benötigt ausgehend UDP 9993.

15 Service: Zugang zu einem Router, der bereits in einem fremden Netz steckt

Situation: Der Router steckt mit Werkseinstellungen im Switch eines Heimnetzes mit anderer Adressierung. Der Browser meldet `ERR_CONNECTION_TIMED_OUT` für 192.168.8.1, obwohl das Kabel steckt.

Lösung ohne Umstecken: Der PC erhält zusätzlich eine Adresse im Router-Netz. Windows PowerShell **als Administrator** (Startmenü, „PowerShell" tippen, Rechtsklick, „Als Administrator ausführen"):

```
Get-NetAdapter | Where-Object Status -eq Up
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.8.51 -PrefixLength 24
ping 192.168.8.1
```

Den Namen des Adapters aus der ersten Ausgabe einsetzen (zum Beispiel „Ethernet 2"). Die Meldung „Zugriff verweigert" bedeutet: nicht als Administrator gestartet. Die ersten ein bis drei Pings melden

„Allgemeiner Fehler", solange die Adresse noch aktiviert wird; danach antwortet der Router. Jetzt `http://192.168.8.1` öffnen.

Nach der Arbeit zurückbauen:

```
Remove-NetIPAddress -IPAddress 192.168.8.51 -Confirm:$false
```

Wurde ein Adapter komplett auf eine feste Adresse umgestellt, zurück auf automatisch:

```
Set-NetIPInterface -InterfaceAlias "Ethernet" -Dhcp Enabled
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ResetServerAddresses
```

Reihenfolge: Erst den Router in den Zielzustand bringen (Kapitel 13: DHCP aus, IP2 im Heimnetz; oder Kabel aus dem Heimnetz ziehen), **dann** den PC zurückstellen. Sonst ist die Oberfläche anschließend nicht mehr erreichbar. Den Router nie dauerhaft mit aktivem DHCP-Server in einem fremden Netz lassen.

Auf macOS/Linux entsprechend: `sudo ip addr add 192.168.8.51/24 dev eth0` (Linux) bzw. Systemeinstellungen → Netzwerk → Details → TCP/IP, manuell (macOS).

16 Neustart, Sicherung, Werkseinstellungen, Firmware-Update

16.1 Neustart

Kopfzeile → **Reboot**, oder Taste RST kurz drücken. Dauer etwa eine Minute.

16.2 Konfiguration sichern und wiederherstellen

System Management → **Config Management** → **Backup** lädt die gesamte Konfiguration als Datei. Vor jeder größeren Änderung und nach Abschluss der Einrichtung sichern. **Restore Config** → **Browse** → **Import** spielt eine Sicherung zurück; das Gerät startet neu.

16.3 Werkseinstellungen

Taste RST gedrückt halten, bis die LEDs einen Neustart anzeigen, oder **Config Management** → **Restore Factory Config** → **Reset**. Danach gelten wieder Zugangsdaten und WLAN vom Typenschild, Adresse 192.168.8.1 mit aktivem DHCP-Server. **Alle Einstellungen gehen verloren** (APN, VPN, Modbus, MQTT, Sekundär-IP, Station-Modus). Der Werksreset ist auch der Rettungsweg, wenn der Router nach einer Fehlkonfiguration (falsches Station-Passwort, falsche IP) nicht mehr erreichbar ist.

16.4 Firmware-Update

System Management → **Upgrade** → **Browse** → **Upgrade.** Nur vom Hersteller freigegebene Dateien verwenden. Vorher Backup. Während des Updates die Spannungsversorgung nicht unterbrechen. Die Konfiguration bleibt laut Hersteller erhalten; bei größeren Versionssprüngen das Häkchen „Restore Factory Config" setzen und anschließend neu konfigurieren oder das Backup einspielen.

17 Fehlerbehebung

Problem	Mögliche Ursache	Abhilfe
PWR leuchtet nicht	keine oder zu geringe Versorgung	Spannung an V+/V− messen (9–35 V DC), Steckklemme richtig aufgesteckt, Netzteil prüfen
Browser: „Seite nicht erreichbar", `ERR_CONNECTION_TIMED_OUT`	PC hat keine Adresse in 192.168.8.x; Router steckt im Heimnetz statt direkt am PC	`ipconfig` prüfen. Direkt per Router-WLAN oder Kabel verbinden (Kapitel 8.2) oder zweite PC-Adresse (Kapitel 15). Nach Zielbild 2 die IP2 verwenden
Browser zeigt Suchergebnisse statt der Oberfläche	Adresse ohne `http://` eingegeben	`http://192.168.8.1` eingeben
Browser: Zertifikatswarnung	HTTPS mit selbstsigniertem Zertifikat	„Erweitert" → „Trotzdem fortfahren", oder `http://` verwenden
Router-WLAN verbunden, aber keine Adresse	DHCP-Server des Routers abgeschaltet (Kapitel 13.2)	am PC feste Adresse 192.168.8.50/24 setzen oder Router-WLAN im Heimnetz nutzen
Anmeldung gesperrt	dreimal falsches Passwort	angezeigte Wartezeit abwarten; Passwort vom Typenschild bzw. Kapitel 3
Passwort vergessen		Werksreset (Kapitel 16.3), danach Typenschild-Passwort
SIM „nicht bereit"	SIM-PIN aktiv, Karte falsch eingesetzt, Karte gesperrt	PIN im Smartphone deaktivieren oder im PDP-Profil eintragen; Karte spannungslos neu einsetzen; Karte im Smartphone testen
Eingebucht, aber „Disconnected"	falscher APN, kein Datenvolumen, Roaming gesperrt, IoT-SIM nicht freigeschaltet	APN manuell eintragen (Kapitel 9.6), Tarif prüfen, Anbieter kontaktieren
Keine LTE-Verbindung	Band nicht verfügbar, schlechter Empfang, Antenne im Metallschrank	Signal unter Overview prüfen, Antenne nach außen verlegen, Network Type AUTO
Verbindung bricht regelmäßig ab	schwaches Signal, Anbieter trennt Sitzung	ICMP-Watchdog (Kapitel 9.7), Antenne verbessern, Timer-Neustart nachts
NTP „Disconnected", Uhrzeit falsch	kein Internet, NTP-Server nicht erreichbar	Mobilfunk herstellen, europäischen NTP-Server eintragen (Kapitel 9.5)
Log voller „MQTT connect to server fail"	m2mCloud aktiv	Application → m2mCloud → Off (Kapitel 9.4)
Modbus: Timeout, keine Antwort	Serial Type steht auf RS232 (Werk); A/B vertauscht; falsche Slave-ID; Baudrate/Parität falsch; fehlendes Bezugspotenzial	Serial Type auf RS485; A und B tauschen; Parameter mit Gerät abgleichen; V− mit GND des Slaves verbinden; 120 Ω prüfen

Problem	Mögliche Ursache	Abhilfe
Modbus: unsinnige Werte	falsche Wortfolge bei 32-Bit, falsches Register (0/1-basiert), Zehntel-Skalierung	Data Type ABCD/CDAB/DCBA durchprobieren, Register ±1, Teiler 10
Modbus: „Illegal data address" / Fehlercode 2	Register existiert nicht	Registerliste prüfen, Register Quantity verringern
DTU oder Modbus Collect lässt sich nicht einschalten	serielle Schnittstelle vom anderen Dienst belegt	den anderen Dienst auf Off (Kapitel 11.1)
Keine MQTT-Daten am Broker	Broker-Adresse/Port/Zugang falsch; Broker aus dem Mobilfunk nicht erreichbar; TLS-Port ohne Zertifikat	Zugangsdaten prüfen; vom PC mit MQTT Explorer testen; Port 1883 statt 8883 testen
Home Assistant Modbus-Sensor „unavailable"	IP2 falsch, Port 502 nicht offen, DTU Off, Slave-ID/Register falsch	Kontrollpunkt Kapitel 11.2 mit Testprogramm wiederholen
VPN WireGuard: kein Handshake	Endpoint/Port falsch, Public Keys vertauscht, Keepalive fehlt, UDP vom Anbieter blockiert	Keys auf beiden Seiten vergleichen, Keepalive 25, Endpoint per DynDNS, Port der Gegenstelle freigeben
Router nach Station-Modus nicht mehr erreichbar	eigenes WLAN abgeschaltet, Heim-WLAN-Passwort falsch	per Direktkabel (Kapitel 8.2 oder 15) Mode zurück auf AP, sonst Werksreset
Heimnetz-Geräte bekommen plötzlich Adressen 192.168.8.x	Router mit aktivem DHCP-Server im Heimnetz	Router abstecken oder DHCP-Server abschalten (Kapitel 13.2), betroffene Geräte neu verbinden

18 Wartung, Entsorgung, Hinweise

- Das Gerät ist wartungsfrei. Gehäuse bei Bedarf mit trockenem Tuch reinigen.
- Firmware-Updates nur bei Bedarf und nach Backup (Kapitel 16.4).
- Mobilfunkverträge: Datenvolumen und Laufzeit im Blick behalten; bei Prepaid-Karten auf Ablauf achten.
- Vor Weitergabe oder Entsorgung: Werksreset (löscht Passwörter, VPN-Schlüssel, Broker-Zugänge) und SIM-Karte entnehmen.
- Elektroaltgeräte nicht über den Hausmüll entsorgen, sondern bei den kommunalen Sammelstellen abgeben.
- Funkanlage: Der Betreiber ist für die Einhaltung der Funkvorschriften bei Verwendung anderer Antennen verantwortlich.

Anhang A: Schnellstart in 5 Schritten (Kundenblatt)

[Abb. 24: Kundenblatt-Layout, eine Seite, mit QR-Code für http://192.168.8.1]

1 Anschließen. Nano-SIM spannungslos einsetzen (PIN vorher deaktivieren). Antenne an ANT. 12 V DC an Klemme 3 (V+) und 4 (V−). RS485: A an Klemme 1, B an Klemme 2. LED PWR leuchtet.

2 Verbinden. Laptop oder Smartphone mit dem WLAN `Wireless-2G-xxxxxx` vom Typenschild verbinden. Oder: Netzwerkkabel **direkt** vom Router zum PC. Nicht in die Fritzbox stecken.

3 Anmelden. Browser: `http://192.168.8.1`. Benutzer `admin`, Passwort vom Typenschild. Die Seite „Overview" erscheint.

4 Absichern. Nacheinander: Config Management → Backup · Account → Passwort ändern · Firewall → Port Setting → Remote Access: WAN-Häkchen bei WEB/SSH/CLI entfernen · Application → m2mCloud → Off · System Time → Berlin, NTP `de.pool.ntp.org` · Network → Modem → APN prüfen. Overview zeigt „Connected".

5 Anlage anbinden. Application → DTU (Modbus-TCP-Gateway, Port 502) **oder** Application → Modbus Collect (MQTT). Serial Type auf **RS485**, Baudrate wie am Gerät. Danach Backup. Details: Kapitel 11 bis 13.

Typenschild-Daten	
SSID	Wireless-2G-_____
WLAN-Passwort	_____
Login	admin / _____

Anhang B: Werkswerte und Menüreferenz

Einstellung	Menü	Werkswert	Empfehlung
LAN-IP / Maske	Network → LAN → IP1	192.168.8.1 / 255.255.255.0	belassen; IP2 für Heimnetz (Kapitel 13)
DHCP-Server	Network → DHCP	On, Pool 192.168.8.1–254, Lease 86400 s	On bei Zielbild 1, Off bei Zielbild 2
WLAN	Network → WIFI2.4G	On, AP, SSID Wireless-2G-xxxxxx, WPA2/AES, Kanal Auto, 802.11n, 20 MHz	eigene SSID und Passwort
Mobilfunk	Network → Modem	Regel 1, APN leer (Auto), Auth PAP+CHAP, IPv4, Network Type AUTO	APN laut Anbieter
Link Priority	Network → Link Priority	Modem, ICMP 223.5.5.5, Interval 10, Retry 2	ICMP 1.1.1.1
ICMP-Watchdog	Application → ICMP	keine Regel	8.8.8.8 / 1.1.1.1, 60 s, 5×, Modem-reset
DTU	Application → DTU	Off, Protocol TCP, Serial RS232 115200 8N1	nach Kapitel 11.2
Modbus Collect	Application → Modbus Collect	Off, MQTT, Response Timeout 1000 ms, Report Rate 5 s	nach Kapitel 11.3
m2mCloud	Application → m2mCloud	**On**, hk.ezulink.com:10808	**Off**
Remote Access	Firewall → Port Setting	PING/WEB/SSH/CLI für LAN, WAN, VPN **alle an**	WAN: nur PING
CLI	Firewall → Port Setting	Telnet	SSH
SPI-Filter	Firewall → SPI Filter	alle an außer IP-Spoofing	alle an
Zeit	System Management → System Time	UTC+8, ntp.sjtu.edu.cn	UTC+1 Berlin, de.pool.ntp.org
Benutzer	System Management → Account	admin (fest), guest (aus)	Passwort ändern, Idle-Logout an

Einstellung	Menü	Werkswert	Empfehlung
VPN	VPN → …	alle Off	WireGuard oder ZeroTier
MASQ	Forward → MASQ	br-lan, Modem, m2mCloud On	belassen

Nicht belegte Menüs auf dieser Hardware: LoRa Node (optional, Endknoten SX1262), SNMP (bei Bedarf), Timer, Tools (Ping/Traceroute für Diagnose).

Anhang C: Praxisbeispiel Temperaturregler AiFUZZY/Yudian

Regler mit Modbus RTU, 9600 Baud, 8N1, Slave-ID 1. Die Registerliste des Herstellers passt nicht in allen Punkten zur Firmware des Reglers; die folgenden Register wurden am Gerät verifiziert.

Wert	Funktion	Register (0-basiert)	Typ	Hinweis
Istwert (PV)	03	2	Unsigned 16bit	32767 = Fühler offen; Anzeige in Zehntelgrad je nach Dezimalstellen-Parameter
Einheit / Netzfrequenz	03	34	Unsigned 16bit	0 = °C 50 Hz, 1 = °F 50 Hz, 2 = °C 60 Hz, 3 = °F 60 Hz; für Deutschland 0

Modbus Collect: Gerät RTU/RS485 9600/none/8/1, Publish Topic `anlage/heizraum/regler`; Command `istwert`, Slave 1, FC 03, Register Start 2, Quantity 1, Unsigned 16bit, Poll 5000 ms.

Home Assistant (Modbus TCP über DTU): `slave: 1`, `address: 2`, `input_type: holding`, `data_type: uint16`.

Kontrollpunkt: Der gelesene Wert entspricht der Anzeige am Reglerdisplay. Ohne angeschlossenen Fühler erscheint 32767.

Anhang D: Abbildungsverzeichnis

Nr.	Inhalt	Art
01	Produktbild mit Antenne	vorhanden (aus Anleitung v1)
02	Schema Zielbild 1	vorhanden (Grafik)
03	Schema Zielbild 2	vorhanden (Grafik)
04	Typenschild mit Markierungen	Foto
05	Frontansicht mit Maßen	vorhanden (v1)
06	Klemmenbelegung Unterseite	vorhanden (v1); Foto der realen Beschriftung noch offen
07	Platzbedarf und Seitenansicht mit Maßen	vorhanden (v1)
08	Anschlussbild Versorgung und RS485-Bus	vorhanden (v1), Beschriftung V+/V− überarbeiten
09	SIM-Karte einsetzen	vorhanden (v1)

Nr.	Inhalt	Art
10	Richtig/Falsch: Direktverbindung vs. Heimnetz-Switch	vorhanden (Grafik)
11	Login-Seite	vorhanden (Screenshot)
12	Overview	vorhanden (Screenshot)
13	Account, Password Change	vorhanden (Screenshot)
14	Remote-Access-Matrix, Zielzustand	vorhanden (Screenshot)
15	System Time	vorhanden (Screenshot)
16	Network → Modem, PDP-Profil	vorhanden (Screenshot)
17	Oberfläche mit Bedienelementen	vorhanden (Screenshot)
18	Entscheidungsgrafik DTU vs. Modbus Collect	vorhanden (Grafik)
19	DTU, Modbus-TCP-Gateway	vorhanden (Screenshot)
20	Modbus Collect, Global Config	vorhanden (Screenshot)
21	Modbus Collect, Device Config mit Command	vorhanden (Screenshot)
22	Netzplan Zielbild 2	vorhanden (Grafik)
23	WireGuard	vorhanden (Screenshot)
24	Kundenblatt mit QR-Code	Layout
14b, 17b, 21b, 22a, 22b, 25, 25b, 26–30	weitere Screenshots der Oberfläche	vorhanden (Screenshot)