Benutzerhandbuch
MC100

MC Technologies GmbH – July 2026

4G
LTE Cat1

WLAN

GNU/Linux

RS-232
& RS-485

USB 2.0

Optionales
GNSS

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Deutschland

www.mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

UG_MC100_DE_V5.2_2026_06_24

1 Änderungshistorie

Version	Datum	Autor	Beschreibung
4.0	01.06.2025	hussein.soueidan@mc-technologies.com	Dokumentendesign ändern und minimale Änderungen am Inhalt
5.0	07.05.2026	sascha.dikhoff@mc-technologies.com hussein.soueidan@mc-technologies.com	• Hinzugefügt: • Sicherheitsanweisungen • Screenshots aktualisiert • Standardpasswort • Mobilfunkinformationen • Netztrennung
5.1	23.06.2026	sascha.dikhoff@mc-technologies.com	Deutsche Version generiert
5.2	25.06.2026	sascha.dikhoff@mc-technologies.com	Kapitel zur Cybersecurity hinzugefügt

2 Inhaltsverzeichnis

3 Einleitung

Vielen Dank, dass Sie sich für ein Produkt von MC Technologies entschieden haben.

Das MC100 ist eine Familie von Linux-basierten IoT LTE Gateways, die für Machine-to-Machine (M2M) und industrielle Internet of Things (IIoT)-Anwendungen optimiert sind. Eine große Auswahl an Modellen bietet den perfekten Funktionsumfang für vielfältige industrielle Anwendungsfälle auf kostengünstige Weise.

Die Gerätevarianten und Optionen umfassen unter anderem:

• Verschiedene Mobilfunkmodems, optimiert für spezifische Anwendungen (z. B. 2G-Fallback, global, EU-only)

• Funkschnittstellen: GNSS-Standortdienste, WLAN, Bluetooth und wM-Bus

• Serielle Schnittstellen: RS-232, RS-485 (Modbus), CAN, 1-Wire, M-Bus

• SensT2-Erweiterung: PT100/PT1000 RTD, 0–20 mA I/O, 10 V DAC, 1-Wire

• GPIO-Erweiterung

• SensorBox

Weitere modellspezifische Informationen finden Sie in modellspezifischen Anhängen auf unserer Website:

https://mc-technologies.com/service-support/download/

3.1 Zweck des Handbuchs

Dieses Dokument dient als Leitfaden für die Installation, Inbetriebnahme, Betrieb und Wartung des IoT Gateway MC100. Ziel ist es, sicherzustellen, dass Nutzer das Gerät effektiv nutzen können und dabei alle relevanten Sicherheitsstandards einhalten können.

3.2 Zielgruppe

Dieses Handbuch richtet sich an Installateure, Systemintegratoren und Bediener, die für die Installation, Konfiguration und den Betrieb des MC100 in industriellen und kommerziellen Umgebungen verantwortlich sind.

Vom Leser wird erwartet, dass er grundlegende technische Kenntnisse von elektrischen Systemen und Netzwerktechnologien hat. Installation und Inbetriebnahme müssen von qualifiziertem Personal durchgeführt werden.

3.3 Bestimmungsgemäßer Gebrauch

Der MC100 ist für den professionellen und industriellen Einsatz vorgesehen. Das Gerät ist für die Integration in Industriegeräte, Steuerungsschränke und eingebettete Systeme konzipiert und wird für Datenkommunikation, Fernüberwachung und Steuerungsanwendungen in kommerziellen und

industriellen Umgebungen eingesetzt. Installation, Konfiguration und Wartung müssen von qualifiziertem Personal mit entsprechendem technischem Wissen über elektrische und Netzwerksysteme durchgeführt werden. Das Gerät muss im Rahmen der in dieser Dokumentation definierten technischen Spezifikationen und Umweltbedingungen betrieben werden.

4 Garantiebestimmungen

Unbefugte Nutzung, Nichtbeachtung dieser Dokumentation, Betrieb oder Wartung durch unzureichend qualifizierte Personen, sowie unautorisierte Änderungen schließen die Haftung des Herstellers für daraus resultierende Schäden aus. Bei Änderungen am Gerät erlischt die Herstellergarantie. Die Bestimmungen unserer allgemeinen Kaufbedingungen (AGB) gelten. Diese finden Sie auf unserer Website:

https://mc-technologies.com/agb-aeb

4.1 Haftungsbeschränkung

Hersteller und Verkäufer haften nicht für Schäden, die durch unsachgemäße Nutzung, Installation oder Wartung entstehen. Dazu gehören Folgeschäden, Personenschäden, Sachschäden und Schäden, die durch das Nichtbefolgen der Sicherheitsanweisungen verursacht wurden. Dieser Haftungsausschluss beeinträchtigt nicht die gesetzlichen Garantieansprüche. Die Haftung für Material- und Herstellungsmängel wird innerhalb der gesetzlichen Garantiefrist übernommen.

4.2 Zugelassene Zubehörteile

Dieses Gerät darf nur mit geeignetem Zubehör betrieben werden, das für das Gerät zugelassen ist.

4.3 Regelmäßige Inspektion

Überprüfen Sie das Gerät und alle Komponenten vor der Nutzung auf Schäden oder Anomalien. Verwenden Sie das Gerät nicht, wenn es beschädigt ist oder Abnutzungserscheinungen zeigt. Stellen Sie sicher, dass alle Kabel in einwandfreiem Zustand sind. Das Gerät darf nicht verwendet werden, wenn Kabel oder Stecker beschädigt sind.

4.4 Technische Grenzen

Das Produkt ist ausschließlich für die Verwendung innerhalb der in diesem Dokument festgelegten technischen Einschränkungen und maximalen Grenzwerte vorgesehen. Insbesondere müssen folgende Bedingungen beachtet werden:

- Die Umgebungstemperatur darf nicht über oder unter die Grenzwerte fallen.
- Die maximale Luftfeuchtigkeit darf nicht überschritten werden, und Kondensation muss vermieden werden.
- Die Versorgungsspannung muss innerhalb der Grenzen liegen und die maximalen Eingangswerte dürfen nicht überschritten werden.
- Die maximale Schaltspannung und -strom dürfen nicht überschritten werden.

5 Sicherheitsanweisungen

Diese Anweisungen ermöglichen einen sicheren und effizienten Umgang mit dem Produkt. Die Anweisungen sind ein integraler Bestandteil des Produkts und müssen stets für Installations-, Wartungs-, Inbetriebnahme- und Bediener zugänglich gehalten werden.

Die Sicherheits- und Wartungsanweisungen müssen strikt eingehalten werden, um einen sicheren Betrieb des Produkts zu gewährleisten. Nur die Beachtung aller Sicherheitsrichtlinien gewährleistet den Schutz von Personen und Umwelt vor Gefahren sowie den sicheren und problemfreien Betrieb des Produkts.

Allgemeine Sicherheitsvorschriften und lokale Richtlinien für den Anwendungsbereich des Geräts sowie zur Unfallprävention sowie Verfahren und Betriebsanweisungen mit sicherheitskritischen Informationen müssen strikt eingehalten werden.

5.1 Verpflichtungen des Betreibers

Der Betreiber muss jederzeit die regionalen Vorschriften bezüglich Bedienung, Funktionstests, Reparatur und Wartung elektronischer Geräte einhalten.

5.2 Qualifikation der Installateure

Die Installation und Wartung des Produkts dürfen nur von geschulten, autorisierten Installateuren durchgeführt werden, die über die erforderliche Qualifikation verfügen, um eine sichere Wartung und den Betrieb sicherzustellen. Der qualifizierte Installateur muss diese Dokumentation gelesen und verstanden haben und deren Richtlinien und Anweisungen befolgen. Dieses Produkt darf nur von oder unter der Aufsicht von geschulten Personen betrieben werden.

5.3 Richtlinien für Transport und Lagerung

- Setzen Sie das Produkt während des Transports oder der Lagerung nicht Feuchtigkeit oder anderen potenziell schädlichen Umweltbedingungen (Strahlung, Gase usw.) aus.
- Schützen Sie das Produkt vor Stößen während des Transports und der Lagerung (z. B. durch Verwendung von luftkissengepolsterter Verpackung)
- Überprüfen Sie vor der Installation des Produkts auf Schäden, die durch unsachgemäßen Transport oder Lagerung entstanden sind. Schäden während des Transports müssen in den Versanddokumenten vermerkt werden. Alle Schadensersatzansprüche müssen sofort und vor der Übergabe an den für die Lagerung oder Logistik zuständigen Transporter oder Unternehmen erhoben werden

5.4 Sicherheitsmaßnahmen

	Elektrostatische Entladungen, Kurzschlüsse und Spannungsspitzen erhöhen die Brandgefahr, verursachen Schäden am Produkt und können Personenschäden verursachen. Beachten Sie die allgemeinen Vorsichtsmaßnahmen beim Umgang mit elektrostatisch empfindlichen Bauteilen. Schalten Sie den Strom ab, bevor Sie irgendwelche Arbeiten an einem elektrischen Gerät durchführen. Stellen Sie sicher, dass ein geeigneter Überspannungsschutz installiert ist. Verwenden Sie das Gerät nicht bei sichtbaren oder anderweitig bekannten Schäden.

	**Schäden durch unsachgemäßes Handling, Reparaturen und Modifikationen erhöhen das Brandrisiko, verursachen Schäden am Produkt und können Personenschäden verursachen.** Es ist nicht erlaubt, das Produkt für Reparaturarbeiten oder Modifikationen zu öffnen, abgesehen vom Entfernen und Einsetzen der bereitgestellten Steckkarten. Stellen Sie sicher, dass das elektrische Zubehör für diesen Zweck gut geeignet ist. Halten Sie das Gerät von Kindern und Tieren fern, um Gefahren wie Ersticken von Teilen und Gefahren durch Beißen zu vermeiden.
	**Staub, Ablagerungen, Feuchtigkeit und Flüssigkeiten aus der Umgebung könnten ins Produkt gelangen, das Brandrisiko erhöhen, das Produkt beschädigen und möglicherweise Personenschäden verursachen.** Das Produkt darf nicht in feuchten Umgebungen oder in unmittelbarer Nähe von Wasser oder anderen Flüssigkeiten verwendet werden. Installieren Sie das Produkt an einem sauberen, trockenen Ort, der vor spritzendem Wasser, Staub und Schmutz geschützt ist, der in das Gerät gelangen könnte.
	Offene Flammen, starke Chemikalien und brennbare Materialien einschließlich Aerosole erhöhen das Brandrisiko, verursachen Schäden am Produkt und können Personenschäden verursachen. Das Produkt muss von direktem Sonnenlicht, offenen Flammen, aggressiven Chemikalien, brennbaren Stoffen, Sprengstoffen und Aerosolen ferngehalten werden.
	Extreme Temperaturen, unzureichende Wärmeabgabe oder Belüftung erhöhen die Brandgefahr, verursachen Schäden am Produkt und können Personenschäden verursachen. Betreiben Sie das Gerät in einem gut belüfteten Bereich, fernab von direkter Sonneneinstrahlung. Um eine gute Wärmeableitung zu gewährleisten, sollten Sie das Gerät oder seine Lüftungsöffnungen nicht einschließen oder abdecken. Das Gerät muss innerhalb der angegebenen Betriebstemperaturgrenzen betrieben werden.
	**Starke magnetische oder elektrische Felder, Vibrationen und Schocks verursachen Fehlfunktionen und können das Gerät beschädigen.** Halten Sie das Gerät von elektronischen Geräten fern, die starke magnetische oder elektrische Felder erzeugen, wie etwa eine Mikrowelle, ein Radar, einen Elektromotor oder einen Generator. Stellen Sie sicher, dass das Gerät richtig befestigt ist, und vermeiden Sie hohe Beschleunigungen.
	Ein zu geringer Abstand zwischen Antennen und Personen kann gesundheitliche Beeinträchtigungen verursachen. Beachten Sie, dass drahtlose Geräte die Funktion von z. B. Hörgeräten oder Herzschrittmachern beeinflussen können. Die Antennen müssen während des Betriebs mindestens 20 cm von Personen entfernt angebracht werden. Falls zutreffend, sollten die Regeln und Vorschriften für den Einsatz von Geräten in Krankenhäusern und Gesundheitseinrichtungen eingehalten werden.

5.5 Elektrische Sicherheitsanforderungen

Die elektrische Installation, Wartung und Inbetriebnahme von Produkten, die mit Hoch- oder Niederspannung betrieben werden (>= 50 V Wechselstrom bzw. >=120 V DC), dürfen nur von Personen durchgeführt werden, die aufgrund ihrer Fachausbildung, ihres Fachwissens und ihrer Erfahrung einschließlich Kenntnis der relevanten Normen und Vorschriften berechtigt sind, Arbeiten an elektrischen Systemen durchzuführen und mögliche Gefahren eigenständig zu erkennen und zu vermeiden, z. B. wie in VDE 1000-10 beschrieben.

Die elektrische Installation muss gemäß allen geltenden Standards (z. B. IEC, EN, VDE, ...) durchgeführt werden. Die elektrische Installation darf nur im fehlerfreien Zustand betrieben werden und nach Prüfung mit einem anerkannten Prüfverfahren wie VDE 0100-600 / IEC 60364-6, wobei alle notwendigen Sicherheitsmaßnahmen vor dem Betrieb getroffen sind.

Die Ausrüstung muss unmittelbar nach Installation, Erweiterung oder anderen Änderungen, z. B. gemäß DIN EN 50699 (VDE 0702), inspiziert werden. Der Prüfer muss für die Inspektion qualifiziert sein, wie z. B. in TRBS 1203 beschrieben, um Inspektionen durchzuführen und die Inspektionsintervalle durch ein Risikobewertungsverfahren festzulegen. Der resultierende Inspektionsbericht muss archiviert werden. Geräte, die die Inspektion bestehen, sollten mit einem Inspektionsaufkleber markiert werden, der die Ergebnisse zusammenfasst und den nächsten Fälligkeitstermin anzeigt.

5.6 Elektrische Sicherheitsvorkehrungen

- Eine unsachgemäße Installation kann zu Elektroschocks, Kurzschlüssen oder Bränden führen
- Die Verkabelung muss z. B. gemäß DIN VDE 0100-520 geeignet sein
- Die versorgende elektrische Anlage muss mit einem Reststromgerät (RCD) ausgestattet sein

6 Cybersecurity / IT-Sicherheit

- Allgemeines Sicherheitskonzept
  Das Produkt verfügt über Sicherheitsmechanismen für den sicheren Betrieb in vernetzten industriellen Umgebungen und zum Schutz vor unbefugtem Zugriff.
- Zugriffsschutz
  Das Gerät wird mit Standard-Zugangsdaten ausgeliefert, die unmittelbar geändert werden müssen. Es sind sichere Passwörter zu verwenden.
- Netzwerksicherheit
  Nur benötigte Dienste aktivieren. Sichere Protokolle wie HTTPS, SSH und VPN verwenden. Zusätzliche Schutzmaßnahmen bei öffentlichen Netzwerken sind empfohlen.
- Software und Updates
  Regelmäßige Firmware-Updates durchführen. Nur vertrauenswürdige Quellen verwenden.
- Verantwortung des Betreibers
  Der Betreiber ist für die sichere Integration und Einhaltung der IT-Sicherheitsrichtlinien verantwortlich.

- Regulatorische Konformität
  Das Produkt erfüllt die Richtlinie 2014/53/EU einschließlich relevanter Anforderungen zur Cybersicherheit (Artikel 3.3, sofern zutreffend). Details sind in der EU-Konformitätserklärung enthalten.
- Sicherheitsvorfälle und Meldepflicht
  Bei vermuteten Sicherheitsvorfällen (z. B. unbefugter Zugriff, unerwartetes Systemverhalten oder erkannte Schwachstellen) müssen unverzüglich geeignete Maßnahmen ergriffen werden.

  Der Betreiber bzw. Systemintegrator ist verantwortlich für:
  - die Isolation betroffener Systeme (falls erforderlich)
  - die Analyse und Behebung des Vorfalls
  - die Wiederherstellung eines sicheren Betriebs

  Sofern erforderlich, sind Sicherheitsvorfälle gemäß internen Prozessen und geltenden Vorschriften zu melden.

  Für Support und Meldung von Sicherheitslücken wenden Sie sich bitte an:
  support@mc-technologies.com

7 Produktetikett

Das Etikett des Produkts befindet sich an der Unterseite des Produkts. Neben Informationen wie einer E1-Zulassungskennzeichnung, Seriennummer, MAC-Adresse, IMEI-Nummer und Betriebsspannung kann sie folgende Markierungen enthalten:

7.1 Sonderabfälle

Dieses Symbol zeigt an, dass das Gerät an geeigneten Sammelstellen getrennt von Restabfällen entsorgt werden muss. Bitte beachten Sie unten den Abschnitt zum Umweltschutz und den Abschnitt zur Entsorgung am Ende dieses Dokuments.

7.2 CE-Markierung

CE

- Durch Anbringen der CE-Kennzeichnung erklärt die MC Technologies GmbH, dass das Produkt den geltenden EU-Richtlinien entspricht.
- EU-Konformitätserklärung: Hiermit erklärt die MC Technologies GmbH, dass dieses Funkgerät der Richtlinie 2014/53/EU entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse verfügbar: https://mc-technologies.com/wp-content/uploads/2026/07/DoC-MC100.pdf

8 Umweltschutz

Das Produkt und die zugehörige Transportverpackung bestehen größtenteils aus recycelbaren Rohstoffen. Es kann zur ordnungsgemäßen Wiederverwertung an die MC Technologies GmbH geschickt werden. Am Ende seiner Nutzungsdauer darf das Produkt nicht mehr als Haushaltsabfall entsorgt werden.

Die Entsorgung des Produkts und seiner Verpackung muss gemäß allen einschlägigen Umweltschutzvorschriften erfolgen. Recyceln Sie verantwortungsvoll, indem Sie Verpackungsmaterialien wie Karton und Papier vom Kunststoff trennen und die speziellen Abfallsammelsysteme verwenden. Siehe den Abschnitt zur Entsorgung am Ende dieses Dokuments für Anweisungen, wie man das Produkt zum Recycling an MC Technologies zurückgibt.

9 Technische Spezifikation

9.1 Physikalische Eigenschaften und Grenzwerte

Physikalische Eigenschaft / Grenzwert	Wert
Stromversorgung	8 V ... 30 V Gleichstrom (mindestens 14 W)*
Abmessungen (W x H x D)	120 x 75 x 35 mm
Gewicht	~ 230 g (~ 4,23 oz)
Betriebstemperatur	-20 °C bis +70 °C (Sensorbox-Variante: -20°C bis +55°C)
Gehäusematerial	ABS

** Siehe Abschnitt unten für Details zum Stromversorgungsbedarf.*

9.2 Funkinformationen

Dieses Gerät enthält Funksender und Empfänger, die in den unten aufgeführten Frequenzbändern arbeiten.
Die maximale übertragene Radiofrequenzleistung wird für jede Technologie angegeben.

Die unterstützten Frequenzbänder und Ausgangsleistungen hängen von der verwendeten Hardwarevariante ab.

Für einen sicheren Betrieb muss ein Mindestabstand von 20 cm zwischen den Antennen des Geräts und einer Person während des Betriebs eingehalten werden.

9.3 Mobilfunkeigenschaften

Das Gerät integriert je nach Produktvariante ein Mobilfunkmodul:

Die Standardproduktvariante ist mit einem Quectel EC21-E-Modul ausgestattet und die als "global" gekennzeichneten Varianten mit einem Quectel EG25-G-Modul.

Varianten	Standardmodul	Globales Modul
Funkmodul	Quectel EC21-E	Quectel EG25-G

Frequenzbänder LTE FDD	B1 (2100 MHz), B3 (1800 MHz), B5 (850 MHz), B7 (2600 MHz), B8 (900 MHz), B20 (800 MHz)	B1 (2100 MHz), B2 (1900 MHz), B3 (1800 MHz), B4 (1700/2100 MHz), B5 (850 MHz), B7 (2600 MHz), B8 (900 MHz), B12 (700 MHz), B13 (700 MHz), B18 (800 MHz), B19 (800 MHz), B20 (800 MHz), B25 (1900 MHz), B26 (850 MHz), B28 (700 MHz)
Frequenzbänder LTE TDD	-	B38 (2600 MHz), B39 (1900 MHz), B40 (2300 MHz), B41 (2500 MHz)
Frequenzbänder WCDMA	B1 (2100 MHz), B5 (850 MHz), B8 (900 MHz)	B1 (2100 MHz), B2 (1900 MHz), B4 (1700/2100 MHz), B5 (850 MHz), B6 (800 MHz), B8 (900 MHz), B19 (800 MHz)
Frequenzbänder (GSM):	B3 (1800 MHz), B8 (900 MHz)	B2 (1900 MHz), B3 (1800 MHz), B5 (850 MHz), B8 (900 MHz)
Maximale HF-Ausgangsleistung	LTE (FDD/TDD): bis zu 23 dBm UMTS (WCDMA): bis zu 24 dBm GSM: bis zu 33 dBm (850/900 MHz), bis zu 30 dBm (1800/1900 MHz) GSM (8-PSK): bis zu 27 dBm (850/900 MHz), bis zu 26 dBm (1800/1900 MHz)	LTE (FDD/TDD): bis zu 23 dBm UMTS (WCDMA): bis zu 24 dBm GSM: bis zu 33 dBm (850/900 MHz), bis zu 30 dBm (1800/1900 MHz) GSM (8-PSK): bis zu 27 dBm (850/900 MHz), bis zu 26 dBm (1800/1900 MHz)

9.4 GNSS Empfänger

Je nach Produktvariante kann das Gerät einen im Mobilfunkmodul integrierten GNSS-Empfänger enthalten (z. B. Quectel EC21-E oder Quectel EG25-G).

Die GNSS-Funktionalität unterstützt Satellitennavigationssysteme wie GPS sowie – abhängig von der jeweiligen Modulvariante – zusätzliche Systeme wie GLONASS, Galileo und BeiDou.

Der GNSS-Empfänger arbeitet in den folgenden Frequenzbereichen:

1560 – 1610 MHz

1170 – 1210 MHz

Die GNSS-Funktion ist ausschließlich empfangend (keine Funkübertragung).

Hinweis: Die GNSS-Leistung hängt von der Antennenplatzierung, den Umgebungsbedingungen und der Sichtverbindung zu Satelliten ab. Für eine optimale Leistung wird die Verwendung einer geeigneten externen GNSS-Antenne mit freier Sicht zum Himmel empfohlen.

9.5 WLAN-Funktionen

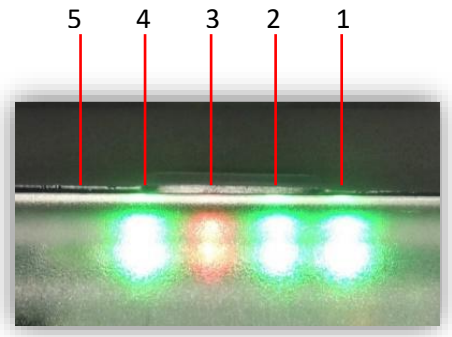
Das Gerät integriert ein 2,4-GHz-WLAN-Modul, das auf IEEE 802.11 b/g/n (Wi-Fi 4) basiert und für zuverlässige drahtlose Kommunikation in Embedded- und industriellen IoT-Anwendungen entwickelt wurde.

Varianten	Varianten mit WLAN
Funkmodul	Eingebettetes Modul mit IEEE 802.11 b/g/n im 2,4-GHz-Frequenzband (WiFi 4)
Frequenzbänder 2,4 GHz	2400 – 2483,5 MHz
Maximale HF-Ausgangsleistung	bis zu 20 dBm (100 mW)

10 Anschlüsse, Anzeigen und Betriebselemente

Die folgenden Abbildungen zeigen eine maximal ausgestattete Version des MC100. Je nach Variante hat Ihr MC100 möglicherweise nicht alle Anschlüsse, Anzeige- oder Steuerelemente.

10.1 Status LEDs



LED	Farbe	Name	Beschreibung
LED 1	Grün	Power	Anzeige der Spannungsversorgung
LED 2	Grün	Informationen	Anpassbar
LED 3	Rot	Warnung	Warnzustand (Unterspannungssituation, System-Upgrade im Gange, benutzerdefinierte Warnung)
LED 4	Grün	Modem (NET-LED)	Schnelles Blinken: Paketdatenübertragung Langsames Blinken: Auf der Suche nach Verbindung Dauerleuchten: Verbindung hergestellt
LED 5	Grün	Status	Blinken: Booten Dauerleuchten: Gerät betriebsbereit

10.1.1 NET-LED-Signalmuster

Diese LED zeigt den Status des integrierten GSM-Moduls an.

Blinkmuster	Netzwerkstatus
Off	Das Modem ist inaktiv
Kurzes Intervall (200 ms an, 1800 ms aus)	Netzwerksuche
Langes Intervall (1800 ms an, 200 ms aus)	Leerlaufzustand
Flackern (125 ms an, 125 ms aus)	Datenübertragung
Immer an	Aktive Verbindung

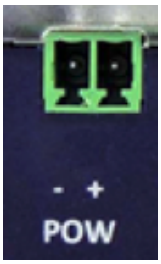
10.2 Taster

Name	Funktion
Reset	Wird verwendet, um das Gateway auf Werkseinstellungen zurückzusetzen
Nutzer	Anpassbar

10.3 Schnittstellen

Name	Steckverbinder	Beschreibung
POW	Klemmbuchse	Stromversorgung
GPIO	Klemmbuchse	Digitale I/O
RS485	Klemmbuchse	RS-485-Schnittstelle
CAN	Klemmbuchse	CAN 2.0B-Schnittstelle
ETH	RJ-45	Ethernet 10/100 Base-T
USB	USB-Typ-A-Buchse	USB-2.0-Hostschnittstelle
RS-232	DE-9 männlich	RS-232 serielle Schnittstelle

10.3.1 Spannungsversorgung (POW) & Netztrennung



Das Gateway kann mit LPS-Netzteilen betrieben werden, mit einer Versorgungsspannung von 8–30 V DC und einer Mindestleistung von 14 W. Die Ausgangsleistung kann als Produkt von Spannung und Strom berechnet werden. Zum Beispiel ist ein 12 V / 1,2 A-Netzteil geeignet, da seine maximale Leistung 14,4 W beträgt.

Eine LPS (Limited Power Source) ist eine Stromquelle, die die Anforderungen von IEC 62368-1 erfüllt, einschließlich Begrenzungen für Spannung (maximal 60 V DC) und Stromversorgung, um einen sicheren Betrieb zu gewährleisten.

Wenn ein externes Netzteil verwendet wird, das an das Netz angeschlossen ist, wird die Trennung vom Netz erreicht, indem die Stromversorgung vom Netz getrennt wird (z. B. durch das Trennen des Netzsteckers).

Die Trennungsmöglichkeit muss jederzeit leicht zugänglich sein.

Warnung: Stellen Sie sicher, dass die Polarität korrekt ist, da sonst das Gerät beschädigt werden könnte.

Port	Beschreibung
POW -	Spannungsversorgung, Minuspol
POW +	Spannungsversorgung, Pluspol

10.3.2 RS485

Warnung: Die Basis-RS-485-Schnittstelle ist nicht galvanisch isoliert.

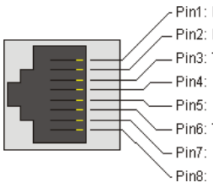
Port	Beschreibung
-/A	Invertierte Leitung (A)
+/B	Nicht-invertierte Leitung (B)
GND	GND

10.3.3 CAN

Warnung: Die Basisschnittstelle CAN 2.0 B ist nicht galvanisch isoliert.

Port	Beschreibung
CH	CAN High
CL	CAN Low
GND	GND

10.3.4 Ethernet



Port	Signal	Beschreibung
1	TD+	TX+ (Senden+)
2	TD-	TX– (Senden -)
3	RD+	RX+ (Empfangen +)
4	CAPa	Interne 100 nF Kapazität zu GND
5	CAPb	Interne 100 nF Kapazität zu GND
6	RD-	RX– (Empfangen -)
7	Nicht verbunden	
8	Schirm	

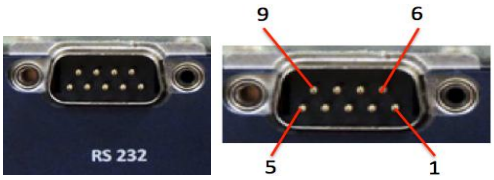
LED (Pos.)	Signal	Beschreibung
Links	GESCHWINDIGKEIT	1 blinkt: LED blinkt einmal = 10 Basislink 2 Blitze: LED-Blinker zweimal = 100Base-Link
Rechts	LINK	ON: Netzwerkverbindung wurde hergestellt Blinken: Netzwerkaktivität wurde erkannt

10.3.5 USB

Der USB-2.0-Anschluss ist eine Standard-Typ-A-Buchse.

10.3.6 RS-232

Der RS-232-Anschluss ist eine DSUB-9-Männchenbuchse (DCE).



Port	Signal	Beschreibung
2	TXD (AUS)	Sendeleitung (des Modems)
3	RXD (IN)	Empfangsleitung (des Modems)
5	GND	GND
7	RTR / RTS (IN)	Bereit zum Empfangen / Anfrage zum Senden (Terminal ist bereit zum Empfang)
8	CTS (AUS)	Clear To Send (Modem ist bereit zum Empfang)

Hinweis: Ein Hardware-Handshake über die RS-232-Schnittstelle ist nicht möglich.

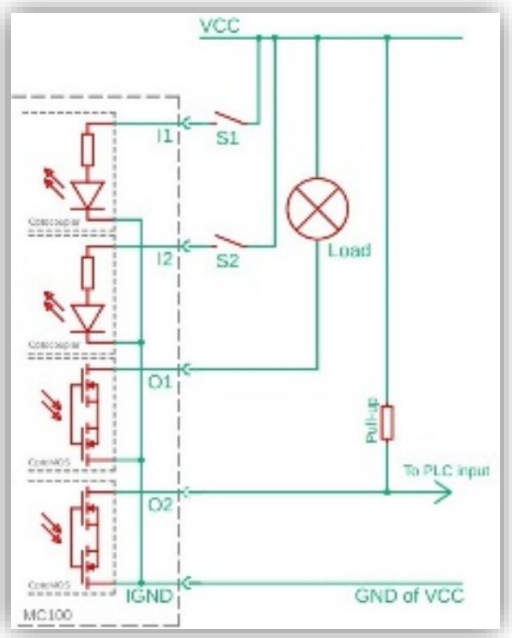
10.3.7 Digitale IOs (GPIO)

Die digitalen Ausgänge ermöglichen es, eine Last von bis zu 120 mA RMS/DC mit einer maximalen Spannung von 30 V DC (Relais, LED usw.) direkt zu steuern oder ein Signal (z. B. SPS) zu schalten. Im aktiven Zustand verbindet er den Ausgang mit der isolierten Massereferenz (IGND) über eingebaute Halbleiterrelais (OptoMOS). Ansonsten ist die Verbindung High-Z.

Die digitalen Eingänge können ein DC-Spannungssignal > 6V (aktiv-hoch, maximal 30 V DC) in Bezug auf die isolierte Massereferenz (IGND) mit Hilfe von Optokopplern detektieren.

Die Schaltung wird in der untenstehenden Abbildung dargestellt.

Port	Beschreibung
I1	Digitaleingang 1, DC-Spannung 0 bis 30V, Schaltschwelle ca. 0,6V DC
I2	Digitaleingang 2, DC-Spannung 0 bis 30V, Schaltschwelle ca. 0,6V DC
O1	Digitaler Ausgang 1, Schaltkapazität maximal 300 mA
O2	Digitaler Ausgang 2, Schaltkapazität maximal 300 mA
IGND	I/O-Masse, elektrisch isoliert vom Standard-GND des Geräts



10.3.8 Antennenverbinder

Alle Antennenstecker sind vom Typ SMA-Buchse.

Port	Beschreibung
LTE	Haupt LTE-Antennen SMA-Buchse
DIV	Diversity LTE-Antenne SMA-Buchse
GPS	GPS-Antenne SMA-Buchse
WLAN	WLAN-Antenne SMA-Buchse

10.3.9 SIM-Kartensteckplatz

Port	Beschreibung
SIM	SIM-Kartensteckplatz

10.4 MC100 GPIO-Anschlussbelegung

Detaillierte Pinouts finden Sie im Kapitel "*Wired Interfaces".*

Port	Beschreibung
Isolierte Eingänge	8 digitale Eingänge
Isolierte Ausgänge	8 digitale Ausgänge (PhotoMOS-Solid-State-Relais)
0 – 10 V	2 analoge Eingänge von 0 bis 10 V
0 – 20 mA	2 analoge Eingänge 0 bis 20 mA
PWM	1 Open-drain PWM-Ausgang (Pulse Width Modulation)

10.5 MC100 SensT2-Anschlussbelegung

Detaillierte Pinouts finden Sie im Kapitel "*Wired Interfaces".*

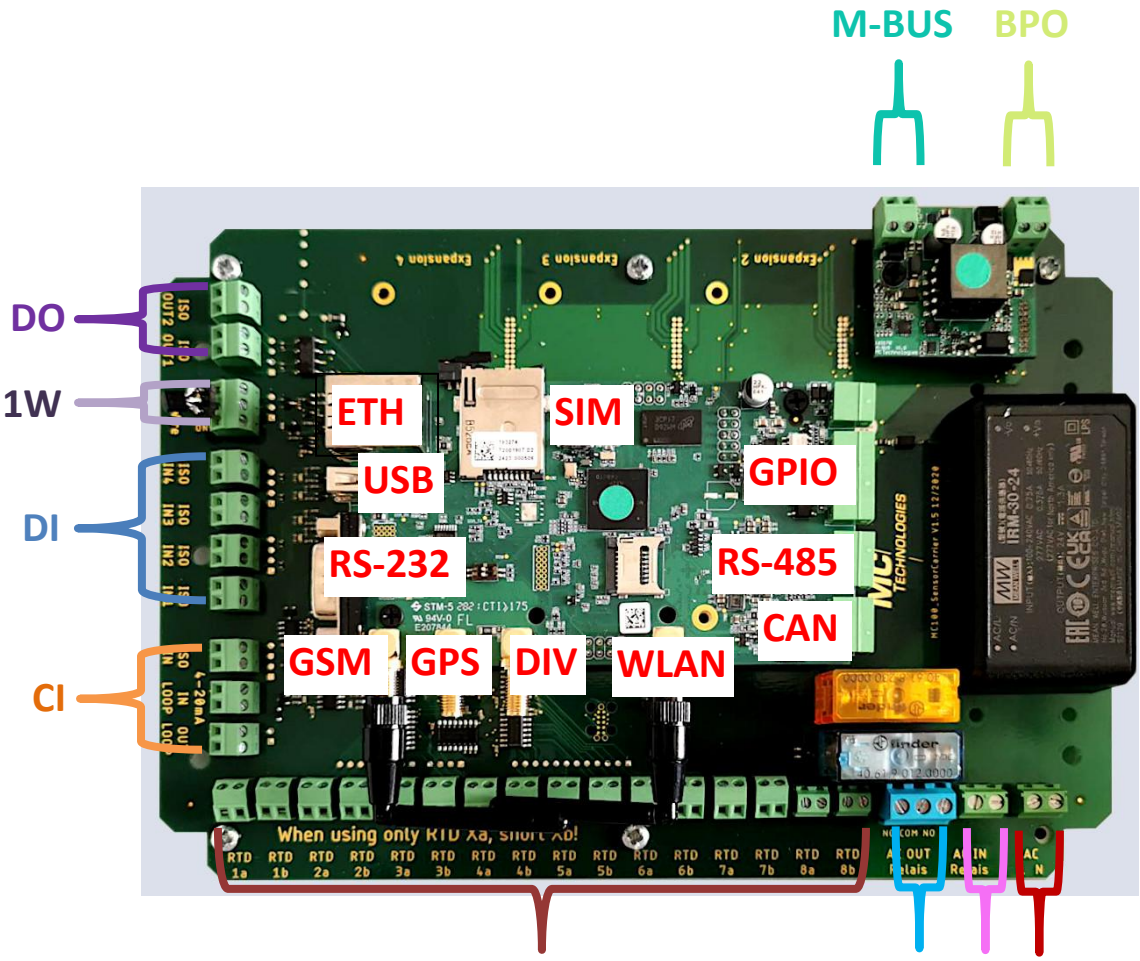
Port	Beschreibung
Isolierter RS-485	1 x serielle RS-485-Schnittstelle (galvanisch isoliert)
Isolierte Eingänge	8 x digitale Eingänge
Isolierte Ausgänge	2 x digitale Ausgänge (OptoMOS Transistorrelais)
PT100/PT1000	4 x PT100/PT1000 Eingänge
4–20 mA-Ausgänge	2 x analoge 4 – 20 mA Ausgänge
0 – 10 V	2 x analoge Eingänge 0 – 10 V
4 – 20 mA LS	2 x analoge Eingänge: 4 – 20 mA LS (Loop Supply)
1-Wire	1 x 1-Wire-Bus

10.6 MC100 SensorBox Anschlussbelegung

Die SensorBox benötigt zertifizierte Techniker für Installation und Wartung. Bitte beachten Sie das Kapitel zur elektrischen Sicherheitsanforderungen am Anfang dieses Dokuments sowie die speziellen Installationsanweisungen im Kapitel *Installation.*

Detaillierte Pinouts finden Sie im Kapitel "*Wired Interfaces*".

Warnung: Schließen Sie die Stromversorgung der Leiterplatte und des Wechselstromeingangs nicht gleichzeitig an!



RTD OUT IN SUP

Port	Beschreibung
RS-485	Galvanisch isolierte RS-485-Schnittstelle
DI	Galvanisch isolierter digitaler Eingang (aktiv-hoch, 5 ... 30 V DC)
DO	Galvanisch isolierter digitaler Ausgang (verwendet PhotoMOS-Solid-State-Relais)
1W	1-Wire-Bus
IN	230 V elektromagnetisches Eingangsrelais
OUT	230 V elektromagnetisches Ausgangsrelais
SUP	85 … 264 V Wechselstrom-Einlass
CI	4–20 mA Stromeingang
M-BUS	M-Bus-Master-Schnittstelle
BPO	M-Bus-Stromversorgung

11 Installation

11.1 Antenne

Installieren Sie die mitgelieferte Antenne am SMA-Anschluss der MC100. Prüfen Sie, ob die lokale Netzabdeckung des Mobilfunkanbieters ausreichend ist.

Warnung: Personen müssen sich während des Gerätebetriebs mindestens 20 cm von der Antenne entfernt befinden.

11.2 SIM-Karte einsetzen

Schalten Sie das Netzteil aus und entfernen Sie alle Verbindungskabel, bevor sie die Mini-SIM-Karte in den Schlitz an der Seite stecken. Achten Sie dabei auf den Schiebeverriegelungsmechanismus.

11.3 Fahrzeuginstallation

Die Installation des MC100, seiner Peripherie wie Kabel und Antennen sowie der elektrischen Verbindungen in einem Kraftfahrzeug muss von einer qualifizierten Fachwerkstatt durchgeführt werden. Nur MC100 mit E1-Zertifizierung dürfen in Fahrzeugen installiert oder betrieben werden (auf dem Typenschild vermerkt).

11.4 SensorBox-Installation

Da die SensorBox ein Produkt für IP65-Installationen mit relativ hohen Spannungen ist, ist besondere Sorgfalt geboten. Für Installation und Wartung sind zertifizierte Techniker erforderlich. Neben den elektrischen Sicherheitsanforderungen zu Beginn dieses Dokuments müssen Folgendes sorgfältig beachtet werden:

- Die SensorBox darf für Kinder nicht zugänglich sein
- Stellen Sie sicher, dass das Gerät vor dem Öffnen vom Stecker getrennt ist
- Es besteht eine Lebensgefahr durch spannungsführende Teile
- Stellen Sie sicher, dass alle Kabel eine ausreichende Dehnentlastung haben
- Das Gerät muss durch einen zusätzlichen externen, allpoligen Leistungsschalter geschützt werden, der in der elektrischen Installation des Gebäudes installiert ist
- Achten Sie darauf, dass die Kabelverschraubungen und Dichtungen im Deckel korrekt passen
- Achten Sie darauf, dass kein Spritzwasser die Elektronik erreicht
- Das Gehäuse muss mit Schrauben an der Wand befestigt werden, bevor das Gerät in Betrieb genommen wird
- Die SensorBox wird mit 4 Schrauben an einer geeigneten Wand montiert
- Die Löcher befinden sich an den Ecken des Gehäuses und sind für Schrauben mit bis zu 4 mm Durchmesser geeignet.
- Die Montagefläche der Box ist 300 x 230 mm groß
- Die Gehäusebasis der SensorBox sollte gleichmäßig an der Wand abliegen, um Schäden zu vermeiden
- Die Abstände zwischen den Löchern sind in den Zeichnungen im *Kapitel Dimensionen* zu finden
- Eine Montagehöhe von 160 bis 180 cm vom Boden bis zur unteren Kante des Gehäuses wird empfohlen

- Um Schutz vor Wassereintritt zu gewährleisten, sollte die SensorBox so montiert werden, dass die Kabelanschlüsse nach unten zeigen

12 Software

12.1 OpenWrt

Das Betriebssystem des MC100 basiert auf OpenWrt. OpenWrt ist eine äußerst anpassbare und erweiterbare GNU/Linux-Distribution, die von Netzwerktechnologie-Enthusiasten und Fachleuten für Gleichgesinnte entwickelt wurde. Das volle Potenzial von OpenWrt zu entfalten, erfordert die Bereitschaft des Nutzers zu experimentieren und zu forschen, da es kaum möglich ist, einen vollwertigen thematischen Leitfaden zu erstellen.

Daher können die in diesem Leitfaden vorgestellten Konfigurations- und Anwendungsbeispiele nicht mehr als eine Einleitung betrachtet werden, die mit bester Bemühung erstellt wurde, ohne Haftung für Schäden oder jegliche Garantien für Genauigkeit und Aktualität.

12.2 Verwendung von Open-Source-Software

Dieses Produkt umfasst Open-Source-Software, die teilweise von Dritten entwickelt und mit einer permissiven Lizenz verteilt wurde. Die Nutzung dieser Software ist laut den Bedingungen der jeweiligen Lizenz gebührenfrei. Im Falle eines Widerspruchs zwischen unseren Bedingungen und den Softwarelizenzbedingungen haben die Softwarelizenzbedingungen Vorrang, soweit die Software betroffen ist.

Die Nutzung der Open-Source-Software ist kostenlos. Wir erheben keine Nutzungsgebühren oder vergleichbare Gebühren für die Open-Source-Software in unseren Produkten.

Um eine Liste der im Produkt verwendeten Open-Source-Software abzurufen, wenden Sie sich bitte an unsere Support-Abteilung (support@mc-technologies.com). Alternativ ist eine Liste der verwendeten Open-Source-Software in der Weboberfläche *unter System -> Software -> Installed zu* finden.

Kunden können den Quellcode der in unserem Produkt enthalten en Software anfordern, wobei die Lizenz vorschreibt, dass der Quellcode und/oder Änderungen dem Kunden zur Verfügung gestellt werden müssen. Beispiele für solche Lizenzen sind die GNU General Public License (GPL), die GNU Lesser General Public License (LGPL) und die Clarified Artistic License. Wir behalten uns das Recht vor, eine Entschädigung für die Vertriebskosten des Quellcodes zu verlangen, falls anwendbar (z. B. Portogebühren und die Kosten des Mediums).

12.3 Softwareentwicklungskit (SDK)

Auf Anfrage stellt MC Technologies Kunden ein SDK auf Basis des OpenWrt SDK zur Verfügung, um individuelle Softwarelösungen auf dem Gerät zu kompilieren und auszuführen.

12.4 Haftung für Software

Wir übernehmen jedoch keine Garantie oder Haftung für Änderungen an der Software, die vom Kunden oder Dritten vorgenommen werden, oder für die Nutzung der Open-Source-Software unseres Produkts in einer Weise, die nicht mit der beabsichtigten Verwendung gemäß der beiliegenden Dokumentation oder, falls zutreffend, dem vertraglich definierten Anwendungszweck des Produkts übereinstimmt.

Dies gilt ebenso für jede Nutzung der Open-Source-Software außerhalb unseres Produkts.

13 Grundlegende Routinen

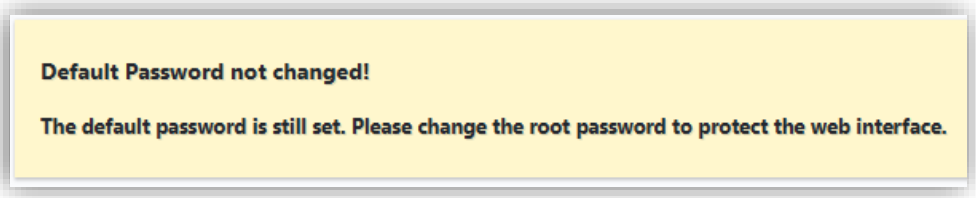
13.1 Zugriff auf die Weboberfläche

Das Gateway kann über seine integrierte Weboberfläche konfiguriert werden. Um auf die Weboberfläche zuzugreifen, verbinden Sie bitte den Computer mit einer der LAN-Schnittstellen des Gateways.

- Wenn entsprechend konfiguriert, erhält der Computer automatisch eine IP-Adresse mittels DHCP
- Am Computer öffnen Sie einen Webbrowser und navigieren Sie zu *https:// 192.168.2.1*
- Eine Anmeldeaufforderung erscheint.
- Folgende Standard-Anmeldedaten sind erforderlich:
  - Benutzername: root
  - Passwort: Tech#5GR
- Das Standardpasswort muss unmittelbar nach dem ersten Login und vor der Verbindung des Geräts mit einem Netzwerk geändert werden.
- Aus Sicherheitsgründen darf das Gerät nicht mit Standardzugangsdaten betrieben werden.

13.2 Passwort ändern

Nach dem ersten Einloggen müssen Sie ein neues Passwort erstellen. Andernfalls können Sie keine weiteren Seiten öffnen.



13.3 Zugriff über SSH

SSH kann verwendet werden, um auf die Linux-Kommandozeile des Gateways zuzugreifen. Für einen bequemen Zugang wird ein dediziertes Terminalprogramm wie z.B. Putty empfohlen.

Alternativ beinhalten Linux-Systeme und neuere Windows-Systeme bereits ein SSH-Programm, das in die Befehlsstruktur integriert ist. Unter Windows kann die Kommandozeile geöffnet werden, indem man **Windows+r** drückt und im Ausführen-Prompt *cmd* eingibt. Um eine SSH-Verbindung herzustellen, führen Sie bitte folgendes aus:

ssh root@192.168.2.1

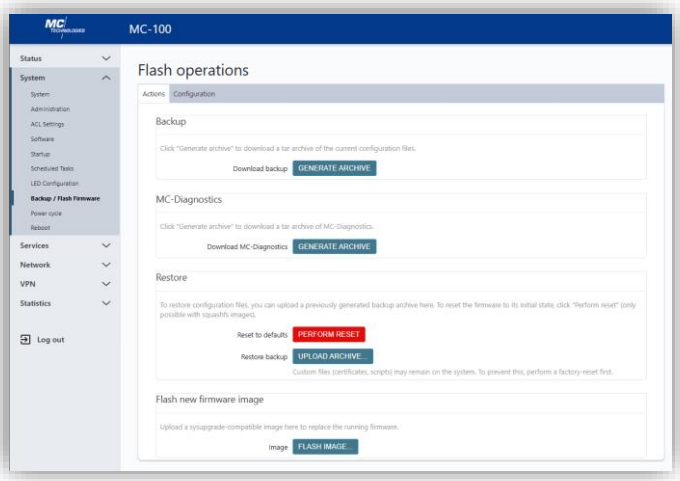
Dabei ist root der Benutzername und 192.168.2.1 die IP-Adresse des Gateways. Vorausgesetzt, ein Passwort wurde festgelegt, werden Sie beim erfolgreichen Verbindungsversuch nach dem Passwort gefragt.

13.4 Flash-Operationen

In System *->Backup / Flash* können Firmware-Updates durchgeführt und Konfigurations-Backups erstellt und wiederhergestellt werden.

13.4.1 Konfigurations-Backup

Backup-Archive mit den Konfigurationsdateien können hier heruntergeladen werden. Diese Archive können später hochgeladen und wiederhergestellt oder auf ein anderes Gerät desselben Typs mit einer entsprechenden Firmware-Version bereitgestellt werden. Backups dürfen nicht auf verschiedenen Modellen oder Geräten mit unterschiedlichen Firmware-Versionen wiederhergestellt werden, da nicht garantiert werden kann, dass das Konfigurationsformat identisch ist. Dies kann zu nicht nachverfolgbaren Fehlern, Systeminstabilitäten und sogar Sicherheitsproblemen führen.

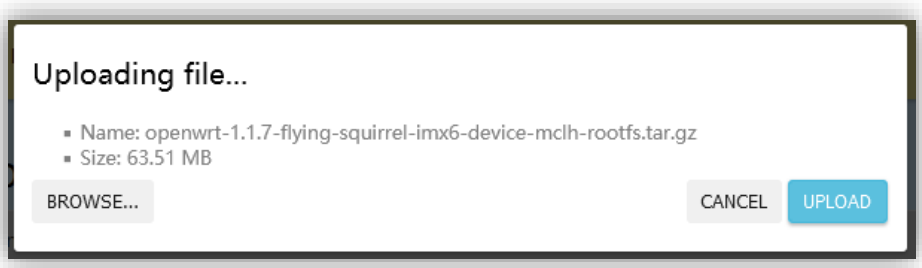


13.4.2 Firmware-Upgrade

Die Firmware-Upgrade-Funktionalität ermöglicht es, die Betriebssystembasis zu aktualisieren. Das bedeutet, dass nicht nur Softwarepakete, sondern auch kritische Systemkomponenten aktualisiert

werden. Daher wird dringend empfohlen, im Vorfeld zu prüfen, ob der Upgrade-Prozess in einer simulierten Umgebung funktioniert, die der realen Installation ähnelt, und die Geräte physisch zugänglich zu halten, um die Fehlersuche beim Upgrade durchzuführen. Dies verhindert Ausfälle und unnötige Servicearbeiten. Die aktuellen Updates der Geräte sind unerlässlich, um die neuesten Funktionen, Sicherheits- und Stabilitätsupdates zu erhalten.

Um die Firmware zu aktualisieren, klicken Sie auf FLASH IMAGE... klicken Sie dann auf DURCHSUCHEN, wähle die Firmware-Update-Datei aus und klicken Sie dann auf HOCHLADEN. Das Hochladen der Firmware-Datei kann eine Weile dauern. Ein Abbruch des Vorgangs ist hier immer noch sicher.

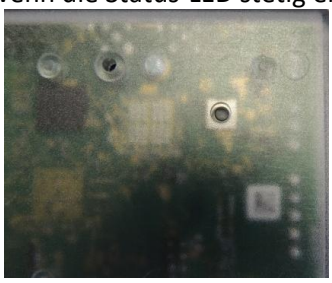


Nachdem die Firmware hochgeladen wurde, zeigt ein neuer Dialog die Prüfsumme der Datei zur Bestätigung an. Der Upgrade-Prozess kann durch Klicken auf die Schaltfläche "Fortsetzen" gestartet werden. Schalten Sie das Gateway während des Upgrades nicht aus. Nach kurzer Zeit startet das Gerät neu und führt weitere Migrationsroutinen durch, die bis zu 10 Minuten dauern können. Das Upgrade ist abgeschlossen, sobald die Weboberfläche wieder erreichbar ist.

13.5 Werkseinstellungen

WARNUNG: Alle Dateien werden gelöscht und die Benutzereinstellungen auf Werkseinstellungen zurückgesetzt. Bitte stellen Sie sicher, dass das Gerät physisch barrierefrei zur Fehlerbehebung ist.

- Suchen Sie den Reset-Taster auf der Rückseite des MC100
- Trennen Sie die Stromversorgung
- Verwenden Sie z. B. eine Büroklammer, um den Reset-Taster zu drücken und gedrückt zu halten
- Schließen Sie das Netzteil an, während Sie den Taster gedrückt halten.
- Lassen Sie den Taster los, nachdem die Status-LED etwa eine Sekunde lang schnell blinkte
- Nach etwa 10 Sekunden beginnt die Status-LED langsam zu blinken
- Das Gerät ist einsatzbereit, wenn die Status-LED stetig eingeschaltet bleibt



14 Kabelgebundene Schnittstellen

Dieses Kapitel soll ein grundlegendes Verständnis vermitteln, und gibt Empfehlungen für die Nutzung der kabelgebundenen Schnittstellen, insbesondere für die Linux-spezifische Implementierung. Für modellspezifische Beschreibungen der Steckverbinder (und Pinouts der Basis) schauen Sie *sich das Kapitel Ports, Display und Bedienelemente an.* Informationen zur Nutzung der Schnittstellen mit Node-RED finden Sie in den entsprechenden *Node-RED-Kapiteln.*

Bitte beachten Sie: Linux repräsentiert viele Schnittstellengeräte durch eine "virtuelle" Dateistruktur. Die Interaktion mit diesen Schnittstellen ist so einfach wie das Lesen oder Schreiben anderer Dateien. In diesem Kapitel werden in Tabellen, die Dateipfade sowie das Ein- und Ausgabeformat für Schnittstellen beschrieben.

Zum Beispiel wird der Wert vom digitalen Eingang 1 abgelesen:

```
root@MC100:~# cat /sys/class/gpio/mc100:in1/value

0
```

Der Befehl gibt 0 aus, was bedeutet, dass der Signalpegel des digitalen Eingangs in diesem Fall "low" ist.

Ebenso schaltet das Schreiben einer 1 in die entsprechende Datei des digitalen Ausgangs 2 den Ausgang ein.

```
root@MC100:~# echo 1 > /sys/class/gpio/mc100:out2/value /
```

14.1 RS-232

Obwohl serielle Schnittstellen in Linux ebenfalls als Dateien dargestellt werden, benötigen sie spezielle Programme oder Bibliotheken, mit denen interaktiv interagiert wird, und spezifizieren daher Einstellungen wie Baudrate (z. B*. picocom).*

14.2 RS-485

Die RS-485-Schnittstelle */dev/ttymxc4* kann wie jedes andere Standard-Linux-Seriellgerät verwendet werden.

14.3 1-Wire

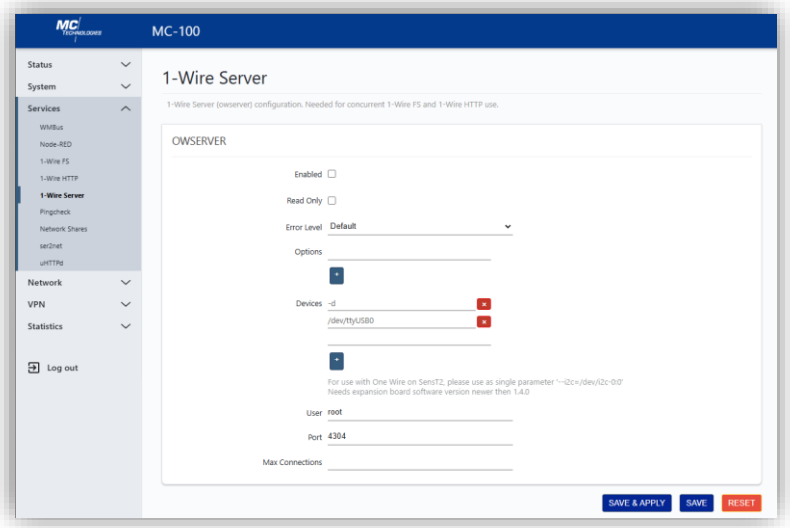
Der 1-Wire-Treiber wird während des Bootvorgangs automatisch geladen und gestartet.

Für Linux-Nutzer ist das vorinstallierte OWFS 1-Wire-Dateisystem wahrscheinlich die intuitivste Möglichkeit, mit 1-Wire-Geräten zu kommunizieren.

14.3.1 OWServer

Der Owserver kann über die LuCI-Weboberfläche aktiviert werden:

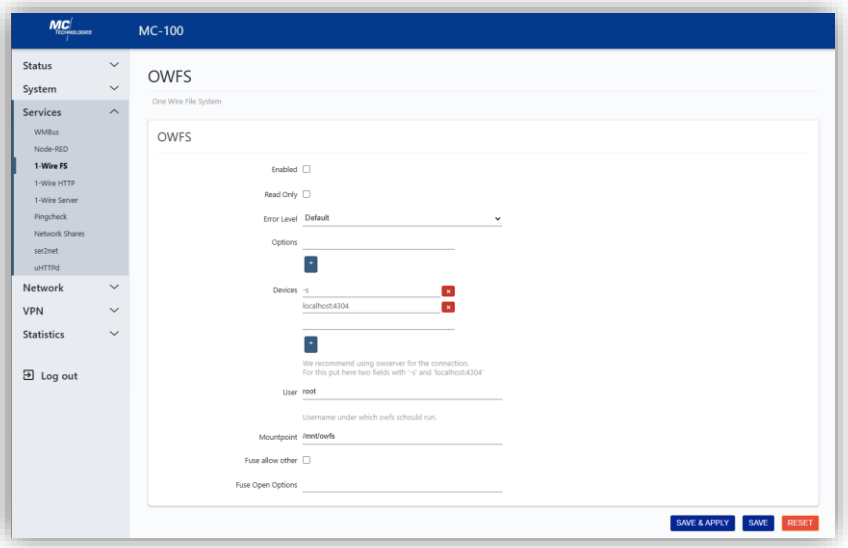
1. Navigieren Sie zum Services->1-Wire Server
2. Aktivieren Sie das *Kontrollkästchen* aktiviert
3. Stellen Sie *Geräte* ein: -i2c=/dev/i2c-0:0
4. Ändern Sie den *Port* nach Belieben (standardmäßig ist 4304)
5. Klicken Sie auf SPEICHERN&ANWENDEN



14.3.2 OWFS

OWFS kann über die LuCI-Weboberfläche aktiviert werden:

1. Navigieren Sie zu Services->1-Wire FS
2. Aktivieren Sie das Kontrollkästchen aktiviert
3. Der Mount-Punkt kann nach Belieben geändert werden (standardmäßig ist /mnt/owfs)
4. Klicken Sie auf SPEICHERN&ANWENDEN



Die Abstraktion des 1-Wire-Dateisystems kann dann in /mnt/owfs gefunden werden.

Eine Auflistung des Ordners zeigt die verfügbaren Geräte als Unterordner:

```
root@MC100:~# ls /mnt/owfs/

10.0702A3030800/ Alarm/ Einstellungen/ Statistik/

10.5B94A3030800/ bus.0/ simultaneous/ Struktur/ nicht gecacht/
```

Die Unterordner enthalten typspezifische Dateien, um mit dem Gerät zu interagieren, das in diesem Beispiel ein Temperatursensor ist:

```
root@MC100:~# ls /mnt/owfs/10.0702A3030800/

Adresse der CRC8-Familie – neueste Temp Power r_id Scratchpad Temphigh Typ Alias
Errata ID Locator r_address r_locator Temperatur Templow
```

Die Temperatur zu messen ist unkompliziert:

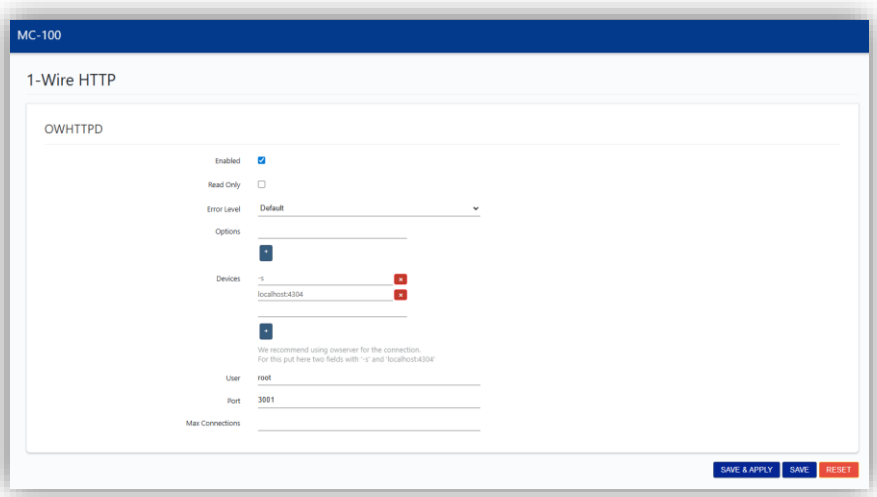
```
root@MC100:~# cat /mnt/owfs/10.0702A3030800/temperatur

24.5625
```

14.3.3 Owhttpd

OWFS stellt einen kleinen Webserver bereit, der den Dallas/Maxim 1-Wire-Bus an einen seriellen Anschluss anzeigt. Die Hauptseite zeigt die gefundenen Geräte. Es ermöglicht es, die Eigenschaften der Geräte anzuzeigen und zu ändern.

Der Server kann wie folgt aktiviert werden:

1. Navigieren Sie zu Services->1-Wire HTTP
2. Aktivieren Sie das *Kontrollkästchen* aktiviert
3. Der Port kann nach Belieben geändert werden (Standardversion ist 3001).
4. Klicken Sie auf SPEICHERN&ANWENDEN



Man kann die owhttpd-Weboberfläche mit derselben Adresse wie die Standard-Weboberfläche erreichen, indem man den Port angibt (z. B. 3001).

Beispiel mit Standard-IP-Adresse: https://192.168.2.1:3001

14.4 M-Bus

Das MC100-Terminal/Gateway kann mit einem M-Bus-Modul ausgestattet werden, das die Kommunikation mit verschiedenen Arten von Sensoren (Wärmekostenzuteiler, Stromzähler usw.) ermöglicht.

Die M-Bus-Schnittstelle */dev/ttymxc2* kann wie jedes andere Standard-Linux-Seriellgerät verwendet werden. Die Einstellungen für M-Bus sind 8 Datenbits, keine Parität und 1 Stoppbit. Die meisten M-Bus-Geräte kommunizieren mit einer Baudrate von 2400 Baud.

Mehrere auf libmbus basierende Programme für die Kommunikation mit M-Bus sind vorinstalliert:

- mbus-serial-request-data-multipli-reply
- mbus-serial-request-data
- mbus-serial-scan
- MBUS-Serien-Scan-Sekundär
- MBUS-Serial-Set-Adresse
- MBUS-Serial-Select-Secondary
- mbus-serial-switch-baudrate

Verwenden Sie den Parameter -h für eine kurze Erklärung der Programme und ihrer Parameter.

Um die verbundenen Geräte aufzulisten, führen Sie aus:

```
root@MC100:~# mbus-serial-scan -b 2400 /dev/ttymxc2
```

Um Daten von Gerät 10 anzufordern, führen Sie aus:

```
root@MC100:~# mbus-serial-request-data -b 2400 /dev/ttymxc2 10
```

14.5 CAN

Der CAN-Schnittstellen-Linux-Kernel-Stack heißt SocketCAN. CAN-Geräte werden wie Netzwerkgeräte mit speziellen Flags, Einschränkungen und Nutzungsanforderungen behandelt, die beachtet werden müssen.

Eine Reihe spezieller Programme namens *can-utils* ist vorinstalliert, um eine bequeme Nutzung des CAN-Busses zu ermöglichen.

14.5.1 Aktivierung der CAN-Schnittstelle

Die CAN-Schnittstelle muss vor der Nutzung wie jedes andere Netzwerkgerät aktiviert werden. Der folgende Befehl veranschaulicht dies bei der Einstellung der Bitrate (Geschwindigkeit des CAN-Busses – 500 kbit/s in diesem Beispiel) und der Fehlerwiederherstellungszeit (Zeit in ms, nach der nach einem Fehlerfall ein Neustart des Geräts versucht wird):

```
root@MC100:~# IP-Link gesetzt ext-can1 up-Typ kann Bitrate 500000 restart-ms 1000
```

Um einen Standard-CAN-Rahmen mit 0x101 als ID und 0x41, 0x42, 0x43 0x44 als 4-Byte-Nutzlast zu senden, tippen Sie:

```
cansend vcan0 101#41424344
```

Um einen erweiterten Rahmen mit 0xA1B2 als ID zu senden, geben Sie folgenden Befehl an:

```
cansend vcan0 0000A1B2#3450
```

Um alle eingehenden Can-Frames auf vcan0 zusammen mit Zeitstempeln zu erfassen, geben Sie ein:

```
candump -t Absolute vcan0
```

Der Schnittstellenname kann beliebiger sein, um alle Schnittstellen zu erfassen, wie folgt:

```
candump -t A any
```

Um alle erfassten Frames in einer Logdatei zu speichern, verwenden Sie folgenden Befehl:

```
candump -l vcan0
```

14.6 Digitale Eingänge

Die MC100-Basis verfügt über zwei digitale Eingänge. Die Eingänge sind hoch aktiv.

Port	Parameter	Lesen	Schreib	Verlauf
I1	1,0	x		/sys/class/gpio/mc100:in1/value
I2	1,0	x		/sys/class/gpio/mc100:in2/value

Beispiel: Eingang I1 lesen

Befehl: cat /sys/class/gpio/mc100:in1/value

Antwort: 1# oder. 0#

14.7 Digitale Ausgänge

Die MC100-Basis verfügt über zwei digitale Ausgänge. Die Ausgänge sind Halbleiterrelais (Solid-State-Relais) und schalten gegen IGND.

Port	Parameter	Lesen	Schreib	Verlauf
O1	1,0		x	Echo 1 > /sys/class/gpio/mc100:out1/value
				echo 0 > /sys/class/gpio/mc100:out1/value
O2	1,0		x	Echo 1 > /sys/class/gpio/mc100:out2/value
				echo 0 > /sys/class/gpio/mc100:out2/value

Beispiel: O1-Schalten Sie einschalten

Befehl: Echo 1 > /sys/mc100_gpios/OUT1

Antwort: #

14.8 MC100 GPIO kabelgebundene Schnittstellen

14.8.1 Digitale Eingänge

Port	Beschreibung
DGND1	Digital Ground1, elektrisch isoliert auf alle (D)GND
I1 bis I4	Digitale Eingänge Eingangsspannung: 0 bis 30V Wechselschwelle: ~ 36.. 6V Alle Eingangsspannungen mit DGND1 als Masse
VPU1	Nicht unterstützt, bitte verbinden Sie kein Signal
DGND2	Digitaler Masse 2, elektrisch isoliert auf alle (D)GND

I1 bis I4	Digitale Eingänge Eingangsspannung: 0 bis 30V Schaltschwelle: 37pprox.. 6V Alle Eingangsspannungen mit DGND2 als Masse
VPU2	Nicht unterstützt, bitte verbinden Sie kein Signal

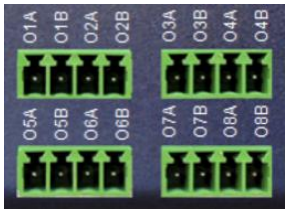
Port	Parameter	Lesen	Schreib	Verlauf
I1	1,0	X		/sys/gpio_board/input/1
I2	1,0	X		/sys/gpio_board/input/2
I3	1,0	X		/sys/gpio_board/input/3
I4	1,0	X		/sys/gpio_board/input/4
I5	1,0	X		/sys/gpio_board/input/5
I6	1,0	X		/sys/gpio_board/input/6
I7	1,0	X		/sys/gpio_board/input/7
I8	1,0	X		/sys/gpio_board/input/8

Beispiel: Lesen Sie Eingabe I1 aus

Befehl: cat /sys/gpio_board/input1/value

Antwort: z. B. 1# oder 0#

14.8.2 Digitale Ausgänge



Wie die grundlegenden digitalen Ausgänge sind die zusätzlichen digitalen Ausgänge des MC100 GPIO galvanisch isolierte Festkörperrelais. OxA ist mit einem Pin des Relais verbunden, OxB mit dem anderen Pin. Der maximale Schaltstrom beträgt 300 mA (maximal 30 V Gleichstrom).

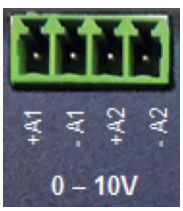
Port	Parameter	Lesen	Schreib	Verlauf
O1A,O1B	1,0		X	/sys/gpio_board/output/1
O2A, O2B	1,0		X	/sys/gpio_board/output/2
O3A,O3B	1,0		X	/sys/gpio_board/output/3
O4A,O4B	1,0		X	/sys/gpio_board/output/4
O5A,O5B	1,0		X	/sys/gpio_board/output/5
O6A,O6B	1,0		X	/sys/gpio_board/output/6
O7A,O7B	1,0		X	/sys/gpio_board/output/7
O8A,O8B	1,0		X	/sys/gpio_board/output/8

Beispiel: Schalten Sie den Ausgang O1A, O1B ein

Befehl: Echo 1 > /sys/gpio_board/output/value

Antwort: #

14.8.3 Spannungseingänge 0 – 10 V



Der Eingangsstrom bei 10V beträgt ca. 2 mA. Die angelegte Gleichspannung darf 10 V nicht überschreiten.

Port	Beschreibung
+A1	Positive Verbindung Eingang 1
-A1	Negative Verbindung Eingang 1
+A2	Positive Verbindung Eingang 2
-A2	Negative Verbindung Eingang 2

Port	Parameter	Lesen	Schreib	Verlauf
+A1,-A1	Wert	x		/sys/gpio_board/ voltage_in/1
+A2,-A2	Wert	x		/sys/gpio_board/ voltage_in/2

Beispiel: Lesespannung am ADC-Eingang +A1,-A1

Befehl: cat /sys/gpio_board/ voltage_in1/value

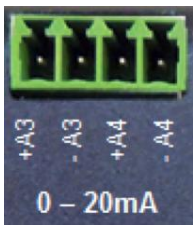
Antwort: z. B. 6400

Hinweis: Umwandlung in Volt

Formel: Spannung in Volt = Wert / 1000

Beispiel: Wert = 6400 entspricht 6,4V

14.8.4 Stromeingänge 0 – 20 mA



Ein Strom von bis zu 20 mA von einer Konstantstromquelle kann in diese Eingänge eingespeist werden.

Port	Beschreibung
+A3	Positive Verbindung Eingang 3
-A3	Negative Verbindung Eingang 3
+A4	Negative Verbindung Eingang 4
-A4	Negative Verbindung Eingang 4

Port	Parameter	Lesen	Schreib	Verlauf
+A3,-A3	Wert	x		/sys/gpio_board/current_in/3
+A4,-A4	Wert	x		/sys/gpio_board/current_in/4

Port	
Kommando	cat /sys/gpio_board/current_in1/value
Reaktion	z. B. 2000

Hinweis: Konvertierung auf mA

Formel: Strom in mA = Wert / 200
Beispiel: Wert = 2000 entspricht 10 mA

14.8.5 PWM

Der PWM-Ausgang (Pulse Width Modulation) ist Open-Drain. Das bedeutet, es verbindet sich mit GND. Für ein aktiv-hoch Signal ist ein Pull-up-Widerstand erforderlich.

Port	Beschreibung
GND	GND
PW2	Open Drain digitaler Ausgang.
PW1	Open Drain digitaler Ausgang.
PU	Eingang für interne Schutzdiode (Freilaufdiode) für induktive Lasten. (positive Versorgungsspannung)

Port	Parameter	Lesen	Schreib	Verlauf
PW2	Prescaler {0,1023}		x	/sys/gpio_board/pwm/prescalar
	Pulse {0,65535}			/sys/gpio_board/pwm/1
PW1	Prescaler {0,1023}		x	/sys/gpio_board/pwm/prescalar
	Pulse {0,65535}			/sys/gpio_board/pwm/2
	Period*{0,65535}		x	/sys/gpio_board/pwm/Punkt

14.9 MC100 SensT2 kabelgebundene Schnittstellen

14.9.1 Digitale Eingänge

Port	Beschreibung
DGND1	Digital Ground1, elektrisch isoliert auf alle (D)GND
I1 bis I4	Digitale Eingänge Eingangsspannung: 0 bis 30V Schaltschwelle: ca. 6V Alle Eingangsspannungen mit DGND1 als Masse
VPU1	Nicht unterstützt, bitte verbinden Sie kein Signal

DGND2	Digitaler Masse 2, elektrisch isoliert auf alle (D)GND
I1 bis I4	Digitale Eingänge Eingangsspannung: 0 bis 30V Schaltschwelle: ca. 6V Alle Eingangsspannungen mit DGND2 als Masse
VPU2	Nicht unterstützt, bitte verbinden Sie kein Signal

Port	Parameter	Lesen	Schreib	Verlauf
I1	1,0	x		/sys/senst2_board/input/1
I2	1,0	x		/sys/senst2_board/input/2
I3	1,0	x		/sys/senst2_board/input/3
I4	1,0	x		/sys/senst2_board/input/4
I5	1,0	x		/sys/senst2_board/input/5
I6	1,0	x		/sys/senst2_board/input/6
I7	1,0	x		/sys/senst2_board/input/7
I8	1,0	x		/sys/senst2_board/input/8

Beispiel: Auslese-Eingabe I1

Befehl: cat /sys/senst2_board/input1/value

Antwort: z. B. 1# oder 0#

14.9.2 Digitale Ausgänge

Wie die grundlegenden digitalen Ausgänge sind die zusätzlichen digitalen Ausgänge des SensT2 galvanisch isolierte Festkörperrelais. OxA ist mit einem Pin des Relais verbunden, OxB mit dem anderen Pin. Der maximale Schaltstrom beträgt 300 mA (maximal 30 V Gleichstrom).

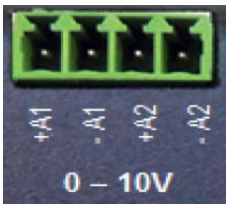
Port	Parameter	Lesen	Schreib	Verlauf
O1A,O1B	1,0		X	/sys/senst2_board/output/1
O2A, O2B	1,0		X	/sys/senst2_board/output/2

Beispiel: Schalten Sie den Ausgang O1A, O1B ein

Befehl: Echo 1 > /sys/senst2_board/output/1

Antwort: #

14.9.3 Spannungseingänge 0 – 10 V



Die angelegte Gleichspannung darf 10 V nicht überschreiten. Der Eingang zieht einen Strom von etwa 2 mA @ 10 V.

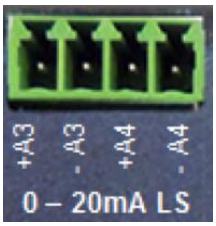
Port	Beschreibung
+A1	Positiver Verbindungseingang 1
-A1	Negativer Verbindungseingang 1
+A2	Positiver Verbindungseingang 2
-A2	Negativer Verbindungseingang 2

Port	Parameter	Lesen	Schreib	Verlauf
+A1,-A1	Wert	x		/sys/senst2_board/voltage_in/1
+A2,-A2	Wert	x		/sys/senst2_board/voltage_in/2

Beispiel: Lesespannung am ADC-Eingang +A1,-A1
Befehl: cat /sys/senst2_board/voltage_in1/value
Antwort: z. B. 6400

Hinweis: Umwandlung in Volt
Formel: Spannung in Volt = Wert / 1000
Beispiel: Wert = 6400 entspricht 6,4V

14.9.4 Stromeingänge 0 - 20 mA



Die analogen Stromeingänge des MC100 SensT2 haben zwei Betriebsmodi:

1. Stromversorgung – Strom vom Sensor – Sensor mit eigener Stromversorgung
2. Low Side Shunt – mit Stromversorgung für den Sensor

Beispiel: Stromversorgung – Strom vom Sensor

Der angeschlossene Sensor verfügt über eine eigene Stromversorgung und einen Stromausgang mit maximalem Strom von 20 mA. Der Sensor ist mit -A3 oder -A4 gegen Masse verbunden.

Port	Beschreibung
-A3	Positive Verbindungseingang 3, Stromausgang des Sensors
GND	Negative Verbindung Eingang 3, Sensormasse
-A4	Positive Verbindungseingang 4, Stromausgang des Sensors
GND	Negative Verbindung Eingang 4, Sensormasse

Beispiel: Low Side Shunt – Stromversorgung für den Sensor

Es ist möglich, den Sensor gleichzeitig mit Strom zu versorgen und gleichzeitig den Strom zu messen, den er über dieselben beiden Drähte zieht. In diesem Beispiel wird der Sensor vom MC100 SensT2 betrieben. An den Anschlüssen +A3 oder +A4 wird eine Spannung angelegt. Verbinden Sie den Sensor mit +A3 und A3 oder +A4 und -A4.

Port	Beschreibung

+A3	Positive Verbindung Ausgangs 3, Sensorversorgung ca. 12V bis 14V
-A3	Negative Verbindung Eingang 3
+A4	Positive Verbindung Ausgang 4, Sensorversorgung ca. 12V bis 14V
-A4	Negative Verbindung Eingang 4

Port	Parameter	Lesen	Schreib	Verlauf
+A3,-A3	Wert	x		/sys/senst2_board/current_in/3
+A4,-A4	Wert	x		/sys/senst2_board/current_in/4

Beispiel: Lesestrom am ADC-Eingang +A3,-A3

Befehl: cat /sys/senst2_board/current_in1/value

Antwort: z. B. 1500

Hinweis: Umstellung auf mA

Formel: Strom in mA = Wert * 20 / 3000

Beispiel: Wert = 1500 entspricht 10mA

14.9.5 Stromausgänge 0 - 20 mA

Port	Parameter	Lesen	Schreib	Verlauf
OI1	Wert		x	/sys/senst2_board/current_out/1
OI2	Wert		x	/sys/senst2_board/current_out/2

Hinweis: Umwandlung von mA in zu liefernden Wert

Formel: Wert = Strom in mA * 1000

Beispiel: Strom = 6mA entspricht Wert = 6000

14.9.6 PT100 / PT1000 Eingänge

Port	Parameter	Lesen	Schreib	Verlauf
RTD1	Wert	x		/sys/senst2_board/rtd/1
RTD2	Wert	x		/sys/senst2_board/rtd/2
RTD3	Wert	x		/sys/senst2_board/rtd/3
RTD4	Wert	x		/sys/senst2_board/rtd/4

Beispiel: Lesen Sie den Wert bei RTD1

Befehl: cat /sys/senst2_board/rtd/1

Antwort: z.B. 100.000

Umwandlung am Port eines Widerstands in Ohm

Formel: Widerstand in Ohm = Wert / 100

Beispiel: Wert = 100000 entspricht 1000Ohm

Umwandlung am Anschluss eines PT1000-Temperatursensors auf °Celsius

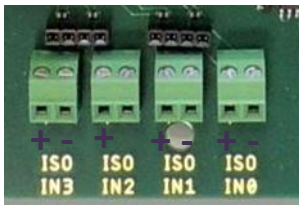
Formel: Temperatur in Grad Celsius = (Wert / 100 -1000) / 3.891

Beispiel: Wert = 112000 entspricht +30,84° Celsius

Wert = 100000 entspricht 0° Celsius
Wert = 90.000 entspricht -25,5° Celsius

14.10 MC100 SensorBox Schnittstellenbelegung

14.10.1 Digitale Eingänge



Die galvanisch isolierten digitalen Eingänge können ein DC-Spannungssignal > 6V (aktiv-hoch, maximal 30 V DC) mittels Optokopplern detektieren.

Port	Parameter	Lesen	Schreib	Verlauf
IN0	1,0	x		/sys/sensor_carrier_board/inputs/isoInput0/value
IN1	1,0	x		/sys/sensor_carrier_board/inputs/isoInput1/value
IN2	1,0	x		/sys/sensor_carrier_board/inputs/isoInput2/value
IN3	1,0	x		/sys/sensor_carrier_board/inputs/isoInput3/value

Beispiel: Lesestatus der Eingabe IN0
Befehl: cat /sys/sensor_carrier_board/inputs/isoInput0/value
Antwort: z. B. 1# oder 0#

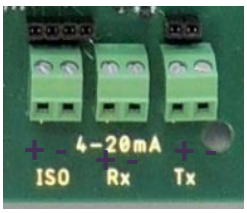
14.10.2 Digitale Ausgänge

Wie die grundlegenden digitalen Ausgänge sind die zusätzlichen digitalen Ausgänge des MC100 GPIO galvanisch isolierte Festkörperrelais. Der maximale Schaltstrom beträgt 300 mA (maximal 30 V Gleichstrom).

Port	Parameter	Lesen	Schreib	Verlauf
ISO OUT1	1,0		X	/sys/sensor_carrier_board/outputs/output1/value
ISO OUT2	1,0		X	/sys/sensor_carrier_board/outputs/output2/value

Beispiel: Schalten Sie den Ausgang ISO OUT1 ein
Befehl: Echo 1 > /sys/sensor_carrier_board/outputs/output1/value
Antwort: #
Beispiel: Wert = 6400 entspricht 6,4V

14.10.3 Stromeingänge 4 - 20 mA RX / ISO



Die analogen Stromeingänge der MC100 SensorBox verfügen über zwei Betriebsmodi.

1. Stromversorgung – Strom vom Sensor – Sensor mit eigener Stromversorgung

2. Low Side Shunt – mit Stromversorgung für den Sensor

Beispiel: Stromversorgung – Strom vom Sensor

Der angeschlossene Sensor verfügt über eine eigene Stromversorgung und einen Stromausgang mit einem Strom von 20 mA.

Der Sensor ist mit + und – von Rx verbunden.

Port	Beschreibung
+	Positiver Verbindungseingang, Stromausgang des Sensors
-	Negative Verbindung Eingang, Sensormasse

Beispiel: Low Side Shunt – Stromversorgung für den Sensor

Es ist möglich, den Sensor sowohl mit Strom zu versorgen als auch den Strom zu messen, den er über die beide Drähten zieht. Der Sensor wird vom MC100 SensorBox mit Strom versorgt. Für diesen Zweck wird an die Anschlüsse + und – eine ISO von 4–20 mA angelegt. Schließen Sie den Sensor an + und – mit ISO 4–20 mA an.

Port	Parameter	Lesen	Schreib	Verlauf
+,- Rx	Wert	x		/sys/sensor_carrier_board/adcinputs/adcinput1/value
+,- ISO	Wert	x		/sys/sensor_carrier_board/adcinputs/adcinput0/value

Beispiel: Lesestrom am ADC-Eingang +,- Rx
Befehl: cat /sys/sensor_carrier_board/adcinputs/adcinput1/value
Antwort: z. B. 1500

Hinweis: Umstellung auf mA
Formel: Strom in mA = Wert * 20 / 3000
Beispiel: Wert = 1500 entspricht 10mA

14.10.4 Stromausgänge 0 - 20 mA Tx

Port	Parameter	Lesen	Schreib	Verlauf
+,- Tx	Wert		x	/sys/sensor_carrier_board/adcoutputs/adcoutput/value

Beispiel: Ausgangsleistung von 6 mA bei OI1

Befehl: Echo 6000 > /sys/sensor_carrier_board/adcoutputs/adcoutput/value
Antwort: Keine

14.10.5 RTD-Eingänge

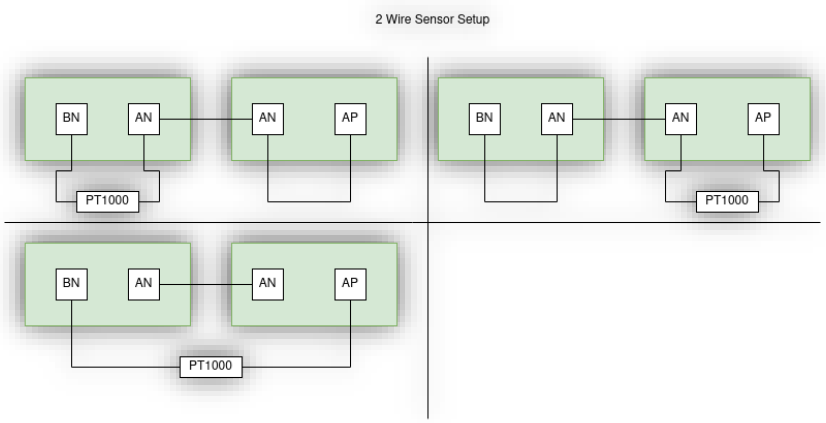
Die RTD-Eingänge können Widerstände messen, z. B. zur Bestimmung der Temperaturen mit PT100- oder PT1000-Sensoren. Es gibt verschiedene Arten von RTDs, darunter 2-adrige, 3-adrige und 4-adrige RTDs.

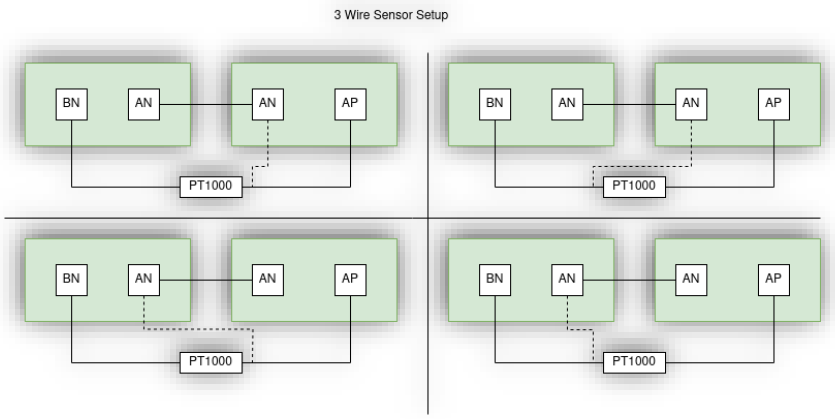
Die Wahl des verwendeten Typs hängt vom spezifischen Temperaturbereich und den Präzisionsanforderungen ab. Bei einem zweiadrigen RTD summieren sich der Widerstand des Sensors und der Leitungsleitungen. Gerade bei einem langen Kabel und hohen Temperaturschwankungen kann der Fehler kritisch sein. Daher sind 3-Draht-RTDs zum Industriestandard geworden, wenn größere Genauigkeit erforderlich ist. Vorausgesetzt, alle Leitungen haben die gleiche Länge, das gleiche Material und den gleichen Durchmesser, ermöglicht ein drittes Kabel, den Drahtwiderstand arithmetisch aufzuheben.

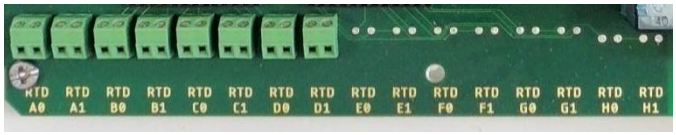
Bitte beachten Sie: Die SensorBox kann zum Messen von 2- und 3-Adrig-RTDs verwendet werden, aber nicht zu 4-adrigen RTDs.

Auf der folgenden Seite sind alle möglichen Kombinationen zur Verbindung von 2- und 3-Adrig mit der SensorBox dargestellt.

Wie aus der untenstehenden Abbildung zu sehen ist, funktionieren die RTD-Eingänge nur paarweise (A0A1, B0B1, ...). Wenn z. B. A0 verwendet werden soll und A1 nicht, muss A1 mit einem kurzen Drahtstück überbrückt werden.







Port	Parameter	Lesen	Schreib	Verlauf
RTD A0	Wert	x		/sys/sensor_carrier_board/rtd/rtd0/value
RTD A1	Wert	x		/sys/sensor_carrier_board/rtd/rtd1/value
RTD B0	Wert	x		/sys/sensor_carrier_board/rtd/rtd2/value
RTD B1	Wert	x		/sys/sensor_carrier_board/rtd/rtd3/value
RTD C0	Wert	x		/sys/sensor_carrier_board/rtd/rtd4/value
RTD C1	Wert	x		/sys/sensor_carrier_board/rtd/rtd5/value
RTD D0	Wert	x		/sys/sensor_carrier_board/rtd/rtd6/value
RTD D1	Wert	x		/sys/sensor_carrier_board/rtd/rtd7/value
RTD E0	Wert	x		/sys/sensor_carrier_board/rtd/rtd8/value
RTD E1	Wert	x		/sys/sensor_carrier_board/rtd/rtd9/value
RTD F0	Wert	x		/sys/sensor_carrier_board/rtd/rtd10/value
RTD F1	Wert	x		/sys/sensor_carrier_board/rtd/rtd11/value
RTD G0	Wert	x		/sys/sensor_carrier_board/rtd/rtd12/value
RTD G1	Wert	x		/sys/sensor_carrier_board/rtd/rtd13/value
RTD H0	Wert	x		/sys/sensor_carrier_board/rtd/rtd14/value

RTD H1	Wert	x		/sys/sensor_carrier_board/rtd/rtd15/value

Beispiel: Lesen Sie den Wert bei RTD A0

Befehl: cat /sys/sensor_carrier_board/rtd/rtd0/value

Umwandlung am Port eines Widerstands in Ohm

Formel: Widerstand in Ohm = Wert / 100

Beispiel: Wert = 100000 entspricht 1000Ohm

Umwandlung am Anschluss eines PT1000-Temperatursensors auf °Celsius

Formel: Temperatur in Grad Celsius = (Wert / 100 -1000) / 3.891

Beispiel: Wert = 112000 entspricht +30,84° Celsius
Wert = 100000 entspricht 0° Celsius
Wert = 90.000 entspricht -25,5° Celsius

14.10.6 AC-OUT-Relais

Port	Beschreibung
NC	Normalerweise geschlossen zu COM
COM	Schalter
NO	Normalerweise geöffnet zu COM

Port	Parameter	Lesen	Schreib	Verlauf
COM, NO	1,0		x	/sys/sensor_carrier_board/ac/acout/value

Beispiel: Relais einschalten

Befehl: echo 1 > /sys/sensor_carrier_board/ac/acout/value

Antwort: #

14.10.7 AC IN-Relais

Dieses Relais kann geschaltet werden, indem 230 V Wechselstrom an die Klemmenblöcke angeschlossen wird. Der Zustand des Relais kann wie ein digitaler Eingang erkannt werden.

Port	Parameter	Lesen	Schreib	Verlauf
AC IN	1,0		X	/sys/sensor_carrier_board/ac/acin/value

Beispiel: Lesen Sie den AC-Eingangsstatus aus

Befehl: cat /sys/sensor_carrier_board/ac/acin/value

Antwort: 1,0

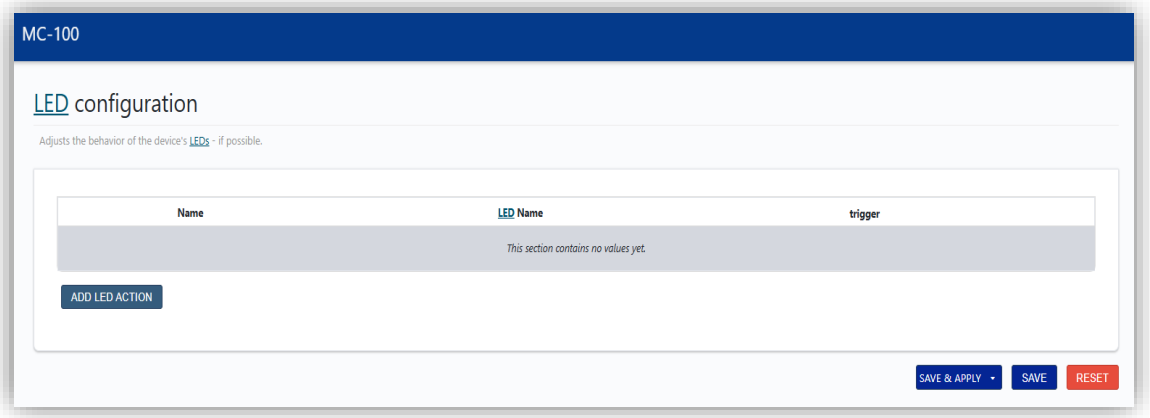
14.11 LEDs

MC100 verfügt über drei LEDs, deren Funktionalität geändert werden kann: Info, Status und Warnung.

Die Signalauslöser und Blinkmuster der LEDs können in der Weboberfläche angepasst werden.

Die Einstellungen sind in *System->LED-Konfiguration zu finden*.

Klicken Sie auf LED-AKTION HINZUFÜGEN, um eine neue, individuell angepasste LED-Definition zu erstellen.



Optionen:

Name: Name der LED-Konfiguration.

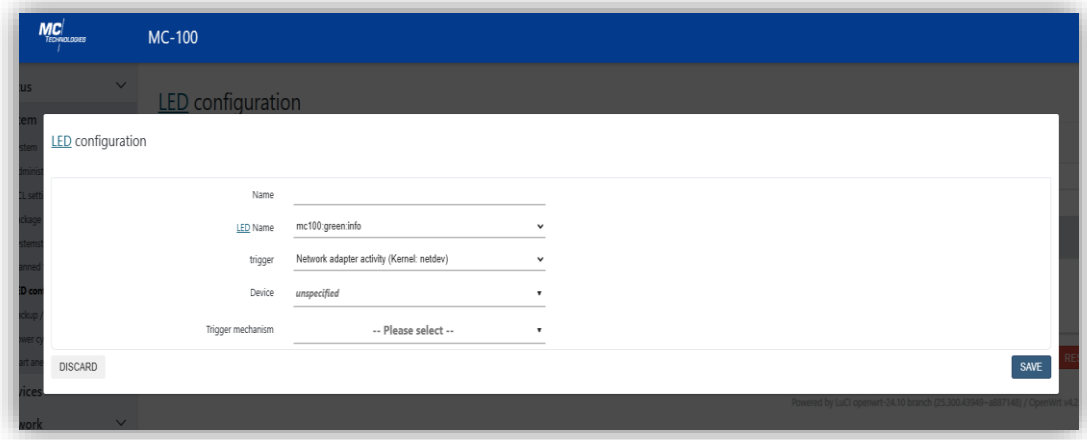
LED-Name: Farbe und Name der LED.

Standardzustand der LED: Ein/Aus.

Trigger: Einer der verschiedenen Trigger kann einer LED zugewiesen werden, um ihre Zustände zu ändern.

Mögliche Werte:

Abzugstyp	Beschreibung
Herzschlag	Simulation tatsächlicher Herzschläge
Immer an	LED bleibt immer an.
Immer falsch	LED bleibt immer aus
Benutzerdefiniertes Blitzintervall	Blinken gemäß vordefiniertem Timer-Muster
netdev	Blinkt entsprechend Linkstatus und Send/Empfangsaktivität



Der Name der LED-Definition kann willkürlich gewählt werden, aber die Angabe des LED-Namens im Dropdown-Menü ist Pflicht. Der Standardzustand definiert, ob die LED zunächst ein- oder ausgeschaltet sein soll, bevor ein Triggersignal ihren Zustand ändert.
Welche Signalquelle das Blinkmuster der LED steuert, kann über das *Trigger-Dropdown-Feld* ausgewählt werden.

LED	LED-Name
INFO	mclx:orange:info
STATUS	mclx:orange:status
WARN	mclx:red:warn
1	mclx-cb:grün:led1
2	mclx-cb:red:led2

Klicken Sie auf SPEICHERN, dann auf SPEICHERN und ANWENDEN, damit die LED-Konfiguration in Kraft tritt.

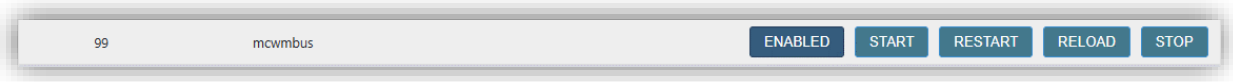
15 Drahtlose Schnittstellen

15.1 wM-Bus

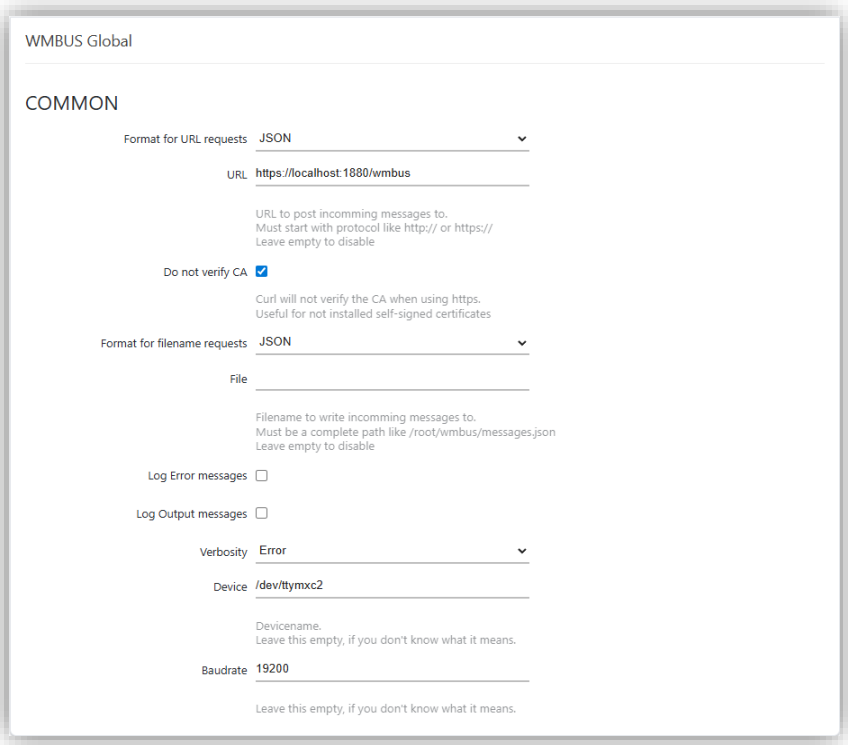
Das MC100 Terminal/Gateway kann mit einer Erweiterungsplatine für Wireless M-Bus geliefert werden.

15.1.1 Ermöglichung von mcwmbus

Vor der Nutzung von wM-Bus ist erforderlich, den mcwmbus-Dienst zu aktivieren. Suchen Sie den entsprechenden Eintrag in *System->Startup* und klicken Sie auf den *DEAKTIVIEREN-Button*, um den automatischen Start beim Start zu aktivieren, falls der Dienst noch nicht aktiviert wurde. Dann klicken Sie auf die START-Taste, um den Service manuell zu starten oder das Gerät neu zu starten.



Im Reiter Dienste klicken Sie auf wM-Bus.



1. Klicken Sie auf Aktivieren
2. Wählen Sie das Ausgabeformat, das die POST-Anfrage anfordert, unter Format für URL-Anfragen
3. Geben Sie die gewünschte URL ein. (Falls nicht nötig, lassen Sie es leer).

4. Wählen Sie das Ausgabeformat, das verwendet wird, um Ausgabedaten als Datei unter Format für Dateinamensanfragen zu speichern
5. Geben Sie den gewünschten Pfad und Dateinamen ein (optional)
6. Klicken Sie auf SPEICHERN&ANWENDEN

15.1.2 Installation von mcwmbus

Um mit der wM-Bus-Erweiterung zu interagieren, wird das Kommandozeilen-Tool mcwmbus benötigt.

15.1.3 Grundlegende Funktionalität

Das Tool unterstützt den Parameter -h, um Informationen über seine Verwendung auszugeben.

```
Einsatz: mcwmbus [Optionen]

Copyright (C) 2020 MC-Technologies GmbH

Optionen:

-h    Zeig diese Hilfe-Nachricht und verlass es.

-V    Versionsinformationen anzeigen und verlassen.

-v    Ausdrucke ausführliche Debug-Informationen

-d    GERÄT tty Gerät (Standard: /dev/ttymxc2)

-b    BAUD Baud-Rate für Kommunikation (Standard: 19200)

-f    DATEINAME Schreibe Daten in Datei.

-    u URL Daten über POST senden Anfrage an URL

-c    Daten auf der Kommandozeile drucken

-F FORMAT    Datenformat für Dateien (Standard: hex)
```

Die Ausgabe könnte so aussehen:

15.1.4 Ausgabeformate

Das Tool unterstützt verschiedene Ausgabeformate, die für jeden Ausgabekanal einzeln eingestellt werden können (URL, FILE, Kommandozeile).

Hexadezimal:

HEX erzeugt die Nachricht hexadezimal. Eine Nachricht pro Leitung.

Beispiel für hexadezimale Ausgabe:

```
1644AF4C02000041011B7A980000000266E8000266E900
```

JSON

JSON interpretiert die Nachricht und liefert so viele Informationen wie möglich. Sie enthält außerdem die rohe Nachricht als hexadezimale Zeichenkette.

Beispiel für JSON-Ausgabe:


```
{
 "SlaveInformation": {
 "Id": 41000002,
 "Hersteller": "SEO",
 "Version": 1,
 "Produktname": "Senseco Wireless M¬Bus 2 NTC Temperatur
 Sensor",
 "Medium": "Ambient Sensor",
 "AccessNumber": 152,
 "Status": "00",
 "Unterschrift": "0000"
 },
 "DataRecords": [
 {
  "id": 0,
  "Funktion": "Momentaner Wert",
  "StorageNumber": 0,
  "VIF": 102,
  "VIFE": 0,
  "Einheit": "Außentemperatur (1e-1 °C)",
  "Wert": "232",
  "Zeitstempel": "2020-06-09T07:51:08Z"
 },
 {
 "id": 1,
  "Funktion": "Momentaner Wert",
  "StorageNumber": 0,
  "VIF": 102,
  "VIFE": 0,
  "Einheit": "Außentemperatur (1e-1 °C)",
  "Wert": "233",
  "Zeitstempel": "2020-06-09T07:51:08Z"
  }
 ],
 "RawMessage": "1644AF4C02000041011B7A980000000266E8000266E900"
}
```


XML

XML-Ausgabe interpretiert die Nachricht und erzeugt eine XML-Ausgabe.

Beispiel zur XML-Ausgabe:

```
<?xml version="1.0" Codierung="ISO-8859-1"?>
<MBusData>
  <Sklaveninformation>
        <Id>41000002</Id>
        <Hersteller>SEO</Hersteller>
        <Version>1</Version>
        <ProductName>Sensoco Wireless M¬Bus 2 NTC Temperatur
Sensor</ProduktName>
        <Medium>Umgebungssensor</Medium>
        <AccessNumber>157</AccessNumber>
        <Status>00</Status>
        <Unterschrift>0000</Unterschrift>
 </SlaveInformation>

 <DataRecord id="0">
        <Funktion>Momentaner Wert</Funktion>
        <StorageNumber>0</StorageNumber>
        <Einheit>Außentemperatur (1e-1 Grad C)</Einheit>
        <Wert>232</Wert>
        <Zeitstempel>2020-06-09T07:52:03Z</Zeitstempel>
 </DataRecord>

 <DataRecord id="1">
        <Funktion>Momentaner Wert</Funktion>
        <StorageNumber>0</StorageNumber>
        <Einheit>Außentemperatur (1e-1 Grad C)</Einheit>
        <Wert>233</Wert>
        <Zeitstempel>2020-06-09T07:52:03Z</Zeitstempel>
 </DataRecord>
</MBusData>
```

json_hex

Es ist auch möglich, die Daten im JSON-Format zu erhalten , das leichter lesbar ist als reines HEX:


```
{"timestamp":"2020-06-09T09:53:47.295+0200","LEN": "22","C":
"44","MAN": "4caf","UID": "41000002","VER": "01","DEV": "1b","CI":
"7a","COUNTER": "a7","STATUS": "00","ENCRYPTION": "0000","DATA":
"0266e8000266e800"}
```


15.1.5 Posten in einer REST-API

Es ist möglich, die Nachrichten an eine REST-API zu senden, indem man die Befehlszeile "parameter –u" übergibt. Zum Beispiel kann dies verwendet werden, um Nachrichten an den internen Node-RED-Server auf dem mc100 zu senden:

```
root@ mcwmbus -u http://localhost:1880/wmbus
```

Oder es kann in Kombination mit dem integrierten Modem verwendet werden, um Nachrichten an einen in der Cloud laufenden Server zu senden, damit Echtzeitdaten auf Ihrem Arbeitsplatz verfügbar sind.

15.1.6 Schreiben in das Dateisystem

Beim Schreiben von Daten auf Festplatte ist es möglich, Teile des Pfades dynamisch mithilfe von magischen Strings zu spezifizieren:

```
%M - Hersteller-ID
%D - Gerätetyp / Medium
%U - Ident Nr.
%V – Version
```

Beispiel:

Der folgende Dateibaum wurde erstellt von:

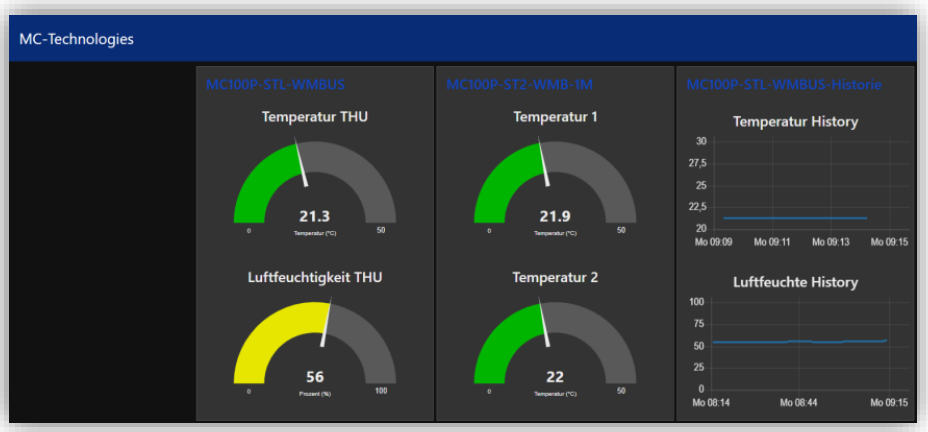
```
root@MC100:~# mcwmbus –F wmbus_messages/%M/%U.json
```

Es erlaubt tp, Hersteller und Geräte-ID über den Dateipfad vorzuwählen, was zu folgender Dateisystemstruktur führt:

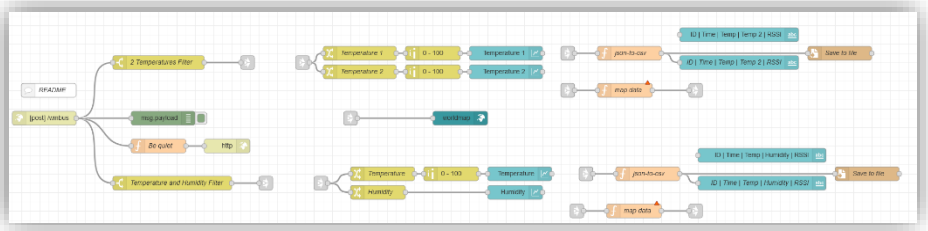
```
wmbus_messages
+-- 18c4
|   +-- 17949.json
+-- 25c5
|   +-- 33100007.json
+-- 4caf
|   +-- 30000007.json
|   +-- 41000002.json
```

15.1.7 Live-Informationen in Node-RED anzeigen

Der in diesem Kapitel beschriebene Beispielfluss verwendet einen REST-Server und zeigt die Informationen mit dem Dashboard-Plugin an. Das Ergebnis sieht so aus:



Beispiel für den roten Knotenfluss:



Befehl:

```
root@MC100:~# mcwmbus -u http://localhost:1880/wmbus -c -C json
```

15.1.8 Aggregiere Daten für 1 Stunden, 6 Stunden, 1 Tag und sende sie über FTP/SCP

Sammle Nachrichten für den ganzen Tag als interpretiertes JSON, aber sende am Ende des Tages nur Nachrichten vom Hersteller SEO in einer Zip-Datei an einen Server.

```
Obwohl zutreffend;
Tun
mcwmbus -F json -f "wmbus_messages/%M.json" &
sleep 86400 # = 60*60*24 = 24 Stunden
Killall McWmbus
Zip SEO.zip wmbus_messages/4caf.json
scp SEO.zip 192.168.1.1:/data/SEO-'date "+%Y-%m-%d"'.zip
RM SEO.zip
fertig
```

15.1.9 Fehlerbehebung

Bitte führen Sie "mcwmbus –vV" aus und senden Sie die Ausgabe zusammen mit Ihrer Fehlerbeschreibung und etwaigen Fehlermeldungen an support@mc-technologies.net

Es ist hilfreich, wenn Sie den Befehl, der den Fehler erzeugt hat, mit "-vvvvvv" ausführst, um die Debug-Länge zu maximieren.

16 GNSS-Satellitennavigation (GPS)

16.1 GNSS beim Start aktivieren

Um die GNSS- und NMEA-Schnittstelle des Modes beim Start zu aktivieren, führen Sie den Befehl aus:

```
mcinfo -c "AT+QGPSCFG=\"autogps\",1"
```

Um das weit verbreitete Location-Daemon *GPSD* beim Start zu aktivieren, führen Sie aus:

```
/etc/init.d/gpsd enable
```

Hinweis: Ein Neustart und schließlich ein Neustart sind erforderlich, damit die Änderungen wirksam werden.

17 Kommunikationsprotokolle

Das Modbus-Messaging-Protokoll wird verwendet, um Client-Server-(Master-Slave-)Kommunikation zwischen Geräten herzustellen. MC100 kann entweder als Master (Server) oder als Slave-Geräte (Client) verwendet werden. Als Master kann der MC100 bis zu 247 Slave-Geräte bedienen. Der MC100 wurde getestet, um Daten mit Modbus RTU problemlos in Frequenzen zwischen 20 und 40 Hz abzufragen.

17.1 Modbus Master-Kommandozeilen-Tool

17.1.1 Verwendung der Kommandozeile

- Register 0 auf Sklave 1 lesen:

```
root@MC100:~# mcmodbus -a 0
```

- Debug-Informationen während der Ausführung drucken:

```
root@MC100:~# mcmodbus -v -a 0
```

```
root@MC100:~# mcmodbus -vv -a 0
```

- Hilfenachricht anzeigen:

```
root@MC100:~# mcmodbus –h
```

- Register 0 auf Sklave 17 lesen:

```
root@MC100:~# mcmodbus -s 17
```

- Stellen Sie den Ausgang von Slave 17 für die I/O-Pins 4, 5, 6 auf 1 0 1 ein:

```
root@MC100:~# mcmodbus -o wb - a 4 -s 17 1 0 1 1
```

- Verwenden Sie ein spezielles serielles Gerät mit einer Baudrate von 115200:

```
root@MC100:~#mcmodbus -d /dev/ttyUSB10 -b 115200
```

- Setze den digitalen Ausgang bei Adresse 0x34 auf ON:

```
root@MC100:~# mcmodbus -o wib -a 0x34 1

root@MC100:~# mcmodbus -o wib -a 064 1

root@MC100:~# mcmodbus -o wib -a 52 1
```

- Analoge Eingänge an Adresse 0x20 und 0x21 lesen:

```
root@MC100:~# mcmodbus -o rir -a 0x20 -n 2
```

- Register 8 auf 0x4563 setzen:

```
root@MC100:~# mcmodbus -o wr -a 0x08 0x4563

root@MC100:~# mcmodbus -a 8 -o wr 17763
```

17.2 Modbus-Slave-Befehlszeilen-Tool

```
 Einsatz: mcmodbus-slave [OPTIONEN]
 Optionen:
  -H,--Hilfe              Drucken Sie diese Hilfenachricht aus und verlassen Sie
  -c,--config-file TEXT   Json-Konfiguration für die Adresszuordnungen. Standard:
./mappings.json
  -d,--device-file TEXT   Serielles Gerät für Modbus RTU
  -p,--Port UINT          Port für Modbus TCP.
  -b,--baud-rate UINT     Baudrate für das serielle Gerät. Standard: 115200
  -v,--verbose            Debug-Eingabe aktivieren
```

17.2.1 Verwendung von Modbus RTU

Befehl: mcmodbus-slave -d <Serial-port-Device-file> -b <baud-rate> -c <JSON-config>
Beispiel (RS-485):

```
root@MC100:~# mcmodbus-slave -d /dev/ttymxc4 -b 115200
```

17.2.2 Verwendung von Modbus TCP

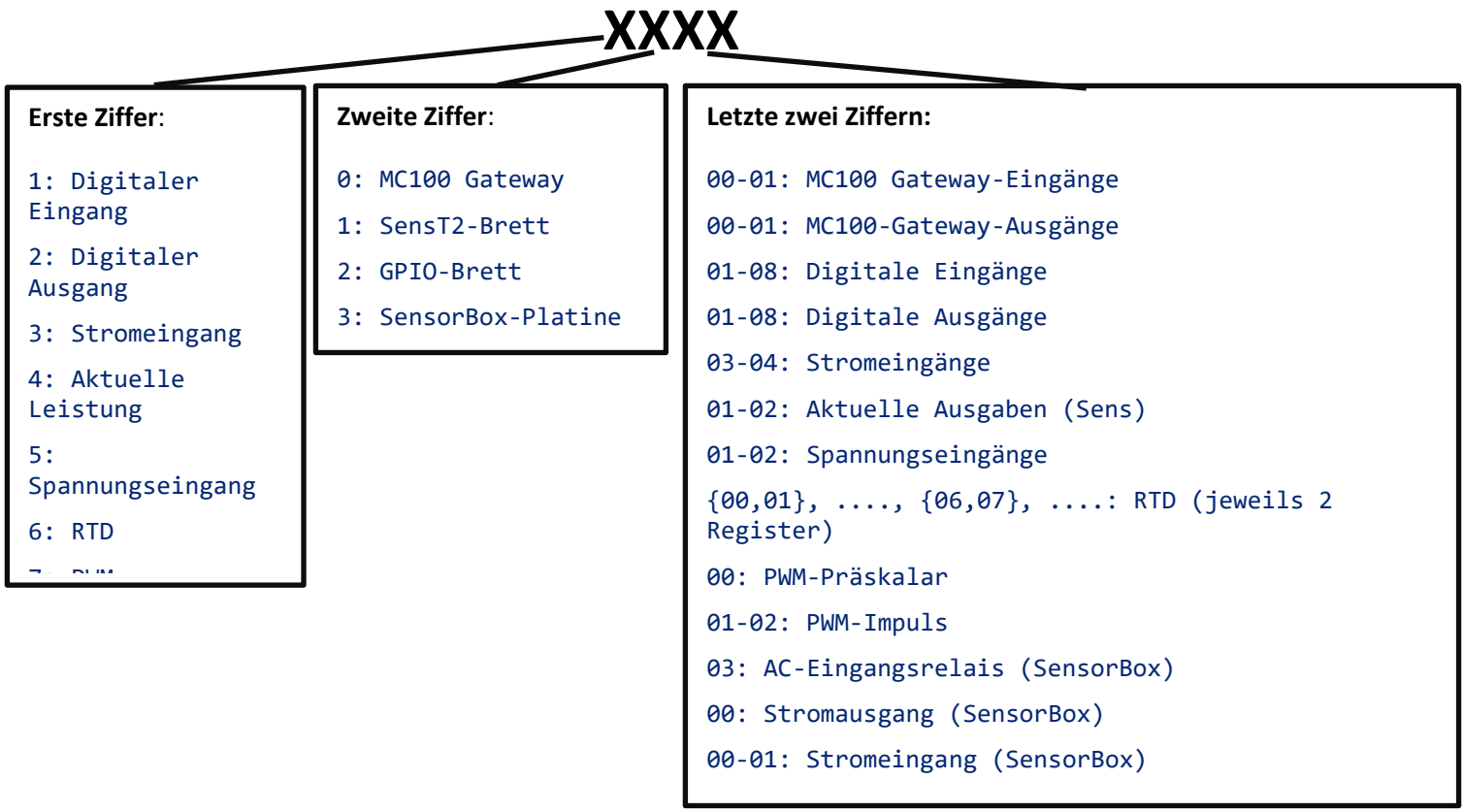
Befehl: mcmodbus-slave -p <port> -b <baud-rate> -c <Json Config>

Zum Beispiel:

```
root@MC100:~# mcmodbus-slave -p 502
```

17.2.3 MC100 Standard-JSON-Mapping.

MC100 Modbus-Adressierungsabbildung:



Beispiel: Die Adresse des digitalen Eingangs 4 auf MC100 GPIO lautet: 1204
Die Adresse von RTD 2 auf MC100 SensT2 lautet: {6104,6105}

17.2.4 JSON-Konfigurationsdatei

Beispiel:

```
{
 "typ": "file",
 "Adresse": 4000,
 "num_addresses": 1,
 "Register": wahr,
 "Output": wahr,
 "Dateiname": " /sys/sensor_carrier_board/adcoutputs/adcoutput/value",
 "Faktor": 1000,
 "isfloat": wahr,
 "MinValue": 4000,
 "MaxValue": 20000
},
```

Modbus-Daten werden meist als "Register" gelesen und geschrieben, also 16-Bit-Datenstücke. Folglich wird eine 32-Bit-Ganzzahl üblicherweise mit zwei und einer 64-Bit-Ganzzahl als vier aufeinanderfolgende Register dargestellt.

Typ	Art der verwendeten Kartierung. Datei: Der Inhalt einer Datei wird zugeordnet. exe: Führe einen Befehl aus
Adresse	Früher wurde die Modbus-Adresse vom Master-Gerät aufgerufen.
num_addresses	Anzahl der Register, die zur Abbildung der Datei verwendet werden. [Standard 1] 1 : 16-Bit-Ganzzahl 2 : 32-Bit-Ganzzahl
Register	True: eine 16-Bit-Ganzzahl lesen/schreiben Falsch: lesen / schreiben 1 oder 0 [Standard]
Ausgabe	Wahr: schreiben Sie Falsch: Lesen [Standard]
Dateiname	Pfad zur Eingabe-/Ausgabedatei.
isfloat	Stimmt, wenn Ein-/Ausgabe Float ist. [Standardfalsch]
Faktor	Faktor, der verwendet wird, um Float in eine ganze Zahl zu transformieren. [Standard 1]
MinValue	Minimaler Eingangswert
MaxValue	Maximaler Eingangswert
Kommando	Befehl auszuführen. (Nur wenn **Der Typ** ist "exe")

18 Netzwerkschnittstellenkonfiguration

Eine Auflistung der Netzwerkschnittstellen findet sich unter *Network->Interfaces*.

Netzwerkschnittstellen in der OpenWrt-Terminologie sind virtuell im Sinne davon, dass sie eine Reihe von Konfigurationsoptionen wie das Schnittstellen-Protokoll, IP-Adresse, Firewall-Zone usw. darstellen, die mit einem Netzwerkgerät verknüpft sind.

Netzwerkgeräte sind in der OpenWrt-Terminologie das, was traditionell als Netzwerkschnittstellen in UNIX-Begriffen verstanden wird, wie Hardware-Ethernet-Schnittstellen, virtuelle Brücken usw.

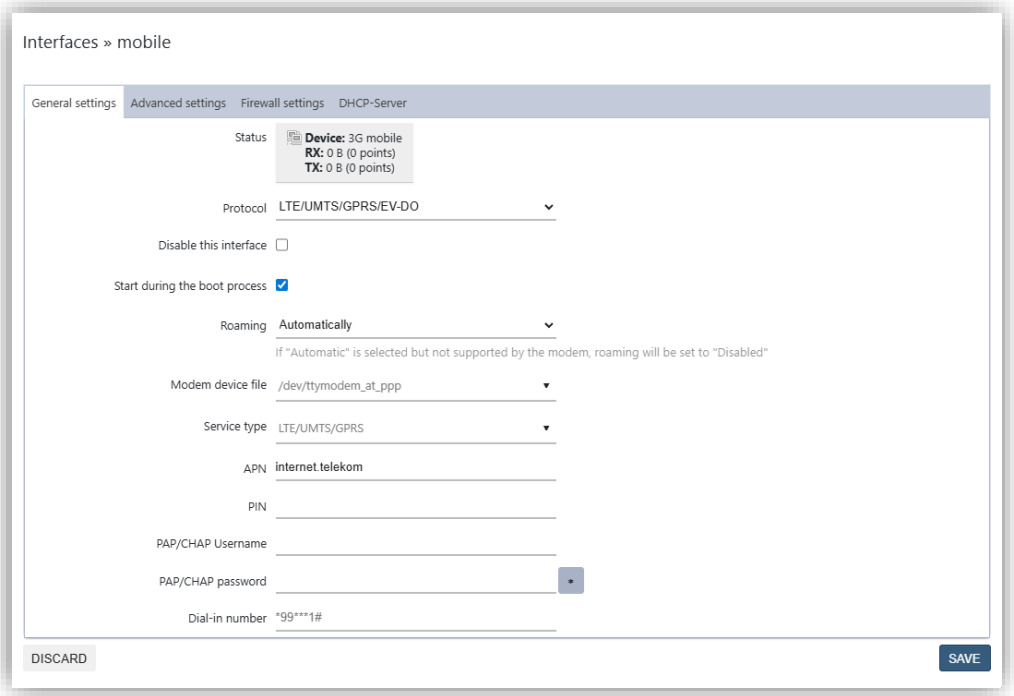
Beispiel: Im Werksstandardzustand *ist die LAN-Schnittstelle als Schnittstelle konfiguriert, die einen DHCP-Server auf dem* br-lan-Netzwerkgerät anbietet . *br-lan* ist tatsächlich eine virtuelle Bridge, die nur die Hardware-Schnittstelle **eth0** des MC100 enthält.

18.1 Mobilfunkverbindung eingerichtet

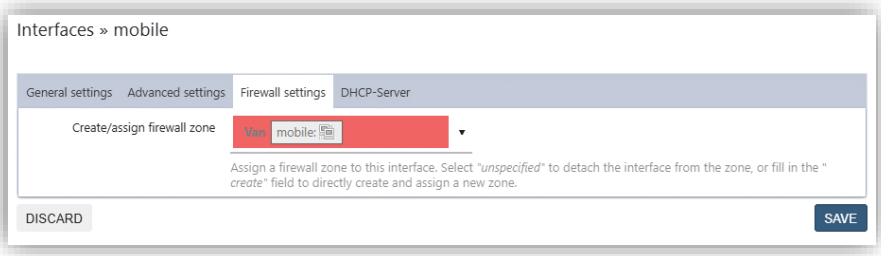
Eine mobile WAN-Schnittstellenkonfiguration ist im Werksstandard vorhanden, was nur geringe, anbieterabhängige Anpassungen erfordern sollte, um eine mobile Breitbandverbindung herzustellen.

Klicken Sie neben der mobilen Oberfläche auf BEARBEITEN.

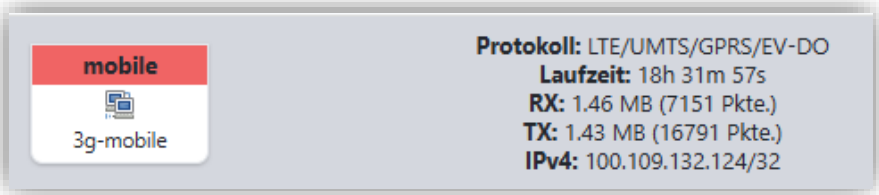
Zugriffskonfigurationsdetails wie Wählnummer, APN, Benutzername und Passwort müssen vom Mobilfunkanbieter abgeholt werden. Viele Anbieter verlangen keine Authentifizierungsdaten, in diesem Fall können Benutzername und Passwortfelder leer bleiben. Geben sie die PIN-Nummer ihrer SIM-Karte ein. Lassen Sie das Feld leer, falls kein PIN gesetzt ist.



Wechsle zum *Reiter Firewall-Einstellungen*, um sicherzustellen, dass die mobile Schnittstelle zur WAN-Firewall-Zone hinzugefügt wird.



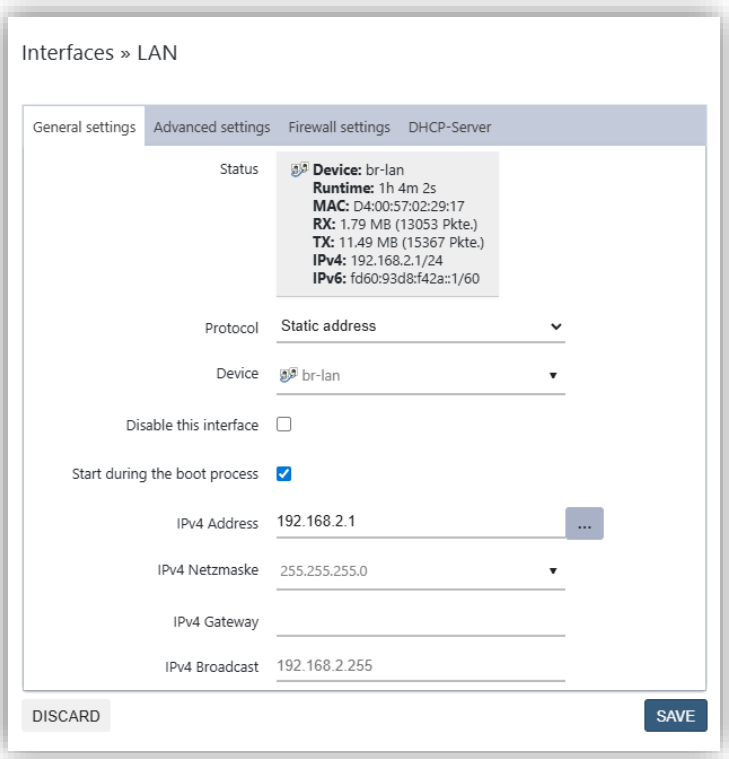
Nach dem Klicken auf SPEICHERN & ANWENDEN wird empfohlen, das Gateway neu zu starten oder kurzzeitig zu trennen, um sicherzustellen, dass das Modem ordnungsgemäß neu initialisiert wird.



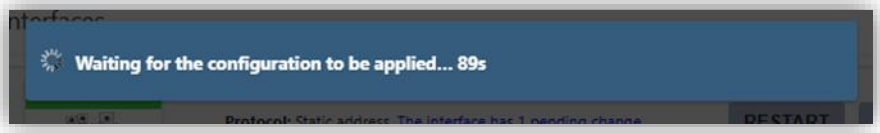
Nach dem Start loggen Sie sich erneut in die Weboberfläche ein. Wenn die Verbindung hergestellt wurde, sollten die Uptime-, übertragenen und empfangenen Datenstatistiken in Netzwerk->Schnittstellen im Feld der mobilen Schnittstellen-Eingabe angezeigt werden.

18.2 Änderung der LAN-IP-Adresse

Navigieren Sie zu Netzwerk->Schnittstellen und klicken Sie neben der LAN-Schnittstelle auf BEARBEITEN. Ändern Sie die IPv4-Adresse und Netzmaske bei Bedarf. Falls ein DHCP-Server von einem anderen Gerät im LAN-Netzwerk bereitgestellt wird, muss der DHCP-Server im DHCP-Server-Tab deaktiviert werden, um Konflikte zu vermeiden.
Klicken Sie auf SPEICHERN, aber wende die Änderungen noch nicht an.



Nachdem die Änderungen angewendet wurden, beginnt ein Countdown. Wenn dieser Countdown abläuft, bevor Sie mit der neuen IP-Adresse auf die Weboberfläche zugreifen konnten, wird das Gateway die Änderungen rückgängig machen. Das ist eine Gegenmaßnahme dagegen, sich versehentlich aus dem System auszuschließen. Sobald Sie bereit sind, mit der neuen IP-Adresse auf die Weboberfläche zuzugreifen, klicken Sie auf SPEICHERN & ANWENDEN.



18.3 WLAN-Aufbau

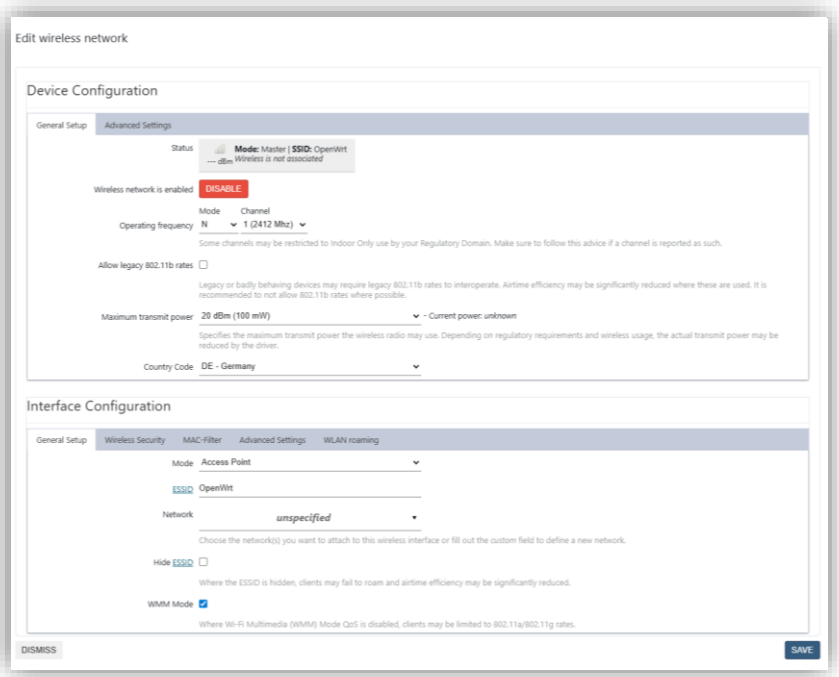
WLAN ist eine optionale Funktion, die nur in einigen Modellen der MC100-Familie integriert ist. Bitte stellen Sie sicher, dass das betreffende Gateway einen entsprechenden SMA-Anschluss hat.

18.3.1 Zugangspunkt-Modus (AP)

Das Gateway kann als Zugangspunkt für andere Geräte genutzt werden, um sich kabellos mit ihm zu verbinden.

Navigieren Sie zu Network->Wireless und klicken Sie auf HINZUFÜGEN, um ein virtuelles WLAN-Gerät zu radio0 hinzuzufügen.

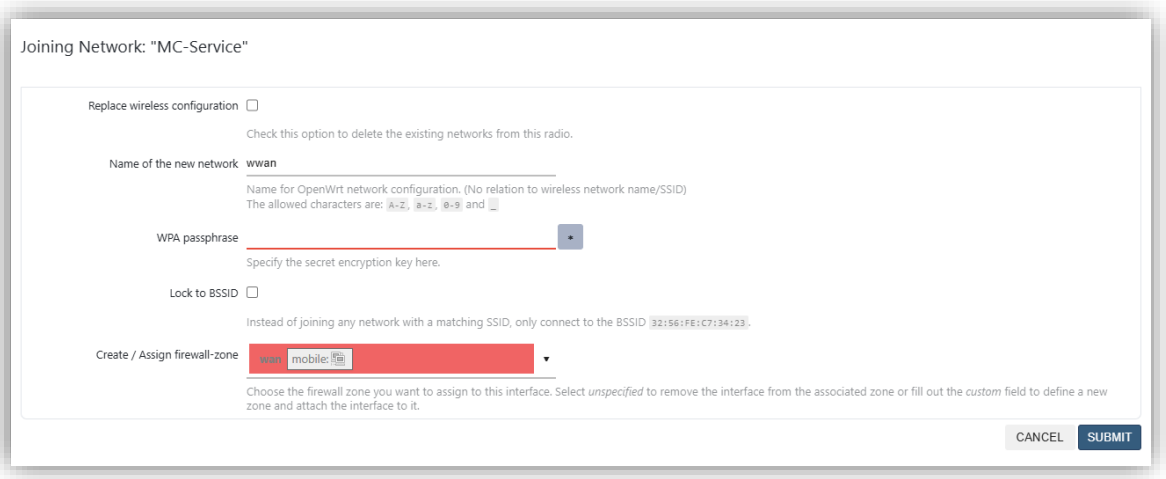
Stellen Sie *Network* auf *LAN* ein und setzen Sie einen Namen für das WLAN-Netzwerk im *ESSID-Feld*. Klicken Sie auf Wireless Security, um die Art der Verschlüsselung festzulegen (WPA2 oder besser empfohlen).



Klicken Sie auf ABSENDEN und dann auf SPEICHERN&ANWENDEN.
Nach einem Moment sollten Sie sich mit dem WLAN-Netzwerk verbinden und auf die Weboberfläche zugreifen können.

18.3.2 Client-Modus (STA)

Das Gateway kann als WLAN-Client verwendet werden, um sich mit einem Access Point zu verbinden. Navigieren Sie zu Network->Wireless und klicken Sie in der Wireless Overview auf SCAN. Wählen Sie das Netzwerk aus, mit dem Sie sich verbinden möchten, und klicken Sie auf BEITRETEN.



Geben Sie das WLAN-Passwort im *WPA-Passphrase-Feld* ein .
Klicken Sie auf ABSENDEN und dann auf SPEICHERN&ANWENDEN. Die WLAN-Verbindung dient nun als WAN-Verbindung.

19 Firewall

19.1 Einleitung

Die Firewall-Konfiguration von OpenWrt ermöglicht die gezielte Steuerung und Absicherung des Netzwerkverkehrs zwischen dem Gerät, internen Netzwerken und externen Verbindungen.

Sie dient dazu, den Datenverkehr basierend auf definierten Regeln zu zulassen, zu blockieren oder weiterzuleiten. Dadurch kann der Zugriff auf Systemdienste eingeschränkt und die Kommunikation zwischen verschiedenen Netzwerken kontrolliert werden.

Die Firewall beeinflusst nicht direkt das Routing, sondern verarbeitet Datenpakete anhand ihrer Eigenschaften (z. B. Quelle, Ziel, Protokoll und Port) und entscheidet auf dieser Basis über deren Behandlung.

Grundlegende Funktionen der Firewall sind:

- Filtern von Netzwerkverkehr
- Einschränken von Zugriffen auf Dienste und Schnittstellen
- Weiterleitung von Verbindungen (Portweiterleitung)
- Umsetzung von NAT (Network Address Translation)

Die Konfiguration erfolgt über ein regelbasiertes System, das auf sogenannten Zonen basiert.

19.2 Überblick

Die Firewall-Konfiguration besteht aus fünf Unterabschnitten:

Allgemeine Einstellungen, Port Forwards, Datenverkehrsregeln, NAT-Regeln und Benutzerdefinierte Regeln.

Im Reiter *Allgemeine Einstellungen* oder *Zoneneinstellungen* können grundlegende Konfigurationsoptionen und Standardpakethandhabungsregeln für das sogenannte Zonenkonzept eingestellt werden, das in den folgenden Kapiteln dargelegt wird.

Port Forwards erlaubt, wie der Name schon sagt, die Festlegung traditioneller Portweiterleitungsregeln zwischen verschiedenen Zonen.

Datenverkehrsregeln ermöglichen es, Ausnahmen zu den Zonenregeln hinzuzufügen und feingranulare Filterfunktionen zur Übereinstimmung des Verkehrs zu ermöglichen.

Mit *NAT-Regeln* können Adressumschreib- und Verbindungsverfolgungsmechanismen implementiert werden.

19.3 Allgemeine Einstellungen (Zoneneinstellungen)

Das Zonenkonzept gruppiert Netzwerkschnittstellen in sogenannte Zonen. Jede Zone verfügt über einen grundlegenden Satz von Regelketten (Eingabe, Ausgabe und Weiterleitung), die zwischen ihren

Netzwerkschnittstellen gemeinsam genutzt werden. Diese Regelketten repräsentieren die Politik zur Verarbeitung von Paketen für diese Zone. Die Richtlinie gilt für allen Datenverkehr, der von oder zu Netzwerkschnittstellen in dieser Zone bestimmt ist. Darüber hinaus kann die Weiterleitung des Verkehrs zwischen Zonen von Zone zu Zone überwacht und eingeschränkt und mittels Port Forwards, Datenverkehrsregeln und NAT-Regeln fein abgestimmt werden.

Die Erklärung der Überwachung der Verkehrsströme zwischen dem Host und den Netzwerkschnittstellen einer Zone verdient besondere Aufmerksamkeit, wie gezeigt wird. *Host* bezeichnet das Gateway und die Sockets der Anwendungen und Dienste, die direkt auf dem Gateway laufen. Regeln überwachen den Fluss und insbesondere die Weiterleitung des Verkehrs zwischen den Schnittstellen einer Zone untereinander und, auf einer höheren Ebene, zwischen Zonen und anderen Zonen.

Die Standardrichtlinie gilt, wenn keine Ausnahmeregel übereinstimmt, und kann entweder sein, das Paket zu akzeptieren (Akzeptieren), stillschweigend fallen zu lassen (Fallen zu lassen) oder das Paket mit einer ICMP-unerreichbaren Nachricht (Abweisen) zu beantworten.

Die Eingabe- und Ausgabeoptionen legen die Standardrichtlinien für den Datenverkehr fest, der zum Host bestimmt ist oder von ihm stammt (z. B. eine Webserver-Anwendung).

Die Weiterleitungsoption beschreibt die Richtlinie zur Behandlung von Verkehr, der aus der Zone stammt, für die der Routing-Algorithmus das Ziel als eine andere Schnittstelle in dieser Zone bestimmt hat.

zwischen verschiedenen Netzwerkschnittstellen innerhalb der Zone weitergeleitet. Diese dürfen nicht mit den Eingangs- und Ausgabeketten von iptables verwechselt werden.

19.3.1 Eingaberegeln

Die Eingaberegeln verarbeiten den Datenverkehr, der von einer der Netzwerkschnittstellen der Zone stammt und an einen Socket des Hosts, also eine Webserver-Anwendung, bestimmt ist. Zum Beispiel: Wenn die Eingaberichtlinie für das LAN-Netzwerk so eingestellt ist, dass sie ohne Ausnahmen abfällt, können Geräte im LAN-Netzwerk die Weboberfläche des Gateways nicht mehr erreichen.

In diesem Beispiel benötigt der Browser etwas Zeit und zeigt dann einen Timeout-Fehler an. Der Grund ist, dass das Paket abgeworfen wird, bevor es den Webserver erreicht. Wäre es auf Ablehnung eingestellt worden, wäre fast sofort eine ICMP-Antwort auf unerreichbar Empfang gesendet worden, was dem Browser erlaubt hätte, stattdessen einen Fehler "Website unerreichbar" anzuzeigen.

Falls ein Paket von der Input-Policy akzeptiert wird, wird für diesen sogenannten "Flow" ein Verbindungstracking-Eintrag erstellt, der eine bidirektionale Kommunikation ermöglicht, selbst wenn die Zone des Instanziators der Verbindung eine Drop- oder Reject-Ausgabepolitik hat.

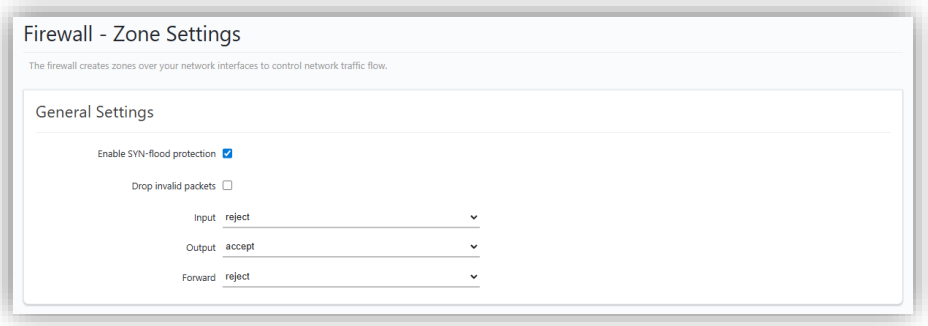
Dementsprechend wird das Akzeptieren des Pakets nicht nur vom LAN-Interface an den Webserver weitergeleitet, sondern ermöglicht es dem Webserver, unabhängig von der Ausgabepolitik dieser Zone zu antworten.

19.3.2 Ausgaberegeln

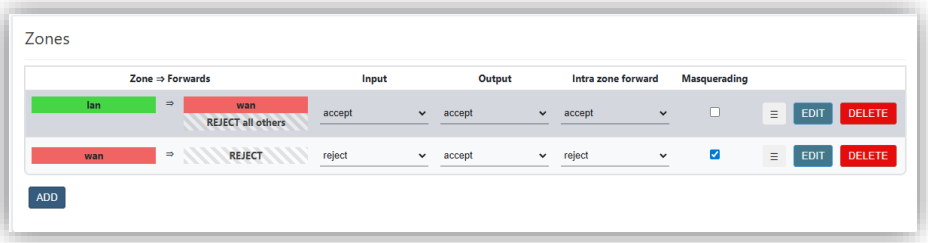
Die Ausgaberegeln überwachen den Datenverkehr, der vom Host stammt und zu einer Netzwerkschnittstelle in der entsprechenden Zone bestimmt ist. Da der Instanziator der Verbindung der Host selbst ist, wird diese Entscheidung direkt vor der Übertragung des Pakets auf dieser Netzwerkschnittstelle getroffen. Der Filter könnte das Paket trotzdem manipulieren oder sogar einfach abbrechen und das Übertragungsverfahren abbrechen.

19.3.3 Weiterleitungsregeln

Wenn auf *Akzeptieren gesetzt*, darf der Datenverkehr, der von einer Netzwerkschnittstelle in der Zone stammt, an eine andere Netzwerkschnittstelle in dieser Zone weitergeleitet werden. Das bedeutet, dass sie geroutet werden kann, wenn eine geeignete Route vorhanden ist. Andernfalls wird es stillschweigend verworfen (Drop) oder abgeworfen und mit einer ICMP-unerreichbaren Nachricht (Reject) beantwortet.

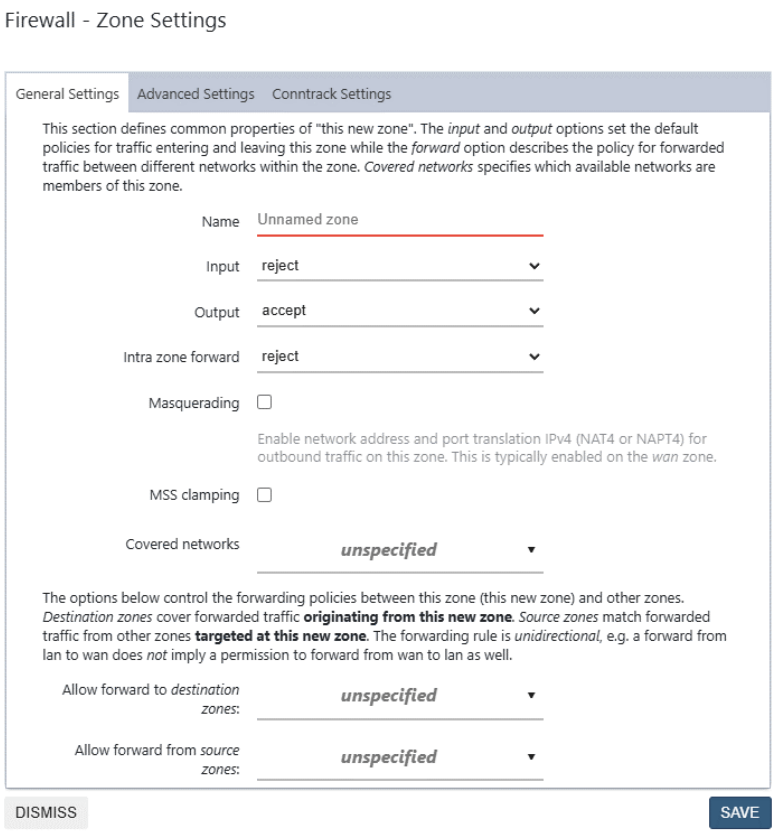


Die Zonenstandardregeln für Eingabe-, Ausgabe- und Weiterleitungsverkehr werden durch eine Menge zonenspezifischer Regeln überschrieben, die unter den grundlegenden Konfigurationsoptionen definiert sind.



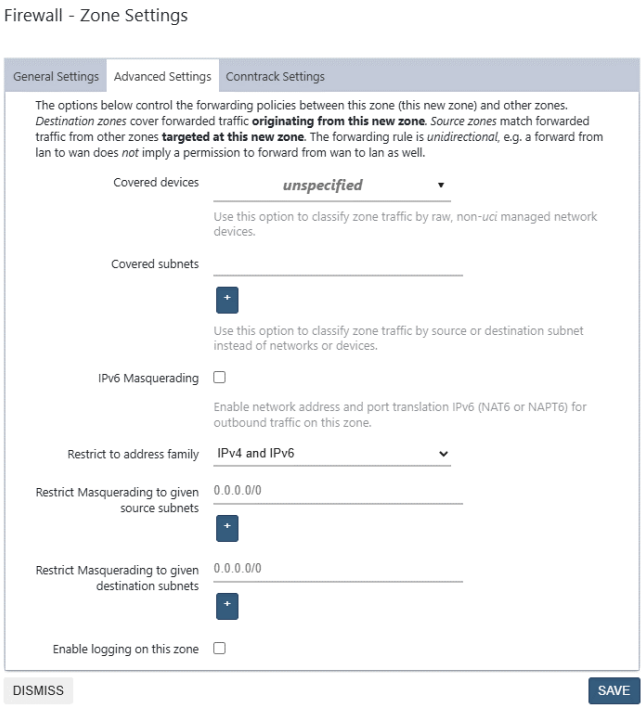
Die Weiterleitungsregel ist unidirektional, z. B. bedeutet eine Weiterleitung von LAN zu WAN keine Berechtigung, auch von WAN zu LAN weiterzuleiten.

19.3.4 Allgemeine Zoneneinstellungen



MSS-Clamping: MSS-Clamping fragmentiert und defragmentiert automatisch TCP-Pakete, die zwischen Netzwerkschnittstellen mit unterschiedlichen MTU-Eigenschaften weitergeleitet werden. Normalerweise würde die PMTU-Entdeckung dazu führen, dass die TCP-Verbindungen eine Paketgröße verwenden, die der niedrigsten MTU entlang des Pfades entspricht. Das könnte den Durchsatz einschränken, wenn es große Unterschiede in den MTU-Größen gibt. Das MSS-Abklemmen könnte diese Situation verbessern. Es erfordert jedoch einen höheren Rechenaufwand für Fragmentierung und Defragmentierung, was zu schlechteren Leistungen oder Latenzproblemen führen kann. Manchmal ist es notwendig, MSS-Klemmen zu verwenden, wenn die MTU eines Weges zu klein ist. Zum Beispiel benötigen IPv6-Pakete eine Paketgröße von mindestens 1280 Byte und könnten sonst nicht durch eine Schnittstelle mit einer kleineren MTU passen. In der Regel ist es sicher, das MSS-Klemmen auszuschalten .

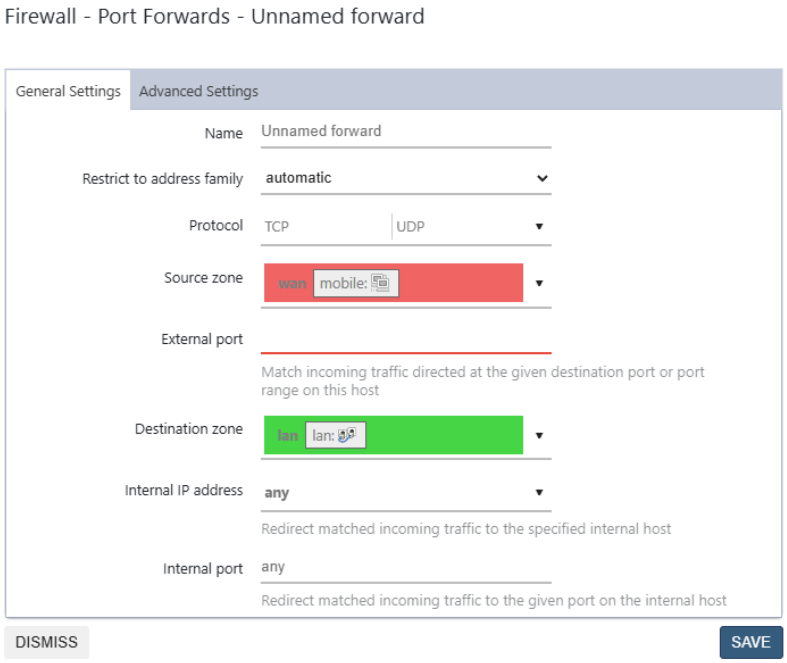
19.3.5 Erweiterte Zoneneinstellungen



- Restrict to address family definiert, zu welchen IP-Familien die Zone gehört (IPv4, IPv6 oder beides).
- Die Beschränkung des Masqueradings auf gegebene Quell-/Zielsubnetze definiert ein oder mehrere Subnetze, auf die die Masquerading-Option angewendet wird.
- Verbindungsverfolgung und Protokollierung ermöglichen zusätzliche Informationssammlung in der Zone.
- Kontrollen der Weiterleitungsrichtlinien zwischen neuen/bearbeiteten Zonen und anderen Zonen.
- Zielzonen decken weitergeleiteten Verkehr ab, der aus der neuen/bearbeiteten Zone stammt.
- Quellzonen stimmen mit weitergeleitetem Verkehr aus anderen Zonen überein, die auf die neue/bearbeitete Zone ausgerichtet sind.

19.4 Portweiterleitung

Die gängige Verwendung von Port Forwarding besteht darin, entfernten Computern aus dem WAN-Netzwerk (Internet) zu ermöglichen, eine Verbindung zu einem Port eines Dienstes zu initiieren, der auf einem Computer innerhalb des privaten (firewallgeschützten) LANs läuft. Einfach und allgemeiner ausgedrückt erlaubt es, ein Loch für einen bestimmten Port in der Firewall zu bohren und die eingehenden Pakete an eine vordefinierte Port-Adress-Kombination in einem anderen Netzwerk umzuleiten. Einstellungen für die Portweiterleitung des Geräts sind wie folgt definiert:



Name: Der Name der Portweiterleitungsregel.

Protokoll: Verwendetes Protokoll (Any/TCP/UDP/ICMP)

Quellzone: Informiert, welcher Schnittstellen-Weiterleitung zugeordnet wird.

Externer Anschluss: Informiert darüber, welcher Port Forward zugeordnet ist.

Zielzone: Informiert, an welche Schnittstelle weitergeleitet wird.

Vorstürzen zu: Informiert darüber, wohin der Port weitergeleitet wird.

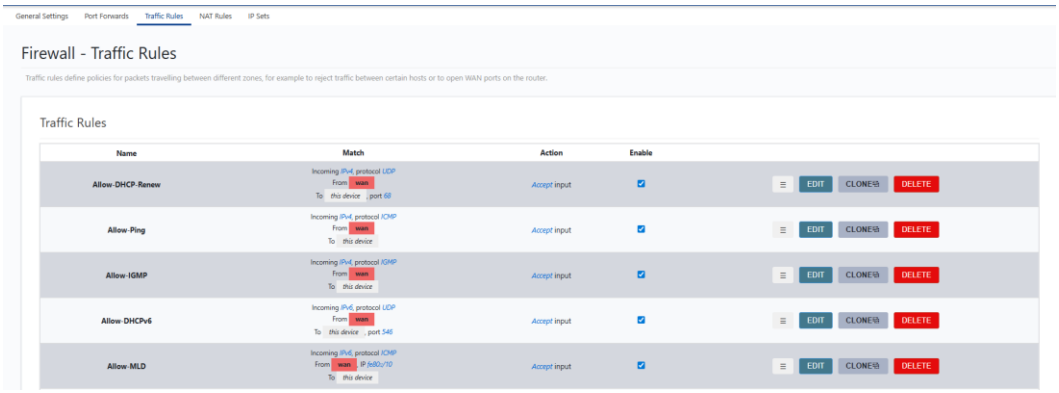
Interne IP-Adresse: Umleitung des eingehenden Datenverkehrs an den angegebenen internen Host.

Interner Port: Umleitung des eingehenden Datenverkehrs an den jeweiligen Port des internen Hosts.

Der Benutzer kann Port-Weiterleitungsregeln hinzufügen, bearbeiten oder löschen.

19.5 Datenverkehrsregeln

Datenverkehrsregeln definieren Richtlinien für Pakete, die zwischen verschiedenen Zonen reisen. Der Matching-Filter ermöglicht eine feine, detaillierte Definition davon, welche Art von Verkehr die Aktion ausgeführt wird.



Traffic kann d. h. basierend auf folgendem gematcht werden:

- IP-Protokoll
- Quell- und Zielzonen
- Quell-IP-Adresse und Port
- Ziel-IP-Adresse und Port
- Quelle-MAC-Adresse
- Paketzeichen
- DSCP (QoS)

Der Name der Verkehrsregel dient nur der internen Referenz und kann willkürlich gewählt werden.

19.6 NAT-Regeln

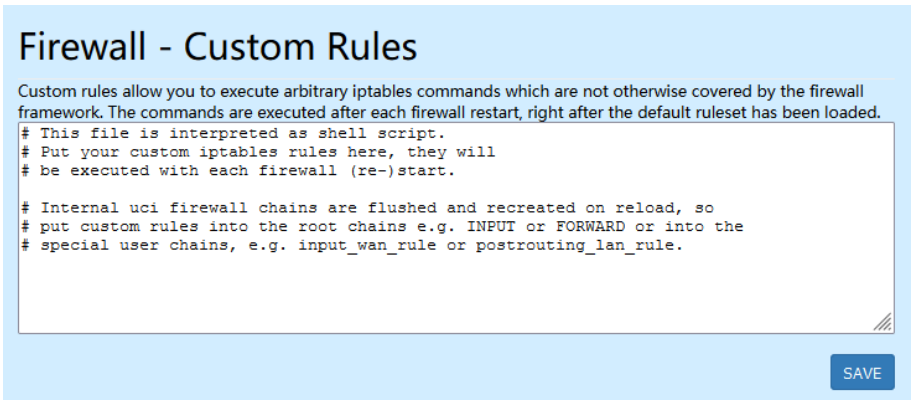
SNAT (Source NAT) ermöglicht es, die Quell-IP-Adresse von Paketen umzuschreiben, die für einen ausgehenden Verkehrsfluss verwendet werden. In Verbindung mit der Verbindungsverfolgung und einem DNAT (Destination NAT) für die eingehenden Antworten auf den Verkehrsfluss entsteht das sogenannte Masquerading, das sehr beliebt ist, um eine begrenzte Anzahl von WAN-IP-Adressen zwischen verschiedenen Geräten im LAN-Netzwerk zu teilen.

Der Benutzer kann Quell-NAT-Regeln hinzufügen, bearbeiten oder löschen. Für jede Regel können diese Optionen definiert werden:

- Name
- Protokoll
- Quell- und Zielzonen
- Quelle
- Ziel
- SNAT-IP-Adressen
- Ports
- Zusätzliche Argumente
- Monat
- Werktags
- Start-/Stoppdaten und -zeiten, Zeit in UTC.

19.7 Benutzer definierte Regeln

Benutzer definierte Regeln ermöglichen es, beliebige iptables-Befehle auszuführen, die sonst nicht vom Firewall-Framework abgedeckt sind. Die Befehle werden nach jedem Neustart der Firewall ausgeführt, direkt nachdem das Standardregelwerk geladen wurde.



20 VPN (Virtual Private Network)

Ein VPN ist ein Konzept zur Einrichtung kryptografisch gesicherter Tunnel zu ansonsten isolierten Netzwerken (z. B. einem Büronetzwerk) über ein ungesichertes Medium (meist das Internet). Durch die Verwendung kryptographischer Authentifizierung kann die Integrität der Übertragung überprüft

werden, während die Verschlüsselung das Abhören erschwert. Die am weitesten verbreiteten Open-Source-Softwarelösungen für diese Aufgabe sind IPSec, OpenVPN und WireGuard.

20.1 Protokollübersicht

Da IPSec ein tiefes kryptographisches Verständnis erfordert, um sicher konfiguriert zu werden, entwickelte sich OpenVPN aufgrund seiner einfacheren Konfiguration zu einer tragfähigen Alternative, was zu einer breiten Verbreitung führte.

Aus Performance-Sicht ist OpenVPN IPSec und WireGuard unterlegen, da OpenVPN-Prozesse im Nutzerland laufen. Zum Zeitpunkt des Schreibens erfordern Netzwerkschnittstellen im User Space einen Syscall für jedes zu verarbeitende Netzwerkpaket. Dies führt zu einer hohen Anzahl von Kontextwechseln, wodurch die Cache-Hotness und die Gesamteffizienz des Systems reduziert werden. Außerdem unterstützt OpenVPN kein Multithreading. Als Faustregel sollte dieser Leistungsnachteil berücksichtigt werden, wenn mehr als 20 Mbit/s Durchsatz zu erwarten ist.

Um die Leistungsbeschränkungen von OpenVPN zu beheben und das kryptografische Setup weiter zu vereinfachen und unmittelbar zu machen, wurde 2020 WireGuard eingeführt. Der Nachteil von WireGuard liegt jedoch in den begrenzten Konfigurationsparametern für Verschlüsselung, Authentifizierungsalgorithmen und Funktionen wie TAP/Layer-2-Tunnel oder Zertifikatsauthentifizierung. Die absichtliche Einschränkung kryptografischer Konfigurationsmöglichkeiten durch den Autor von WireGuard zielt darauf ab, Nutzer daran zu hindern, unsichere Einstellungen zu wählen.

Für Betreiber der VPN-Server-Infrastruktur stellt WireGuards fehlende offizielle Unterstützung für Abwärtskompatibilität zwischen Versionen Herausforderungen dar. Die Bereitstellung von WireGuard auf Geräten im Außendienst, wie zum Beispiel Customer Premise Equipment (CPE), erfordert eine alternative Methode zur Aktualisierung der Geräte unabhängig von der VPN-Verbindung, da Stromausfälle das Gerät möglicherweise aus dem Netzwerk ausschließen können, wenn die Serverversion ohne das Gerät aktualisiert wird. Dies, kombiniert mit dem Fehlen von Zertifikatsauthentifizierungsmöglichkeiten, kann die Bereitstellung von WireGuard in bestimmten Situationen schwierig machen.

Zusammen mit den fehlenden Zertifikats-Authentifizierungsmöglichkeiten macht dies sie für professionelle CPE-Einrichtungen manchmal unattraktiv.

Aus Sicherheitssicht ist es, da ein sachkundiger Sicherheitsexperte die Systeme ständig überprüft, wünschenswert, eine Reihe kryptografischer Algorithmen auf dem Server unterstützen zu können, während diese sich ständig weiterentwickeln. Verarbeitungsfähigkeiten (CPU-Befehlssatz, Hardware-Krypto-Beschleuniger) und Sicherheitsanforderungen können je nach Gerät und Anwendungsszenarien variieren. Mit der Fähigkeit von IPSec, die Menge kryptographischer Algorithmen zu verhandeln, kann es individuelle Anforderungen erfüllen, z. B. die Verschlüsselungsstärke anpassen und die Hardwarefähigkeiten auf Verbindungsebene effizient nutzen. So kann neue Kryptographie mit alten Konfigurationen koexistieren und so reibungslose Migrationen ermöglichen.

Zusammengefasst: WireGuard ist einfach zu bedienen, OpenVPN ist weit verbreitet und IPSec ist kompliziert, eignet sich aber am besten für fortgeschrittene Setups.

20.1.1 Öffentliche Schlüsselkryptographie

Im Vergleich zu gemeinsamen Geheimnissen bietet Public Key oder asymmetrische Kryptographie den Hauptvorteil, einen sicheren Kommunikationskanal über ein unsicheres Medium einrichten zu können. Anstelle eines gemeinsamen Geheimnisses haben bei Public-Key-Kryptographie beide Kommunikationsparteien ihren eigenen geheimen Schlüssel.

Diese sogenannten privaten Schlüssel werden mit einem entsprechenden öffentlichen Schlüssel geliefert und ermöglichen es dem Eigentümer, Daten zu signieren. Die Signaturen können dann von allen überprüft werden, um zu diesem spezifischen öffentlichen Schlüssel zu gehören.

Der öffentliche Schlüssel ist kein Geheimnis. Während er algorithmisch leicht aus dem privaten Schlüssel abgeleitet werden kann, gilt der umgekehrte Weg, einen privaten Schlüssel aus einem öffentlichen Schlüssel abzuleiten, als schwierig für sichere Algorithmen.

Neben der Möglichkeit, Daten zu signieren und die resultierenden Signaturen zu verifizieren, ermöglichen asymmetrische Verschlüsselungsschemata auch die Verschlüsselung von Daten mit einem öffentlichen Schlüssel, sodass der entsprechende private Schlüssel für die Entschlüsselung benötigt wird. Einfach ausgedrückt erzeugt er einen Chiffretext, den nur der Empfänger entschlüsseln kann.

Mit dieser Methode wird dann ein sicherer Kommunikationskanal eingerichtet, in dem z. B. ein gemeinsames Geheimnis ausgehandelt werden kann. Auf diese Weise können Chiffren mit effizienteren symmetrischen Verschlüsselungsschemata verwendet werden.

20.1.2 Zertifikate

Mit Public-Key-Kryptographie ist es möglich, eine Vertrauenskette aufzubauen. Ein häufig vertrauenswürdiger Dritter und sein private/öffentliches Schlüsselpaar werden als Vertrauensbasis gewählt. Diese häufig vertrauenswürdige dritte Partei wird üblicherweise genannt

Zertifikate sind CSRs (Certificate Signing Requests), die mit Public-Key-Kryptographie von einer CA (Certificate Authority) signiert wurden.

CA (Zertifizierungsstelle):

Zertifikat
Private KeyPublic Key

20.1.3 Sicherheitsbedenken

Es gibt im Grunde vier verschiedene Dateien

Um zu verhindern, dass Angreifer die entsprechenden privaten Schlüssel des Root-Zertifikats kompromittieren, ist es gute Praxis, die Schlüssel auf einem physisch gesicherten, vollständig verschlüsselten Computer zu generieren und zu speichern, der niemals Netzwerkzugang oder drahtlose Netzwerkperipheriegeräte haben wird. Dieser Computer darf nur für autorisierte Personen zur Unterzeichnung von Zertifikaten zugänglich sein. In Hochsicherheitsumgebungen konnte dieser Computer in einem Safe mit abgetrenntem Display und Kamera aufbewahrt werden. Spezielle Anwendungen können verwendet werden, um die Signing-Anfragen und Signaturen (QR-Codes) visuell zu übertragen, um Schnittstellenangriffe (z. B. BadUSB-Angriff) zu verhindern.

1. Die Übertragung eines Zertifikats (*.crt) und des zugehörigen privaten Schlüssels (*.key) über dasselbe Medium ist strengstens verboten.

2. Es ist unerlässlich, dass ein privater Schlüssel (*.key) zu jedem Zeitpunkt nur an einem Ort aufbewahrt wird.

3. Symmetrische Verschlüsselung eines privaten Schlüssels (*.key) ist unerlässlich, und EasyRSA benötigt dafür eine "Passphrase". Es ist jedoch nicht praktikabel, einen privaten Schlüssel (*.key) für den Servergebrauch symmetrisch zu verschlüsseln, da dies bei jedem Serverstart manuelle Eingabe der "Passphrase" erfordern würde. Daher müssen weitere Sicherheitsmaßnahmen vorhanden sein, um physischen Zugriff auf den Server zu verhindern.

4. Um maximale Sicherheit zu gewährleisten, signiert die Zertifizierungsstelle Zertifikatsanfragen (*.csr) von Clients und Servern, ohne Kenntnis ihres privaten Schlüssels (*.key). Weitere Informationen finden Sie in der README.quickstart.html-Akte.

5. EasyRSA verwendet Schlüssellängen von 2048 Bits, aber stärkere Schlüssellängen können bei Bedarf separat konfiguriert werden.

6. Die Erstellung von DH-Parametern mit 4096 Bit kann mehrere Tage dauern.

7. Server- und Client-Zertifikate, die mit EasyRSA generiert werden, sind 2 Jahre (825 Tage) gültig und müssen danach neu erstellt oder erneuert werden. 1. Die bereitgestellten Richtlinien wurden nach unserem besten Verständnis und Glauben formuliert und berücksichtigen die neuesten technologischen Fortschritte. Dennoch können täglich neue Sicherheitslücken auftreten, die die in diesem Handbuch beschriebenen Verfahren möglicherweise unsicher machen. Daher erfolgt die Nutzung dieses Handbuchs auf eigene Gefahr und Verantwortung. Es liegt an dem Nutzer, die hier dargelegten Vorschläge, Prinzipien, Anweisungen und Aufbauten zu bewerten. Die Entscheidung, ob und wie Sie diese Empfehlungen befolgen, liegt bei Ihnen als gewissenhaftem Administrator.

20.2 OpenVPN

Das OpenVPN-Protokoll verwendet üblicherweise einen Client-Server-Ansatz. Der Client fungiert als Initiator und stellt die Verbindung zum Server her. Sie wurde nicht standardisiert, aber Software-Client-Implementierungen existieren für viele Geräte, einschließlich Smartphones.

OpenVPN bietet zwei verschiedene Arten von Tunneln an. Das übliche verwendet eine TUN-Schnittstelle, die es ermöglicht, OSI-Datenpakete der Schicht 3 (IP-Protokoll) wie ein Gateway auszutauschen, während der TAP-Schnittstellentyp den Austausch von OSI-Layer-2-Paketen (Ethernet) wie ein Netzwerkswitch ermöglicht, der die beiden entfernten Netzwerke verbindet.

Die Initiierung einer OpenVPN-Verbindung erfordert eine passende Client- und Serverkonfiguration, die die Authentifizierungs-, Verschlüsselungs- und Adresszuordnungseinstellungen definiert.

20.2.1 Authentifizierung

Die drei Authentifizierungsmethoden, die OpenVPN unterstützt, sind eine Kombination aus Benutzernamen und Passwort, ein vorab geteilter Schlüssel (PSK), die Authentifizierung mit öffentlichen Schlüsseln und die Authentifizierung mit Zertifikaten.

Eine Kombination aus Benutzernamen und Passwort ist der intuitive Ansatz, erfordert jedoch ein starkes Passwort für ausreichende Sicherheit. Auch wenn dies beim Vor-Shared-Key-Ansatz nicht allzu bedenklich ist, muss man bedenken, dass ein kompromittiertes Passwort oder ein vorab geteilter Schlüssel es einem Angreifer ermöglicht, sowohl den Client als auch den Server in einem MITM-Angriffsszenario (Man-in-the-Middle) zu imitieren. Das ist besonders problematisch, wenn mehrere Geräte dieselben Zugangsdaten teilen.

Durch die Verwendung öffentlicher Schlüssel oder Zertifikate zur Authentifizierung können Server und Client jedoch eigene private Schlüssel haben. Sie überprüfen die Echtheit der Initiierungsnachricht mit dem öffentlichen Schlüssel der jeweils anderen oder bestätigen, dass das Zertifikat von einer vertrauenswürdigen dritten Partei (CA – Zertifizierungsstelle) unterzeichnet wurde. So beeinträchtigt z. B. der private Schlüssel eines kompromittierten Clients nicht zwangsläufig den Server. Zertifikate haben den zusätzlichen Vorteil, dass sie ein Ablaufdatum haben können, und falls z. B. der private Schlüssel eines Servers kompromittiert wurde, kann ein neues Zertifikat für ein neues öffentlich-privates Schlüsselpaar ausgestellt werden, ohne dass die Clients über den öffentlichen Schlüssel des neuen Servers informiert werden müssen.

20.2.1.1 Authentifizierung mit Benutzername und Passwort

```
# Speichern Sie Benutzername/Passwort-Zugangsdaten

umask go=

cat << EOF > /etc/openvpn/client.auth

BENUTZERNAME
```

PASSWORT

EOF

VPN-Dienst konfigurieren

cat << EOF >> /etc/openvpn/client.conf

auth-user-pass client.auth

EOF

Service OpenVPN Neustart

20.2.1.2 Erstellung eines CA

Eine CA ist ein öffentlich-privates Schlüsselpaar, das verwendet wird, um Zertifikate zu signieren, die in der Regel öffentliche Schlüssel von Einrichtungen enthalten, denen man vertraut, sowie Definitionen der gewährten Rechte. Im Fall von OpenWrt handelt es sich dabei um die öffentlichen Server- und Client-Public-Keys.

20.2.2 Client-Konfiguration

Im Folgenden wird ein Beispiel für die Interpretation und Konfiguration von OpenWrt mit einer OpenVPN-Client-Konfiguration gegeben, ähnlich wie sie ihren Kunden üblicherweise von kommerziellen VPN-Anbietern bereitgestellt werden. Für Setups, die eine ausgefeiltere Konfiguration erfordern, ist es ratsam, die offizielle OpenVPN-Dokumentation zu lesen.

Die erforderlichen Zertifikate werden in der Regel ebenfalls mit den Konfigurationsdetails bereitgestellt. OpenVPN kann entweder über die Weboberfläche konfiguriert werden oder indem man die Konfigurationsdateien hochlädt.

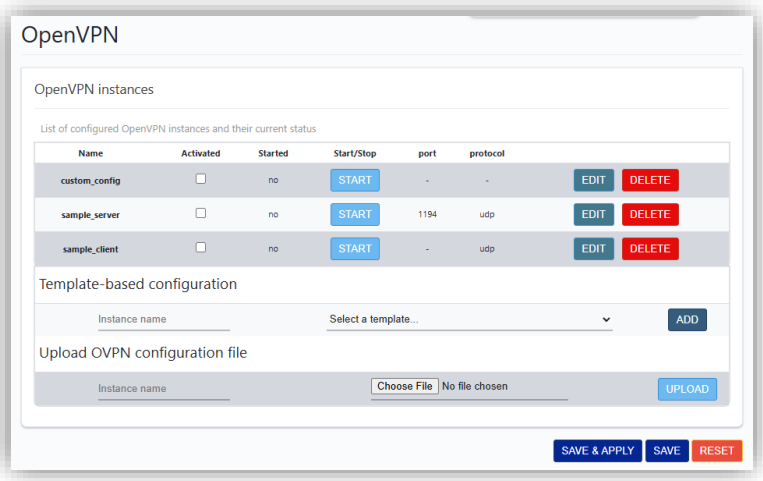
???? OpenVPN versucht automatisch, alle *.conf-Dateien im /etc/openvpn-Ordner zu laden. OpenVPN-Beispielkonfigurationen sind online verfügbar. Diese können in der Regel mit kleineren Änderungen angepasst werden.

Bevor Sie beginnen, erstellen Sie Ihre eigene Zertifizierungsstelle (CA), Zertifikate und Schlüssel für einen OpenVPN-Server und Clients.

Sie benötigen:

- Zertifizierungsstelle (ca.crt)
- Serverzertifikat (server.crt) und Serverschlüssel (server.key)
- Client-Zertifikat (client.crt) und Client-Schlüssel (client.key)
- Client-Konfiguration

Navigieren Sie zu OpenVPN->VPN.

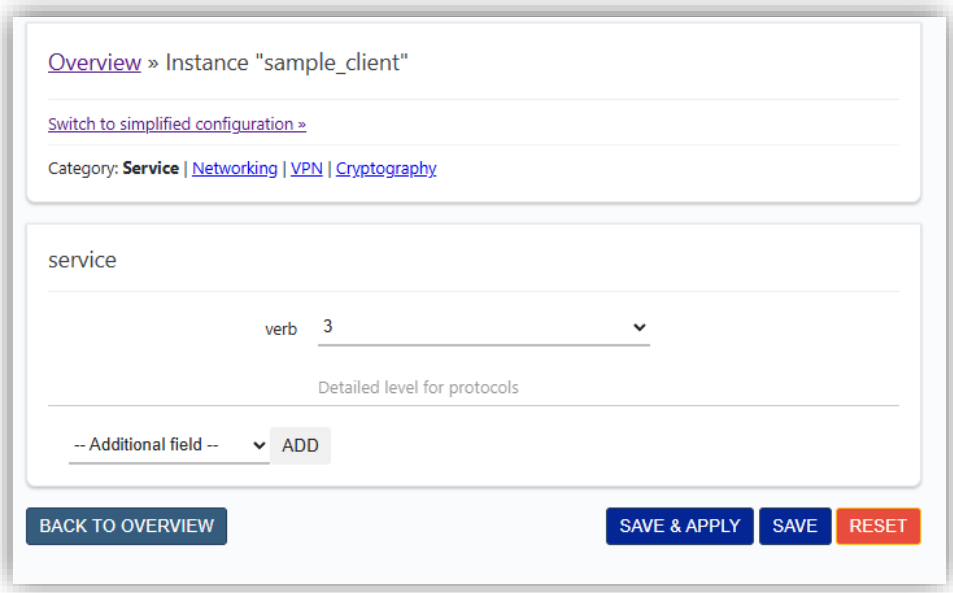


Klicken Sie neben sample_client auf BEARBEITEN.

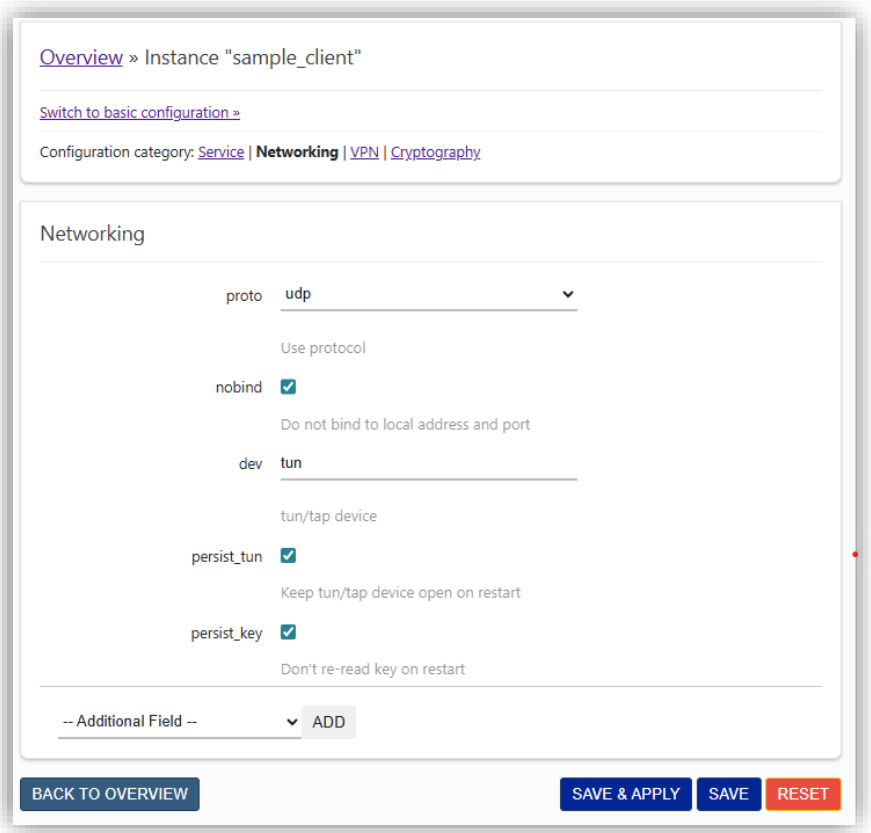
Klicken Sie auf Wechsel zur erweiterten Konfiguration.

Beispiel:

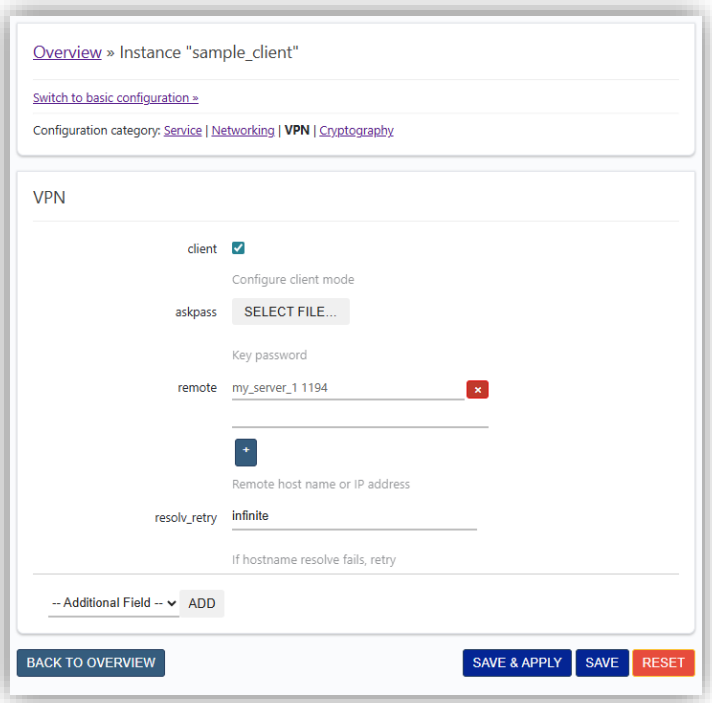
Unter Service ändert man "Verb" (Wortlautstärke), das ist nötig.



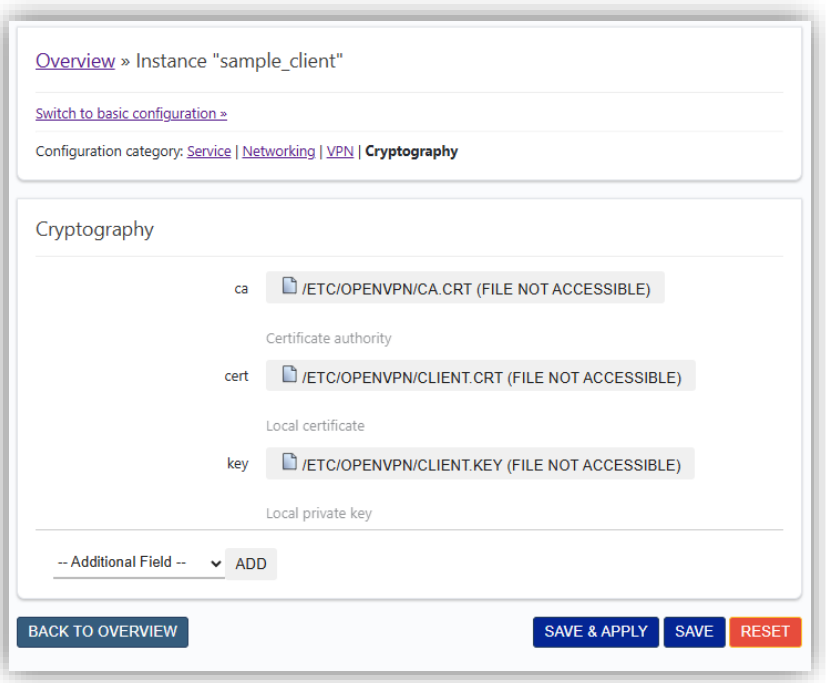
Unter Netzwerken ändere jede Einstellung nach Bedarf.



Wende die gleichen Einstellungen für den VPN-Bereich an.



Unter *Kryptographie* ändern Sie den Chiffre-Typ auf den, der für Ihre Zertifikate verwendet wird (Sie können die fehlende Konfiguration mit der Option –Additional Field-- hinzufügen).



Lade die Dateien in den Ordner /etc/luci-uploads/ hoch.

Klicken Sie auf SPEICHERN & ANWENDEN und dann ZURÜCK ZUR ÜBERSICHT.

Aktivieren Sie die konfigurierte Instanz, klicken Sie dann auf "SPEICHERN UND ANWENDEN" und dann auf "START".

21 Einführung in Node-RED

Node-RED ist ein visuelles Programmierwerkzeug, das es ermöglicht, Web-APIs, IoT-Geräte, APIs und Online-Dienste einfach miteinander zu verbinden und zu steuern. Es baut auf Node.js auf und nutzt die Vorteile seines ereignisgesteuerten, nicht blockierenden Modells voll aus.

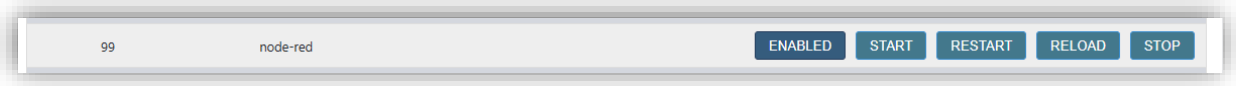
Es bietet einen browserbasierten Editor, der es ermöglicht, Flows einfach zu verdrahten, indem man die große Bandbreite an Knoten in der Palette nutzt.

Man kann die Node-RED-Webschnittstelle mit derselben IP-Adresse wie die Standard-Weboberfläche und der Portspezifikation (z. B. 1880) erreichen.

Beispiel mit Standardadresse: https://192.168.2.1:1880

21.1 Aktivieren von Node-RED

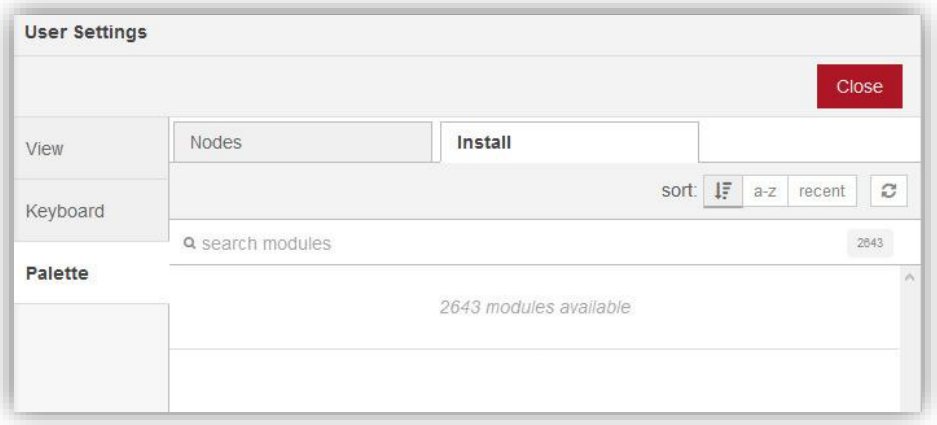
Klicken Sie unter System->Startup auf die Schaltfläche "Aktivieren/Deaktivieren" neben dem Dienst "node-red".



21.2 Installation von Modulen

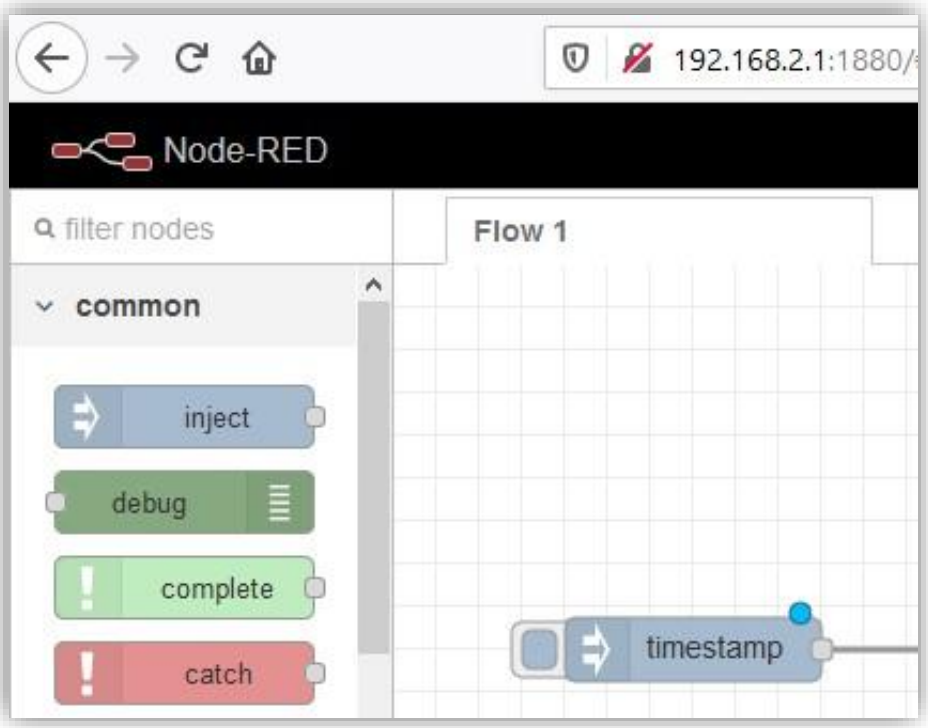
Um Module für Node-RED zu installieren:

1. Navigieren Sie in Ihrem Browser zur Node-RED-Weboberfläche
2. Öffnen Sie das Menü (≡)
3. Klicken Sie auf Palette verwalten.
4. Wechsle zum Installationsreiter



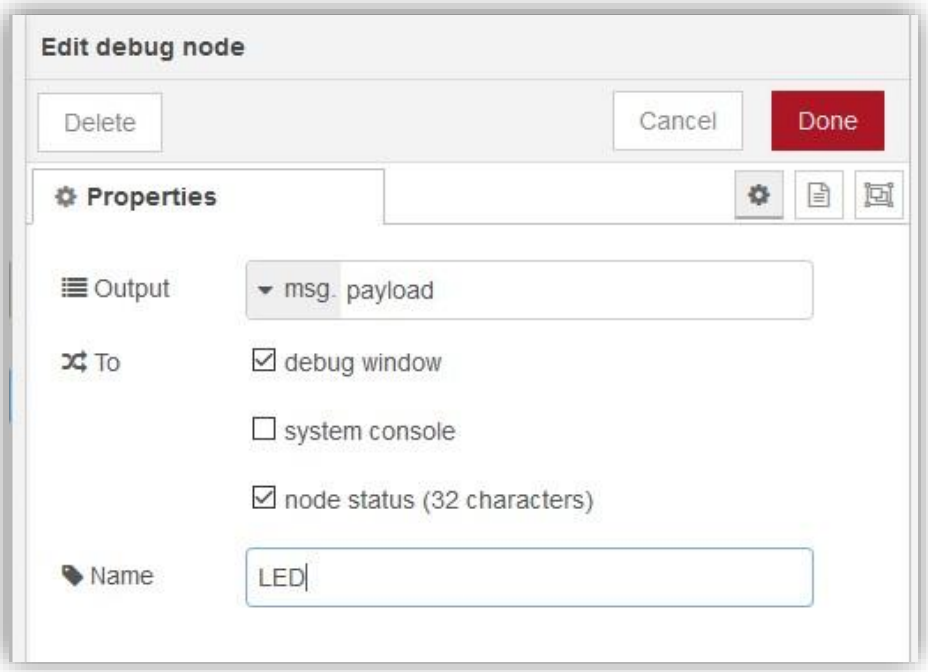
Geben Sie den Namen des Moduls in das Sucheingabefeld ein und klicken Sie auf *Module suchen*.

21.3 Hinzufügen eines Knotens



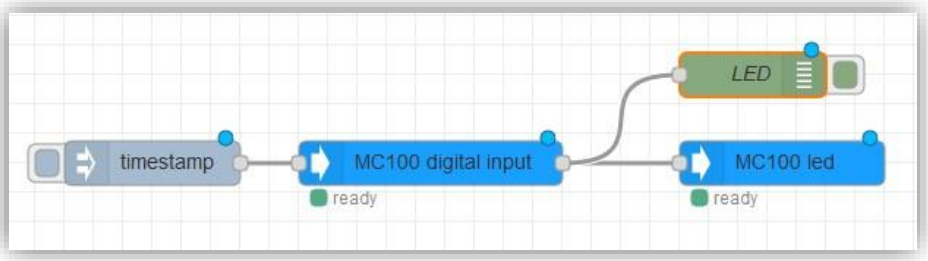
Wählen Sie den Knoten aus, den Sie aus der Knotenliste hinzufügen möchten (z. B. Knoten injizieren, Nachrichten in einen Fluss einfügen). Ziehen Sie den ausgewählten Knoten in den Arbeitsbereich.

21.4 Hinzufügen eines Debug-Knotens



Der Debug-Knoten zeigt die Nutzlast der Nachricht oder des gesamten Nachrichtenobjekts an. Sie kann aus ihrer Einstellung durch Doppelklick umbenannt werden.

21.5 Verbindung der Knoten



Nachdem alle gewünschten Knoten hinzugefügt wurden, werden sie miteinander verdrahtet, indem eine Leitung von einem Ausgang eines Knotens zum Eingang eines anderen Knotens gezogen wird, wodurch die Ausgangsdaten eines Knotens an den Eingang des anderen weitergeleitet werden.

21.6 Bereitstellen des Flows (Deploy)

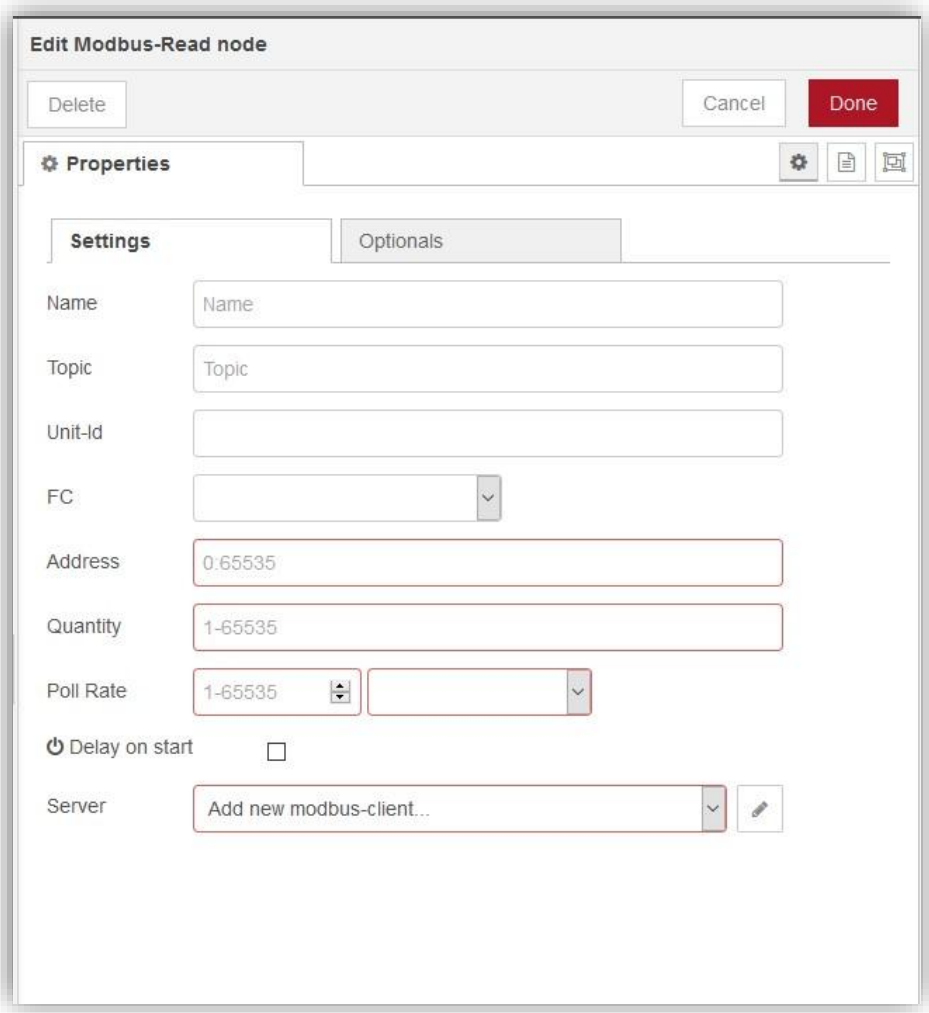
Um die Änderungen in Kraft zu setzen und die Verarbeitung zu starten, klicken Sie oben rechts auf die Schaltfläche "Deploy ".

21.7 Modbus mit Node-RED

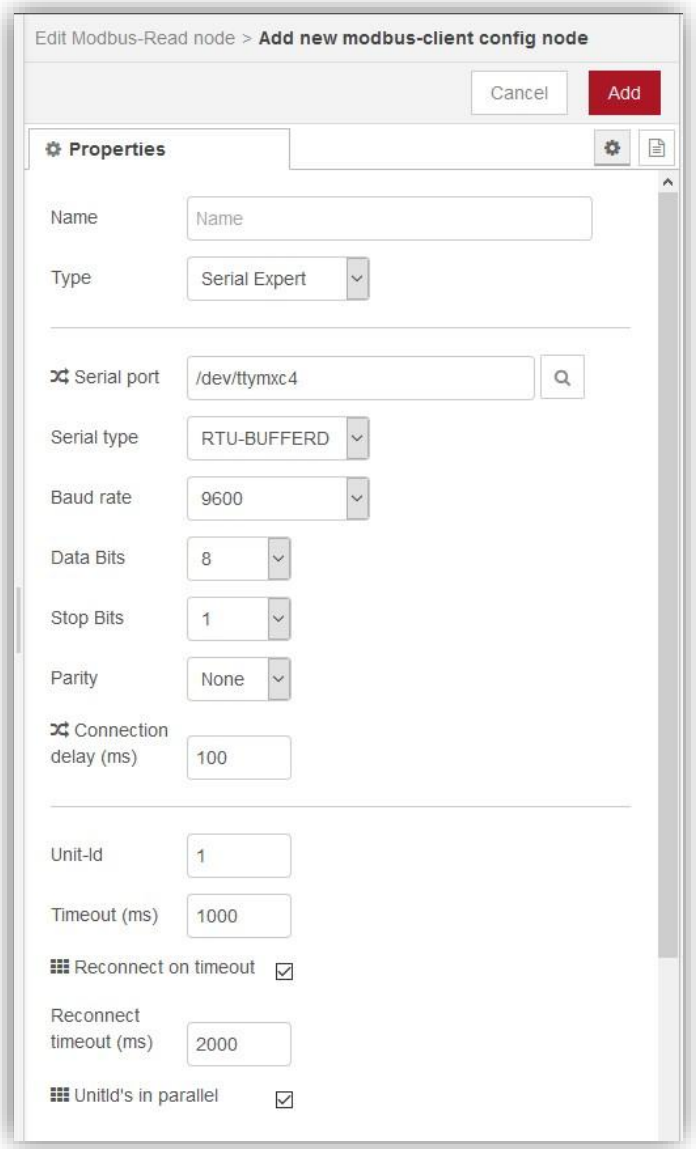
node-red-modbus ist ab Werk auf dem MC100 installiert. Versuchen Sie nicht, das Node-red-contrib-modbus-Paket innerhalb von Node-RED zu installieren.

21.7.1 Schaffung eines ersten Flusses

1. Öffnen Sie Node-Red in ihrem Browser.
2. Debug-Knoten hinzufügen.
3. Modbus-Leseknoten hinzufügen.
4. Verbinden Sie die Knoten miteinander.
5. Doppelklicken Sie auf den Modbus-Leseknoten, um ihn zu konfigurieren.
6. Ändern Sie die Einstellungen je nachdem, welches Gerät Sie auslesen möchten.
7. Klicken Sie auf den Bearbeiten-Button in der Nähe des Servers, um das Modbus-Gerät zu konfigurieren.



8. Typ zu Serial Expert ändern.



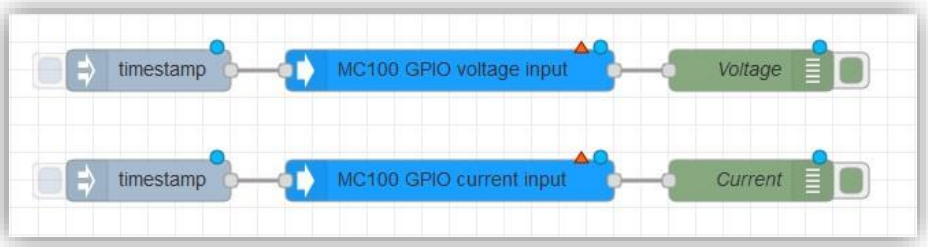
9. Seriellen Port in /dev/ttymxc4 ändern
10. Stellen Sie sicher, dass der Serial Type RTU-BUFFERED und nicht RTU ist.
11. Setzen Sie den Knoten ein.

Im *Debug-Tab* können die Nachrichten angezeigt werden.

21.8 MC100 GPIO

21.8.1 Analoge Eingänge (Strom oder Spannung)

1. Fügen Sie den Inject-Knoten hinzu
2. Spannungseingangs-/Stromeingangsknoten hinzufügen
3. Debug-Knoten hinzufügen.
4. Verbinden Sie die Knoten und stellen Sie den Flow über "Deploy" bereit

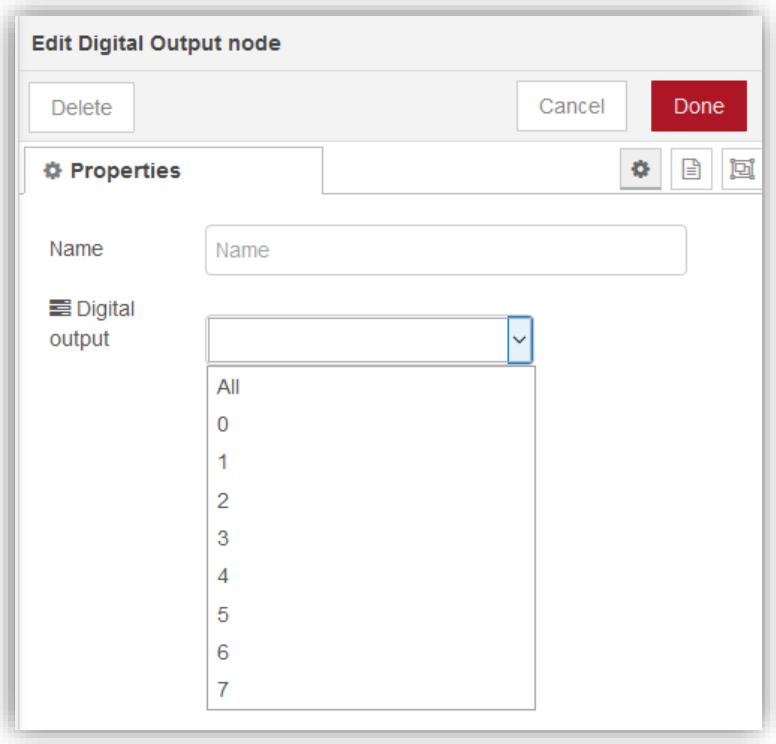


21.8.2 Digitale Eingänge

1. Fügen Sie den Inject-Knoten hinzu.
2. Fügen Sie den digitalen Eingangsknoten hinzu.
3. Doppelklicken Sie auf den digitalen Eingangsknoten MC100 GPIO, um das Einstellungsmenü zu öffnen und einen digitalen Eingang auszuwählen.
4. Fügen Sie den Debug-Knoten hinzu (Name ändern, falls wünschend).
5. Verbinden Sie die Knoten und stellen Sie den Flow über "Deploy" bereit

21.8.3 Digitale Ausgänge

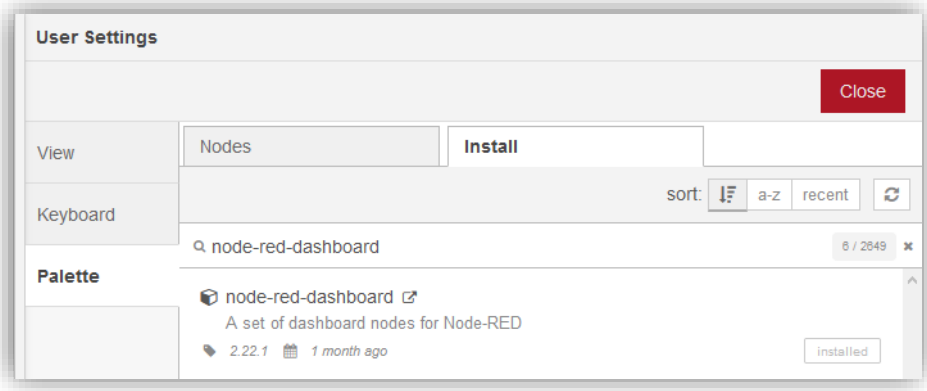
1. Fügen Sie den Inject-Knoten hinzu.
2. Fügen Sie den digitalen Ausgangsknoten hinzu.
3. Doppelklicken Sie auf den digitalen Ausgangsknoten MC100 GPIO, um das Einstellungsmenü zu öffnen und einen der digitalen Eingänge aus der Dropdown-Liste auszuwählen.



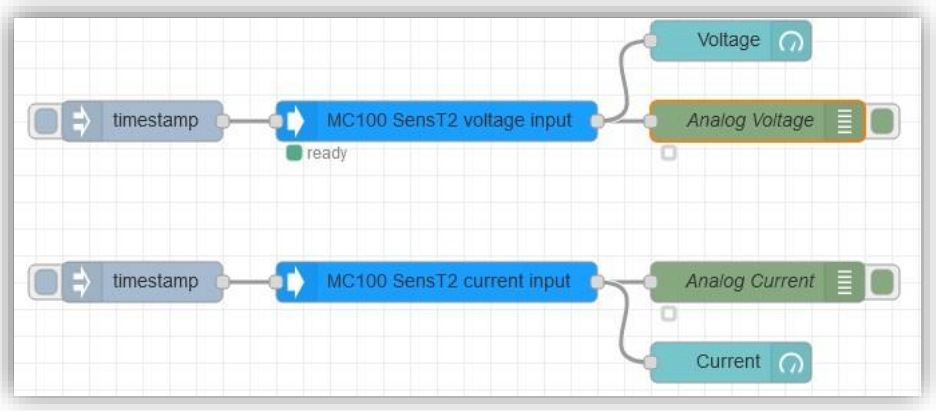
4. Debug-Knoten hinzufügen (Name ändern, falls wünschend).
5. Verbinden Sie die Knoten und stellen Sie den Flow über "Deploy" bereit

21.8.4 Armaturenbrett

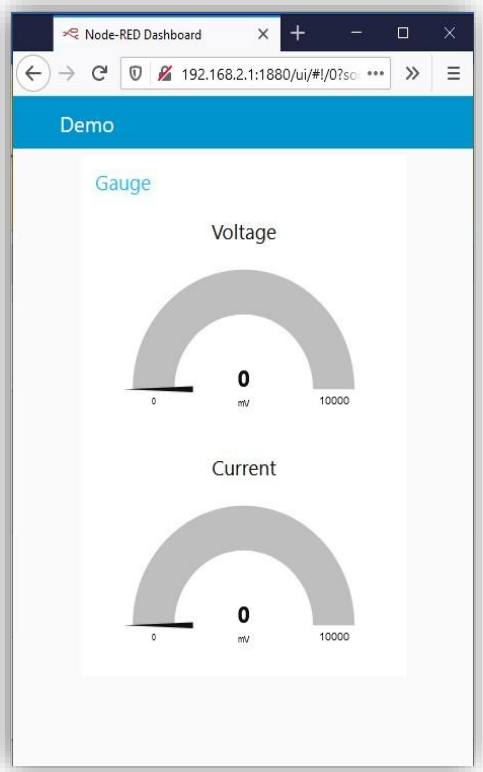
1. Verwenden Sie Menü – Palette verwalten, um nach "node-red-dashboard" zu suchen und klicken Sie auf Installieren.



2. Neustarte Node-RED, der Dashboard-Tab sollte im rechten Panel erscheinen.
3. Vom Dashboard-Tab aus fügen Sie die gewünschten Knoten (z. B. Gauge) hinzu und verbinden Sie sie.



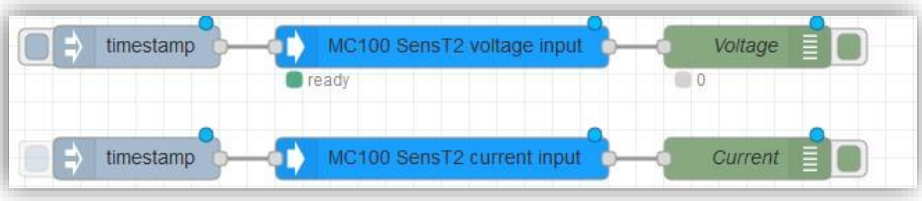
4. Doppelklicken Sie auf die Knoten, um ihre Eigenschaften nach Belieben zu ändern.
5. In einem neuen Tab öffnen Sie http://localhost:1880/ui (z. B. http://192.168.2.1:1880/ui)



21.9 MC100 SensT2

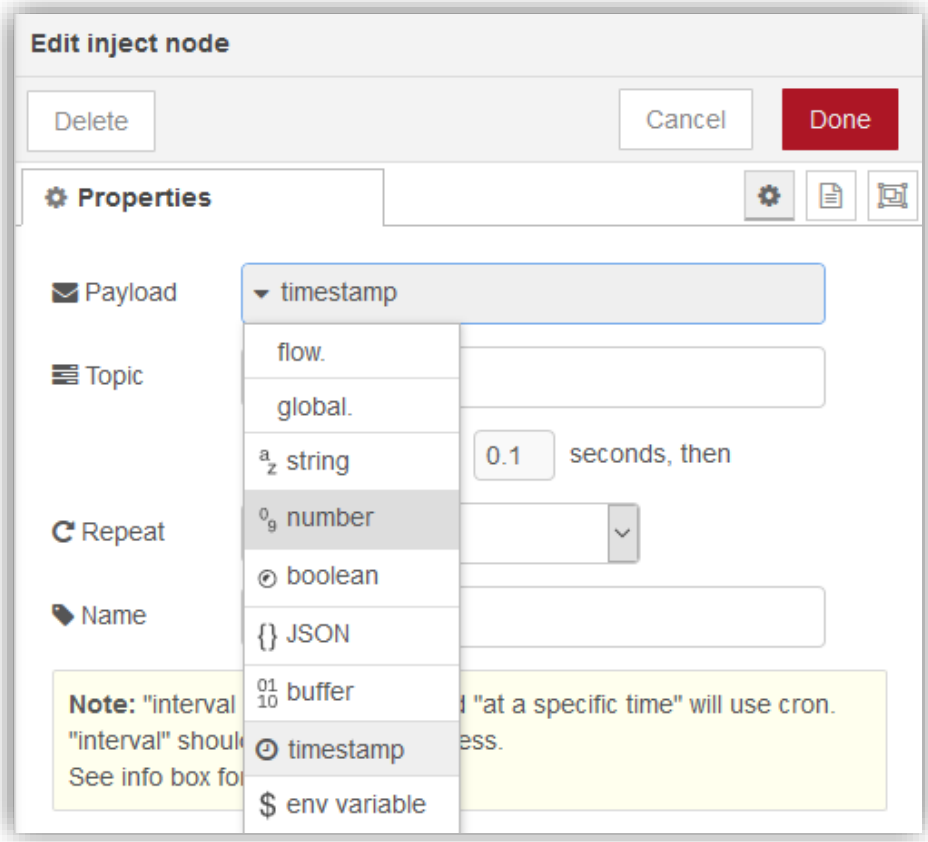
21.9.1 Analoge Eingänge

1. Fügen Sie den Inject-Knoten hinzu.
2. Fügen Sie den Spannungseingangs-/Stromeingangsknoten hinzu.
3. Debug-Knoten hinzufügen.
4. Alles verbinden (wie auf dem Bild gezeigt) und bereitstellen (deploy).



21.9.2 Analoge Ausgänge schreiben

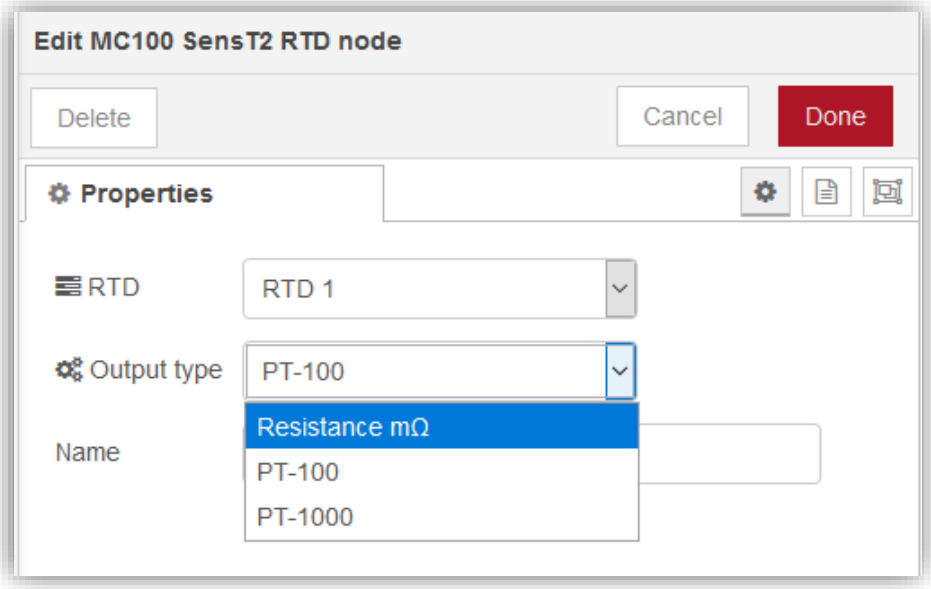
1. Fügen Sie inject node hinzu, doppelklicken Sie und ändere die Payload auf Zahlen und gib den analogen Wert ein (= Strom in [4-20] mA).



2. Fügen Sie MC100 SensT2 Stromausgangsknoten hinzu.
3. Verbinden Sie die Knoten und stellen Sie den Flow über "Deploy" bereit

21.9.3 PT100/1000

1. Fügen Sie den Inject-Knoten hinzu
2. MC100 SensT2 RTD hinzufügen
3. Doppelklicken Sie auf den MC100 SensT2 RTD-Knoten, um das Einstellungsmenü zu öffnen und wählen Sie RTD und Ausgabe-Typ aus.
4. Debug-Knoten hinzufügen (Name bei Wunsch ändern)



5. Verbinden und ausführen

21.10 SMS mit Node-RED

Um SMS mit Node-RED empfangen und senden zu können, empfehlen wir die Verwendung von *smstools3*, das vorinstalliert ist. Sie muss im *System->Startup* in der Hauptweboberfläche des Geräts aktiviert werden. Zusätzlich muss das Modul *node-red-contrib-smstools* in der Node-RED-Weboberfläche installiert werden.

Beispielablauf:

```
[
  {
    "id": "ba93e143ba53abb0",
    "typ": "tab",
    "Label": "Flow 1",
    "disabled": falsch,
    "Info": "",
    "ENV": []
  },
  {
    "id": "7f6ca9491a224ed4",
    "tippen": "SMS-in",
    "z": "ba93e143ba53abb0",
    "name": "",
    "x": 690,
    "y": 120,
    "Drähte": [
      [
        "5472e1d192fd03ae"
      ]
    ]
  },
  {
    "id": "809bf79731e1eb78",
    "Typ": "SMS-Out",
    "z": "ba93e143ba53abb0",
    "name": "",
    "Thema": "+4915786336816",
    "x": 1040,
    "y": 280,
    "Drähte": []
  },
  {
    "id": "3a3810b48635eda8",
    "Typ": "Injizieren",
    "z": "ba93e143ba53abb0",
    "name": "",
    "Requisiten": [
      {
        "p": "Nutzlast"
      },
      {
        "p": "Thema",
        "VT": "STR"
      }
    ],
    "wiederholen": "",
    "Crontab": "",
    "einmal": falsch,
    "onceDelay": 0,1,
    "Thema": "",
    "Nutzlast": "Hallo",
    "payloadType": "str",
    "x": 690,
    "y": 280,
    "Drähte": [
      [
        "809bf79731e1eb78"
      ]
    ]
  },
  {
    "id": "5472e1d192fd03ae",
    "type": "debug",
    "z": "ba93e143ba53abb0",
    "name": "",
    "aktiv": wahr,
    "Tosidebar": Wahr,
    "Konsole": falsch,
    "Tostatus": falsch,
    "vollständig": "wahr",
    "targetType": "full",
    "statusVal": "",
    "statusType": "auto",
    "x": 1030,
    "y": 120,
    "Drähte": []
  }
]
```


Hinweis: Ein Neustart kann notwendig sein, damit die Änderungen in Kraft treten.

22 Diagnostik und Systemüberwachung

22.1 Konnektivitätsprüfung

Ein Tool zur Durchführung von Ping- und Traceroute-Tests findet sich in Network->Diagnostics. Klicken Sie auf die entsprechenden Schaltflächen unter "Diagnostik", um einen Test durchzuführen.

22.2 MCINFO

mcinfo ist ein auf dem Gateway installiertes Kommandozeilen-Tool, das über SSH verwendet werden kann. Es bietet ausführliche Debugging-Informationen wie den Modemstatus und Geräteinformationen.

mcinfo info	Drucken Sie allgemeine Informationen zum Modem aus.
MCINFO Mobile	Druck Informationen zum Status der mobilen Kommunikation aus.

```
root@MCLH:~# mcinfo
Usage: mcinfo [options] [command[ command]]

Options:
  -h          Show this help message and exit.
  -v          Print verbose debug information to error
  -V          Show version information and exit.
  -d DEVICE   Set the tty device (default: /dev/ttyUSB3)
  -c COMMAND  Send COMMAND to modem.
  -t TIME     define the timeout in deciseconds
                  default: 1

Command:
info   Print general information about the modem.
mobile Print information about mobil communication status
gpio  Print information about external GPIO module pins
root@MCLH:~#
```

22.3 ACT8847 Hardware-Watchdog

Der MC100 ist mit einem eingebauten Hardware-Watchdog ausgestattet, der in seinen PMIC-Chip ACT8847 integriert ist. MC Technologies hat für diesen Hardware-Watchdog ein Kernel-Modul entwickelt, das der Linux-Kernel-API-Spezifikation für Hardware-Watchdog-Treiber entspricht.

22.3.1 Parameterübersicht

Das Modul heißt mc-act8847-wdt und kann mit folgenden Parametern geladen werden:

Nowayout	Verbieten Sie das Stoppen der Hardware-Watchdog, sobald sie gestartet wurde. (type=boolean, default=0)
Herzschlag	Das Zeitintervall in Sekunden, in dem der User Space das Kernel-Modul pingen muss, um einen Power-Cycle zu verhindern (Wert = Ganzzahl, Standard = 60)
Hardreboot	Stoppen Sie den Hardware-Watchdog nicht vor einem Neustart oder Abschalten . Dadurch kann das Gerät anstelle eines normalen Neustarts neu gestartet werden. (type=boolean, default=0)
Hardunload	Halte den Hardware-Watchdog aktiv, auch wenn das Kernel-Modul entladen ist. So wird sichergestellt, dass das Gerät vier Sekunden nach dem Entladen des Moduls einen Neustart durchführt und das Gerät durch Entladen des Moduls zwangsweise neu starten kann. (type=boolean, default=0)

22.3.2 Entlastung des Moduls

Falls das Modul bereits geladen ist, kann es mit dem Befehl entladen werden:

RMMOD MC-ACT8847-WDT

22.3.3 Laden mit Parametern

Mehrere Parameter können durch Räume getrennt definiert werden:

insmod /lib/modules/<kernelversion>/mc-act8847-wdt.ko <parameter>=<value>

22.3.4 Parameteränderung zur Laufzeit

Einige Parameter sind zur Laufzeit mit Sysfs-Einträgen im folgenden Verzeichnis beschreibbar:

/sys/module/mc_act8847_wtd/parameters/

22.3.5 Festlegen persistenter Optionen

Um Optionen zum Booten einzustellen, kann man eine Konfigurationsdatei in */etc/modules.d/ erstellen,* z. B. *mc-act8847-wdt.conf,* mit Optionen, die im folgenden Format definiert sind:

Option MC-act8847-WDT-heartbeat=30

option-mc-act8847-wdt-nowayout=1

22.3.6 Nutzung des Watchdog

Standardmäßig wird OpenWrt mit einem in procd integrierten Watchdog-Daemon geliefert, der als Init-Prozess (mit PID1) läuft. Es übernimmt die Kontrolle über das Watchdoggerät und startet

automatisch den Watchdog-Timer beim Boot. Es ist möglich, den Watchdog-Daemon von procd zu deaktivieren, um z. B. eine kritische Anwendung stattdessen das Ping übernehmen zu lassen. Wenn die kritische Anwendung abstürzt oder den Watchdog nicht pingt, wird der Watchdog ausgelöst.

22.3.7 Den Status von Procds Watchdog-Dämon lesen

Der Status kann durch Ausführung des Befehls *ubus Call System Watchdog ausgelesen werden*

Beispielausgabe:

```
{
   "Status": "laufend",
   "Auszeit": 30,
   "Frequenz": 5
}
```

22.3.8 Wechsel zur manuellen Steuerung

Nur ein Prozess kann die Watchdog-Datei gleichzeitig öffnen. Um den Procd-Watchdog-Daemon zu deaktivieren, führe aus:

```
UBUS ruft System-Watchdog '{"MagicClose":True}' an
```

```
UBUS Call System Watchdog '{"stop":true}'
```

22.3.9 Beispiel für das Pingen des Watchdog

Sobald die Watchdog-Datei geöffnet wurde, startet der Timer. Ein Schreiben in die Watchdog-Datei setzt den Timeout-Zähler zurück und verhindert, dass der Watchdog auslöst. Die folgende Schleife läuft, bis der Benutzer ein SIGINT (Strg + c) sendet. Der Watchdog nimmt schließlich eine Auszeit und wird ausgelöst.

```
während :; Mach Echo 1 > /dev/watchdog; sleep 5; fertig
```

22.3.10 Beispiel für das Stoppen des Watchdog

Sofern der *Nowayout-Parameter* nicht auf true gesetzt ist, kann das Schließen der Watchdog-Datei den Watchdog stoppen, wenn das magische Zeichen "V" direkt vor dem Schließen der Datei geschrieben wird.

Die folgende Schleife läuft, bis der Benutzer ein SIGINT (Strg + c) sendet, die dann den Watchdog durch das Schreiben des Sonderzeichens "V" beendet.

```
trap 'echo -n V > /dev/watchdog; break' SIGINT && während :; Do Echo 1 >
/dev/watchdog && sleep 5; fertig
```

23 Konfigurations- und Anwendungsbeispiele

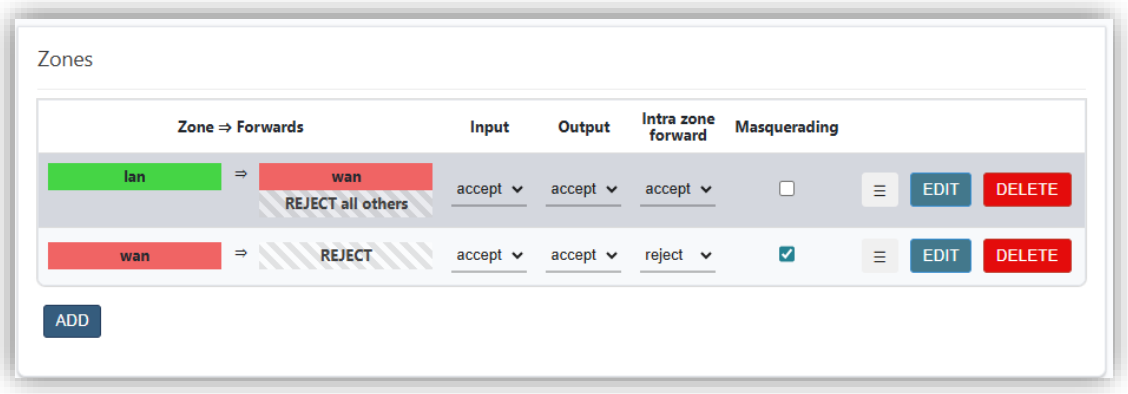
23.1 Neukonfiguration eines Ethernet-Anschlusses als WAN-Schnittstelle

Wenn Ihr Gateway noch keine WAN-Schnittstelle konfiguriert hat, ist es notwendig, die bestehende LAN-Schnittstelle als WAN-Schnittstelle neu zu konfigurieren. Falls bereits eine WAN-Oberfläche konfiguriert wurde, stellen Sie bitte sicher, dass die Einstellungen mit den unten aufgeführten Vorschlägen übereinstimmen.

23.1.1 Zugriff auf die Weboberfläche vom WAN-Netzwerk aus gewährt

Bevor die LAN-Schnittstelle entfernt wird, muss dem Gateway ein Firewall-Zugriff von der WAN-Netzwerkzone gewährt werden. Andernfalls ist der Zugriff auf das Gateway nicht mehr möglich und ein Werksreset könnte der einzige Ausweg sein, um den Zugriff wiederherzustellen. **Bitte beachten Sie, dass dies ein Sicherheitsrisiko darstellt, da die Weboberfläche und die Dienste allen Netzwerken in dieser Firewall-Zone, einschließlich des mobilen WAN-Netzwerks, ausgesetzt sind.** Es ist z. B. möglich, eine separate Zone zur Einschränkung des Zugriffs vom mobilen WAN-Netzwerk zu schaffen, aber das fällt für dieses Beispiel nicht in den Anwendungsbereich.

Um Zugriff auf das Gateway aus der WAN-Zone zu gewähren, wählen Sie in der Spalte "Eingabe" der WAN=>REJECT Weiterleitungsregel auf akzeptieren und klicken dann auf SPEICHERN & ANWENDEN.

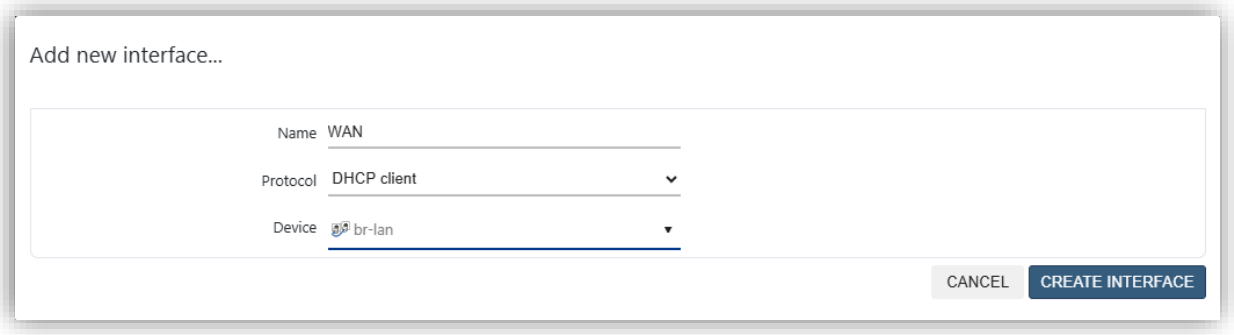


23.1.2 Entfernung der bestehenden LAN-Schnittstelle

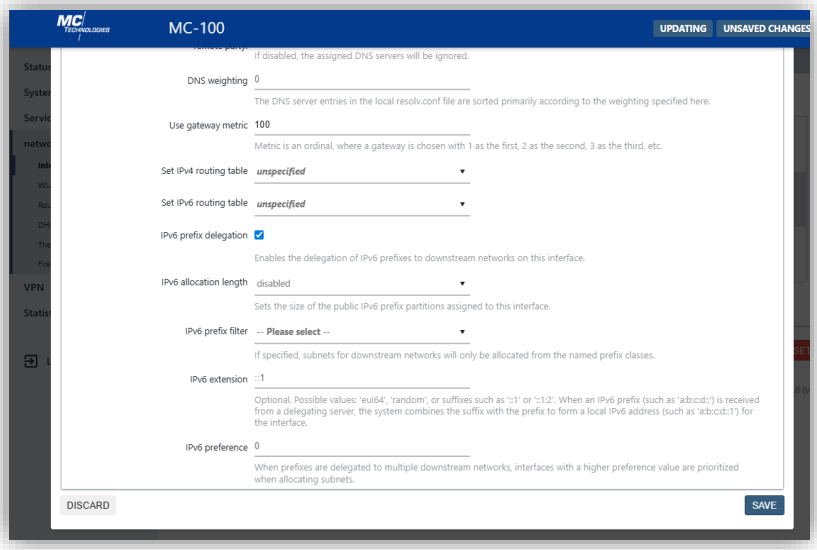
Navigieren Sie zu Netzwerk->Schnittstellen und klicken Sie auf den Lösch-Button neben der LAN-Schnittstelle. Wenden Sie die Änderungen noch nicht um.

23.1.3 Erstellung einer WAN-Schnittstelle

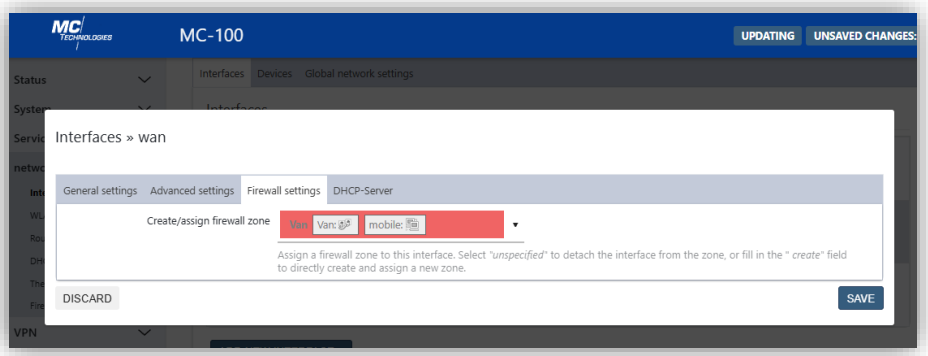
Klicken Sie auf die NEUE OBERFLÄCHE HINZUFÜGEN... Knopf. Im Dialog geben Sie wan als Namen ein, wählen Sie den DHCP-Client als Protokoll und br-lan als Gerät. Dann klicken Sie auf INTERFACE ERSTELLEN.



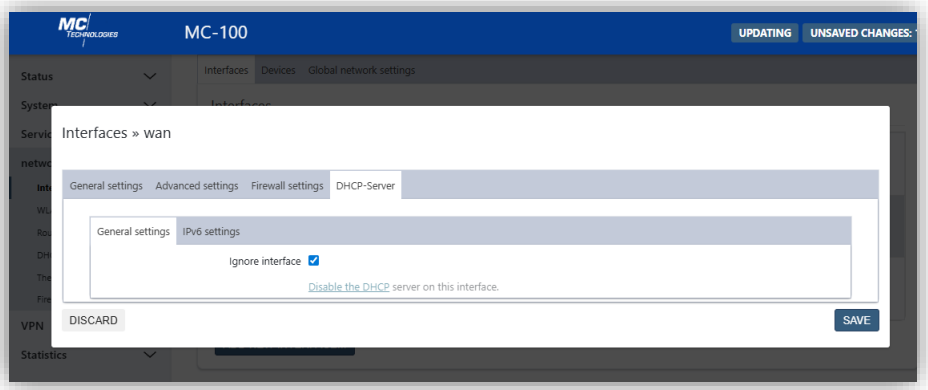
Im *Reiter Erweiterte Einstellungen* setzen Sie *die Gateway-Metrik auf* 100.



Stellen Sie sicher, dass die Schnittstelle *im Tab* Firewall-Einstellungen *zur Firewall-Zone hinzugefügt* wird.

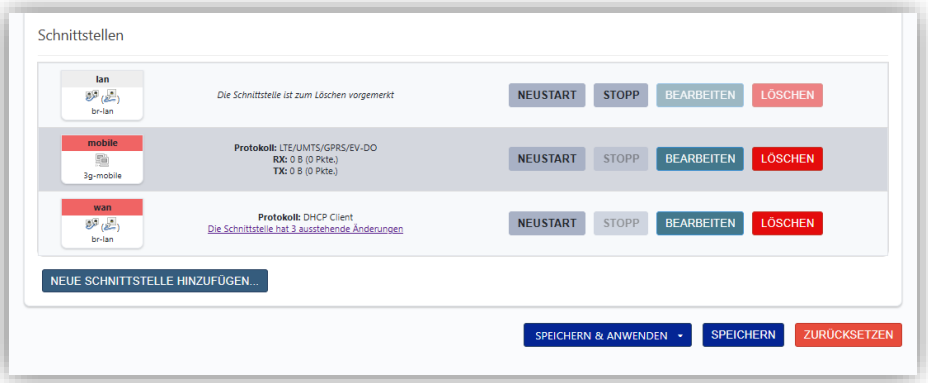


Stellen Sie außerdem sicher, dass das *Kontrollkästchen* "Schnittstelle ignorieren" im *Tab DHCP Server* angekreuzt ist .



Klicken Sie auf SPEICHERN.

Bevor Sie mit der Umsetzung der Änderungen beginnen, sollten Sie sich darauf vorbereiten, das Gateway zeitnah vom WAN-Netzwerk aus zu erreichen. Nachdem die Änderungen angewendet wurden, beginnt ein Countdown. Wenn dieser Countdown abläuft, bevor Sie vom WAN-Netzwerk aus auf die Weboberfläche zugreifen konnten, wird das Gateway die Änderungen rückgängig machen. Das ist eine Gegenmaßnahme dagegen, sich versehentlich aus dem System auszuschließen. Sobald Sie bereit sind, vom WAN-Netzwerk auf die Weboberfläche zuzugreifen, klicken Sie auf SPEICHERN & ANWENDEN.



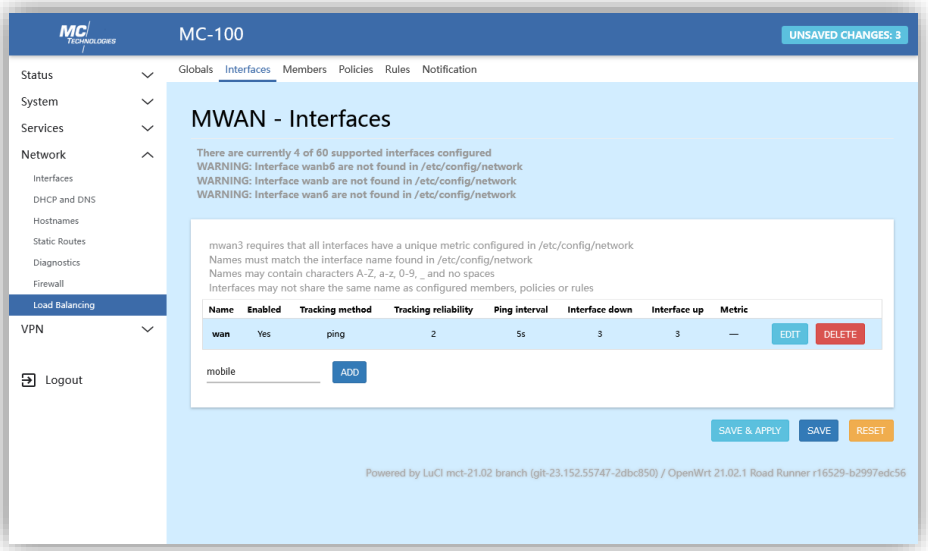
23.2 Verbindungs-Failover und Lastverteilung

Es wird dringend empfohlen, für alle Standardrouten von Schnittstellen, die mit mwan3 verwendet werden, einen Metrikwert festzulegen. Dies stellt sicher, dass die Routen mit dem niedrigsten metrischen Wert auch im Falle eines Ausfalls bevorzugt werden.

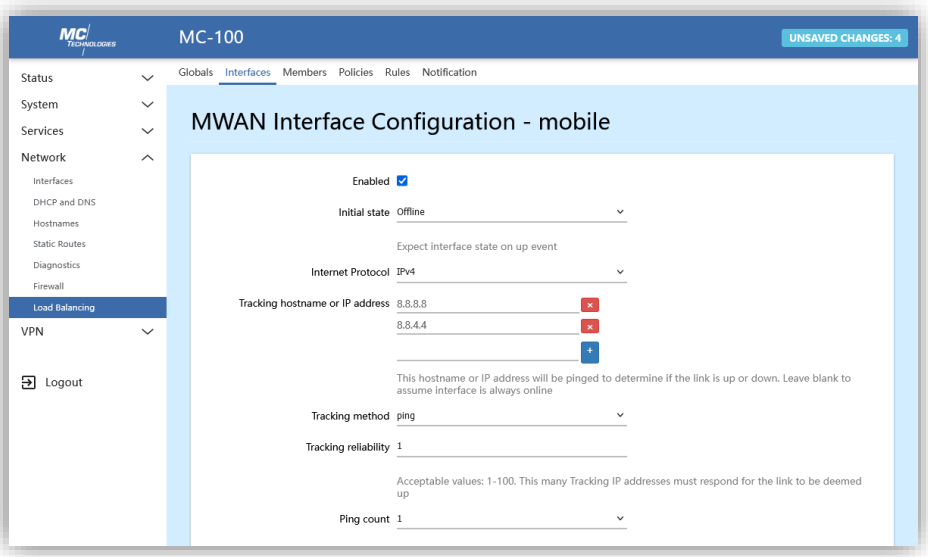
Klicken Sie auf die Schaltfläche "Bearbeiten" neben der mobilen Benutzeroberfläche. Um die mobile Schnittstelle als bevorzugte Schnittstelle zu konfigurieren, setze im Reiter Erweiterte Einstellungen die Nutz-Gateway-Metrik auf 50. Ansonsten setzen sie sie auf 200.

23.2.1 Hinzufügen der Schnittstellen zur Konnektivitätsverfolgung

Gehen Sie zu Netzwerk->Laden Balancing->Interfaces und löschen Sie alle vorkonfigurierten Schnittstellendefinitionen, indem Sie neben den Einträgen auf DELETE klicken. Gib dann den Namen der hinzuzufügenden Oberfläche (WAN oder Mobil in diesem Beispiel) in das untere linke Textfeld ein und klicke Sie auf den HINZUFÜGEN-Button daneben.



Ihnen werden viele Optionen zur Bestimmung des Verbindungsstatus der Schnittstelle präsentiert. Der Standardbefehl ist ein gewöhnlicher Ping-Befehl, der gemäß den hier angegebenen Optionen ausgeführt wird. Es ist möglich, mehrere *Tracking-Hostnamen oder IP-Adressen zu definieren.*Die Option *Tracking Reliability* definiert, wie viele dieser Adressen erfolgreich gepingt werden müssen, damit die Verbindung funktioniert. Erweiterte Einstellungen ermöglichen Verbindungsqualitätsprüfungen, indem auch der Paketverlust bewertet wird.



Google- und OpenDNS-Server (8.8.8.8, 8.8.4.4 und 208.67.222.222, 208.67.220.220) haben sich als zuverlässige Indikatoren für eine funktionierende Internetverbindung erwiesen. Doch diese Dienste sind nicht garantiert, dauerhaft verfügbar zu sein, noch bedeutet das Pingen, dass die Internetverbindung zu anderen Servern ordnungsgemäß funktioniert. Es gibt alternative Testmethoden, die im *Dropdown-Menü "Tracking-Methode*" ausgewählt werden können , wobei jede ihre eigene Auswahl an Optionen bietet. Zum Beispiel *httping* zur Überprüfung der Erreichbarkeit von HTTP(S)-Servern.

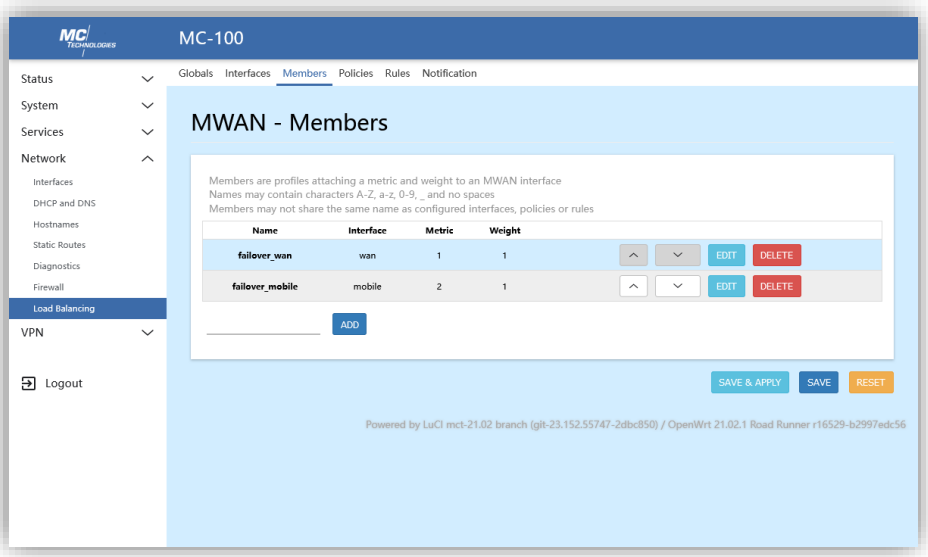
23.2.2 Gruppierungsschnittstellen mit Mitgliederprofilen

Löschen Sie alle vorkonfigurierten *Mitgliederprofile*, indem Sie auf die *DELETE-Buttons* neben den Einträgen klicken.

Um Schnittstellen später in (mehreren) *Richtlinien zu gruppieren* , müssen diese zuerst zu Mitgliederprofilen hinzugefügt werden . *Mitgliederprofile* haben im Grunde zwei Möglichkeiten:

Die *Metrik* priorisiert die Schnittstellen bei einem Failover-Fall (genau wie bei einer Routing-Metrik bedeutet ein niedrigerer Metrikwert, dass die Schnittstelle gegenüber einer mit höherem Wert bevorzugt wird). Bitte verwechseln Sie dies nicht mit der zuvor konfigurierten Standard-Routenmetrik.

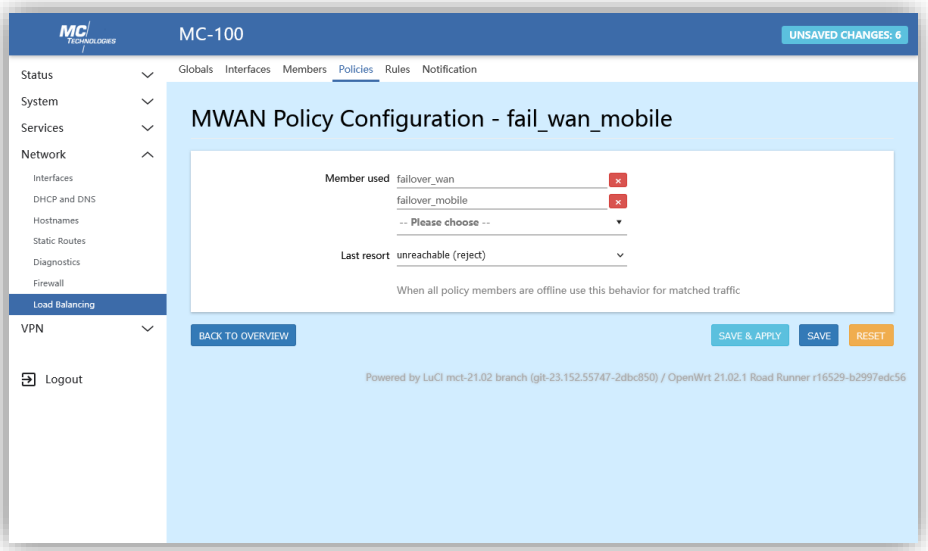
Der Weight-Wert wird verwendet, um die Lastverteilung von zwei oder mehr Schnittstellen mit demselben Metrikwert zu ermöglichen. Zum Beispiel betrachtet man eine Politik, die aus zwei Schnittstellen A und B besteht, die denselben metrischen Wert teilen, mit einem Gewichtungswert von 3 für Schnittstelle A und 2 für Schnittstelle B, bedeutet im Allgemeinen, dass 60 % (3 * 100 % / (3 + 2)) der neu instanziierten Verbindungen Schnittstelle A verwenden.



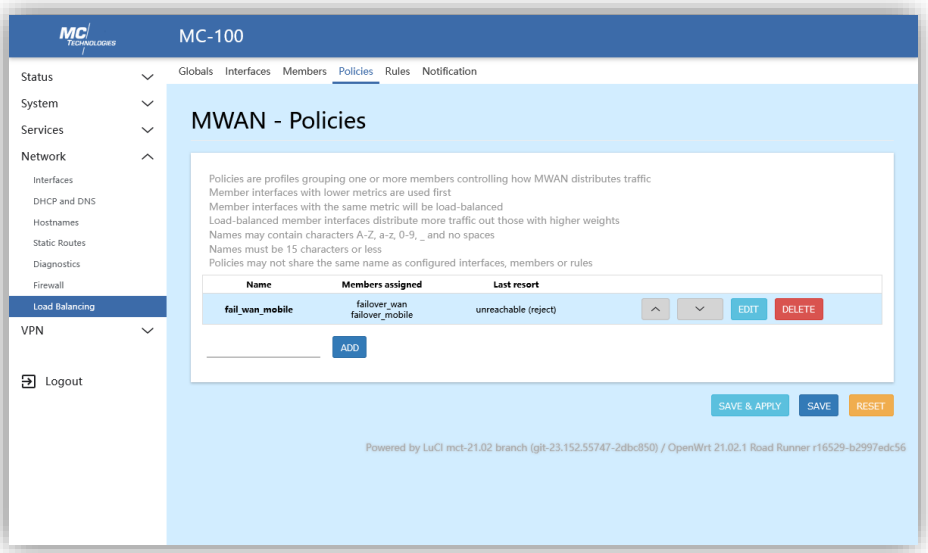
23.2.3 Richtlinien

Löschen Sie alle vorkonfigurierten *Richtlinien*, indem Sie auf die DELETE-Buttons neben den Einträgen klicken.

Richtlinien erlauben die Gruppierung von *Mitgliedern* zur Definition von Failover-, Load-Balance- oder sogar gemischten *Regeln.*



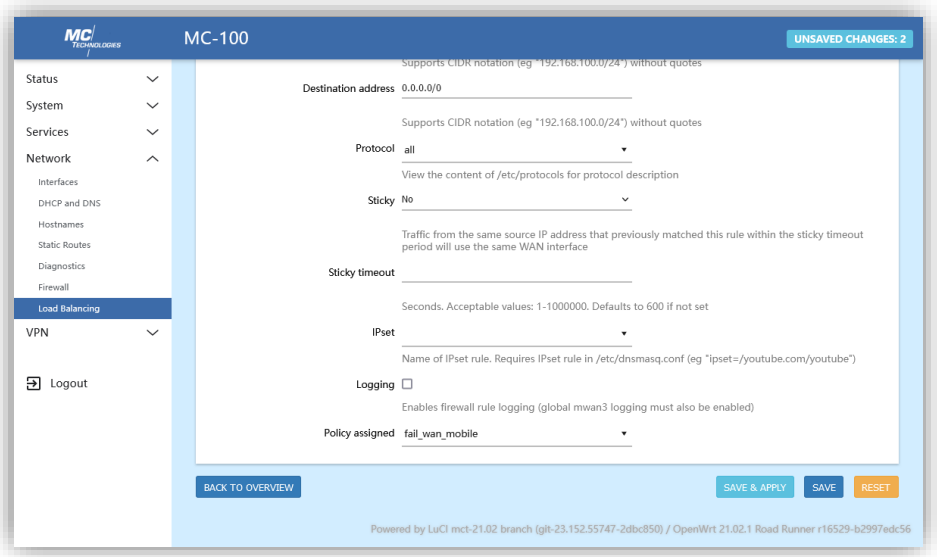
Wie bereits erwähnt, überprüft mwan3 den Konnektivitätsstatus der *Mitglieder* im ersten Durchlauf, geordnet nach ihren metrischen Werten. Wenn mehrere der funktionalen Mitglieder mit der niedrigsten Metrik dieser Richtlinie denselben Metrikwert haben, wird nur dann der Gewichtungswert für die Lastverteilung der Verbindungen berücksichtigt.



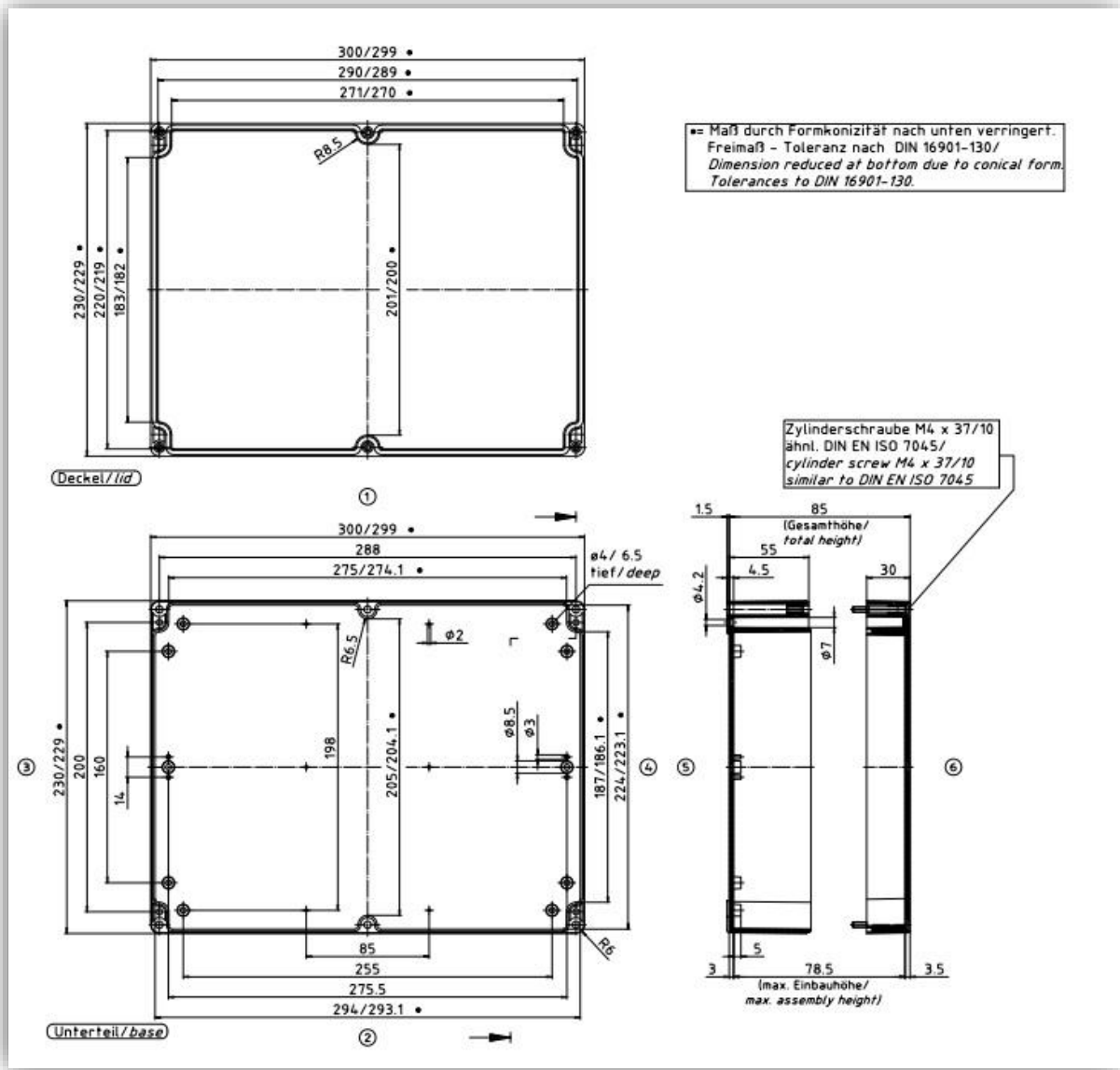
23.2.4 Regeln

Schließlich *müssen Regeln* eingerichtet werden, um die Anwendungsfälle der Richtlinien zu definieren. Löschen Sie alle vorkonfigurierten Regeldefinitionen, indem Sie neben *den Einträgen auf die* DELETE-Buttons klicken.

Regeln definieren, für welche Art von Verbindungen eine Richtlinie angewendet werden soll. Gültige Kriterien sind die IP-Protokolle, die Quell- und Zieladresse, der Portbereich und die erweiterten Lastverteilungseinstellungen. Es ist sogar möglich, ein benutzerdefiniertes *IPSet* für dynamische Setups zu definieren.



25 Abmessungen SensorBox



26 Produktpflege und -handhabung

26.1 Instandhaltung

Das Produkt ist wartungsfrei und erfordert keine spezielle regelmäßige Wartung. Das Gerät kann jedoch eine regelmäßige Inspektion erfordern (siehe Kapitel *Elektrische Sicherheitsanforderungen*).

26.2 Fehlerbehebung

Wenn während des Betriebs des Produkts ein Fehler auftritt und Sie Hilfe benötigen, wenden Sie sich bitte an den Support von MC Technologies. Sie erreichen unsere Support-Abteilung per E-Mail oder Telefon:

support@mc-technologies.com
+49-511-676 999-126

26.3 Reparatur

Nur qualifiziertes Personal bei MC Technologies GmbH ist zur Durchführung von Reparaturen befugt.

Senden Sie defekte Produkte mit einer detaillierten Fehlerbeschreibung an:

MC Technologies
-Reparatur-
Kabelkamp 2
30179 Hannover

Bevor Sie das Gerät versenden, stellen Sie sicher:

- Rufen Sie unser Support-Team an und fordern Sie eine RMA-Nummer (Return to Manufacturer Authorization) an.
- Entfernen Sie alle persönlichen Gegenstände wie eingesteckte SIM-Karten
- Sichere relevante Daten wie Konfigurationen auf dem Gerät

26.4 Entsorgung

Gemäß den WEEE-Vorschriften wird die Rückgabe und das Recycling alter MC Technologies-Geräte für unsere Kunden wie folgt geregelt:

Bitte schicken Sie Ihre alten Geräte mit bezahlter Ladung an folgende Adresse:

MC Technologies
-Entsorgung-
Kabelkamp 2
30179 Hannover