Helmholz
COMPATIBLE WITH YOU

PN/MQTT Coupler

Handbuch

Ausgabe 4 | 04.02.2022 | gültig ab Firmware V1.08

Link zur neuesten Version des Handbuchs

Helmholz GmbH & Co. KG | Hannberger Weg 2 | D-91091 Großenseebach
Phone +49 9135 7380-0 | Fax +49 9135 7380-110 | info@helmholz.de | www.helmholz.com

Hinweise

Die jeweils aktuellste Version des Handbuchs finden Sie im Internet unter www.helmholz.de.

Wir freuen uns über Verbesserungsvorschläge und Anregungen.

Helmholz GmbH & Co. KG

Hannberger Weg 2, 91091 Großenseebach

Änderungen in diesem Dokument:

Stand	Datum	Änderung
1	12.4.2021	erste Version
2	18.6.2021	Aktualisierung für Firmware V1.04; Microsoft Azure Beispiel hinzugefügt
3	26.10.2021	Abmessungen korrigiert Anpassungen Firmware V1.06 Aktualisierung Security Empfehlungen
4	4.2.2022	Anpassungen Firmware V1.08: Payload Editor Subscribing Modules Update AWS und HiveMQ Anwendungsbeispiele

Inhalt

1 Allgemeines

Diese Betriebsanleitung gilt ausschließlich für Geräte, Baugruppen, Software und Leistungen der Helmholz GmbH & Co. KG.

1.1 Aufbau des Handbuchs

Dieses Handbuch ist in 19 Abschnitte aufgeteilt.

Abschnitt 1 enthält **Allgemeine Informationen** und **Sicherheitshinweise.**

Abschnitt 2 weist auf **Security Empfehlungen** hin.

Abschnitt 3 erläutert die **Systemübersicht** und **Eigenschaften** des Produkts.

Abschnitt 4+5 erläutern die **Montage** und den elektrischen **Anschluss** des Produkts.

Die Abschnitte 6-11 erläutern die **Konfiguration** und **Programmierung** des Produkts.

Im Abschnitt 12+13 werden Funktionen zur **Wartung** und **Diagnose** des Produktes beschrieben.

Die Abschnitte 14-18 enthalten **Anwendungsbeispiele.**

Die **technischen Daten** sind im Abschnitt 19 zu finden.

1.2 Zielgruppe des Handbuchs

Diese Beschreibung wendet sich ausschließlich an ausgebildetes Fachpersonal der Steuerungs- und Automatisierungstechnik, das mit den geltenden nationalen Normen vertraut ist. Zur Installation, Inbetriebnahme und zum Betrieb der Komponenten ist die Beachtung der Hinweise und Erklärungen dieser Betriebsanleitung unbedingt notwendig.

Projektierungs-, Ausführungs- und Bedienungsfehler können den ordnungsgemäßen Betrieb des Gerätes beeinträchtigen und Personen-, Sach- oder Umweltschäden zur Folge haben. Es darf nur ausreichend qualifiziertes Fachpersonal die Geräte bedienen!

Das Fachpersonal hat sicherzustellen, dass die Anwendung bzw. der Einsatz der beschriebenen Produkte alle Sicherheitsanforderungen, einschließlich sämtlicher anwendbaren Gesetze, Vorschriften, Bestimmungen und Normen erfüllt.

1.3 Sicherheitshinweise

Die Sicherheitshinweise müssen beachtet werden um Personen und Lebewesen, materielle Güter und die Umwelt vor Schäden zu bewahren. Die Sicherheitshinweise zeigen mögliche Gefahren auf und geben Hinweise, wie Gefahrensituationen vermieden werden können.

1.4 Hinweiszeichen und Signalwörter

GEFAHR

Wenn der Gefahrenhinweis nicht beachtet wird, besteht die unmittelbare Gefahr für Gesundheit und Leben von Personen durch elektrische Spannung.

WARNUNG

Wenn der Gefahrenhinweis nicht beachtet wird, besteht die wahrscheinliche Gefahr für Gesundheit und Leben von Personen.

VORSICHT

Wenn der Gefahrenhinweis nicht beachtet wird, können Personen verletzt oder geschädigt werden.

ACHTUNG

Macht auf Fehlerquellen aufmerksam, die Geräte oder Umwelt schädigen können.

HINWEIS

Gibt einen Hinweis zum besseren Verständnis oder zur Vermeidung von Fehlern.

1.5 Bestimmungsgemäße Verwendung

Der „PN/MQTT Coupler“ ermöglich den Datenaustausch zwischen einem PROFINET-Netzwerk und MQTT-Brokern.

Die gesamten Komponenten werden mit einer werkseitigen Hard- und Software-Konfiguration ausgeliefert. Die Hard- und Software-Konfiguration auf die Anwendungsbedingungen muss durch den Anwender erfolgen. Änderungen der Hard-, oder Software-Konfiguration, die über die dokumentierten Möglichkeiten hinausgehen sind unzulässig und bewirken den Haftungsausschluss der Helmholz GmbH & Co. KG.

WARNUNG

Das PN/MQTT Coupler darf nicht als alleiniges Mittel zur Abwendung gefährlicher Zustände an Maschinen und Anlagen eingesetzt werden.

Der PN/MQTT Coupler ist nicht für eine direkte Verbindung mit dem Internet verwendbar. Verwenden Sie für eine Internetverbindung immer einen dedizierten Router mit einer ausreichend dimensionierten Internet-Firewall. Beachten Sie bei der Projektierung, Verwendung und Wartung die Empfehlungen zur Security (s. Kap. 2).

Der einwandfreie und sichere Betrieb des PN/MQTT Coupler setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus.

Die in den technischen Daten angegebenen Umgebungsbedingungen müssen eingehalten werden.

Das PN/MQTT Coupler besitzt den Schutzgrad IP 20 und muss zum Schutz vor Umwelteinflüssen in einem elektrischen Betriebsraum oder einem Schaltkasten/Schaltschrank montiert werden. Um unbefugtes Bedienen zu verhindern, müssen die Türen der Schaltkästen/Schaltschränke während des Betriebes geschlossen und ggf. gesichert sein.

1.6 Missbrauch

WARNUNG

Die Folgen einer nicht bestimmungsgemäßen Verwendung können Personenschäden des Benutzers oder Dritter sowie Sachschäden an der Steuerung, am Produkt oder Umweltschäden sein. Setzen Sie den PN/MQTT Coupler nur bestimmungsgemäß ein!

1.7 Haftung

Der Inhalt dieser Bedienungsanleitung unterliegt technischen Änderungen, die durch die ständige Weiterentwicklung der Produkte der Helmholz GmbH & Co. KG entstehen. Für den Fall, dass diese Bedienungsanleitung technische Fehler oder Schreibfehler enthält, behalten wir uns das Recht vor, Änderungen jederzeit und ohne Ankündigung durchzuführen.

Aus den Angaben, Abbildungen und Beschreibungen in dieser Dokumentation können keine Ansprüche auf Änderung bereits gelieferter Produkte gemacht werden. Über die in der Bedienungsanleitung enthaltenen Anweisungen hinaus sind in jedem Fall die gültigen nationalen und internationalen Normen und Vorschriften zu beachten.

1.7.1 Haftungsausschluss

Die Helmholz GmbH & Co. KG haftet nicht bei Schäden, wenn diese durch nicht bestimmungs- oder sachgemäße Benutzung oder Anwendung der Produkte verursacht wurden.

Die Helmholz GmbH & Co. KG übernimmt keine Haftung für eventuell in der Bedienungsanleitung enthaltene Druckfehler oder sonstige Ungenauigkeiten, es sei denn, es sind gravierende Fehler, die Helmholz GmbH & Co. KG nachweislich bereits bekannt sind.

Über die in der Bedienungsanleitung enthaltenen Anweisungen hinaus sind in jedem Fall die gültigen nationalen und internationalen Normen und Vorschriften zu beachten.

Die Helmholz GmbH & Co. KG haftet nicht bei Schäden, die durch Software, die auf Geräten des Anwenders aktiv ist und über die Fernwartungsverbindung weitere Geräte oder Prozesse beeinträchtigt, schädigt oder infiziert und unerwünschten Datentransfer auslöst oder ermöglicht.

1.7.2 Gewährleistung

Melden Sie Mängel sofort nach Feststellung des Fehlers beim Hersteller an.

Die Gewährleistung erlischt bei:

- Missachtung dieser Betriebsanleitung
- Nicht bestimmungsgemäßer Verwendung des Geräts
- Unsachgemäßem Arbeiten an und mit dem Gerät
- Bedienungsfehlern
- Eigenmächtigen Veränderungen am Gerät

Es gelten die bei Vertragsabschluss unter "Allgemeine Geschäftsbedingungen der Firma Helmholz GmbH & Co. KG" getroffenen Vereinbarungen.

1.8 Open Source

Unsere Produkte enthalten unter anderem Open Source Software. Diese Software unterliegt den jeweils einschlägigen Lizenzbedingungen. Die entsprechenden Lizenzbedingungen einschließlich einer Kopie des vollständigen Lizenztextes sind auf der Produkt-Webseite herunterladbar. Sie werden auch in unserem Downloadbereich der jeweiligen Produkte unter www.helmholz.de bereit gestellt.

Weiter bieten wir Ihnen an, den vollständigen, korrespondierenden Quelltext der jeweiligen Open Source Software gegen einen Unkostenbeitrag von Euro 10,00 als DVD auf Ihre Anfrage hin Ihnen und jedem Dritten zu übersenden. Dieses Angebot gilt für den Zeitraum von drei Jahren, gerechnet ab der Lieferung des Produktes.

2 Security Empfehlungen

Der PN/MQTT-Coupler ist eine Netzwerkinfrastruktur Komponente und damit ein wichtiges Element in der Security Betrachtung einer Anlage oder eines Netzwerkes. Beachten Sie bei der Verwendung des PN/MQTT-Coupler deshalb folgende Empfehlungen, um nicht autorisierte Zugriffe auf Anlagen und Systeme zu unterbinden.

Allgemein:

- Stellen Sie in regelmäßigen Abständen sicher, dass alle relevanten Komponenten diese Empfehlungen und ggf. weitere interne Sicherheits-Richtlinien erfüllen.
- Bewerten Sie Ihre Anlage ganzheitlich im Hinblick auf die Sicherheit. Nutzen Sie ein Zellen-schutzkonzept („Defense-in-Depth“) mit entsprechenden Produkten, wie z.B. dem WALL IE.
- Informieren Sie sich regelmäßig über Security Bedrohungen für alle ihre Komponenten

Physischer Zugang:

- Beschränken Sie den physischen Zugang zu sicherheitsrelevanten Komponenten auf qualifiziertes Personal.

Sicherheit der Software:

- Halten Sie die Firmware alle Kommunikationskomponenten immer aktuell.
- Informieren Sie sich regelmäßig über Firmware Updates für das Produkt.
- Aktivieren Sie nur Protokolle und Funktionen, die Sie wirklich benötigen.
- Verwenden Sie nach Möglichkeit stets diejenigen Varianten von Protokollen, die mehr Sicherheit bieten.

Passwörter:

- Definieren Sie Regeln und Rollen für die Nutzung der Geräte und die Vergabe von Passwörtern.
- Ändern Sie Standard-Passwörter.
- Verwenden Sie ausschließlich Passwörter mit hoher Passwortstärke. Vermeiden Sie schwache Passwörter wie z. B. "passwort1", "123456789" oder dergleichen.
- Stellen Sie sicher, dass alle Passwörter unzugänglich für unbefugtes Personal sind.
- Verwenden Sie dasselbe Passwort nicht für verschiedene Benutzer und Systeme.

Helmholz ist Mitglied beim **CERT@VDE**. Wir kommunizieren – neben unserem technischen Newsletter - unsere Security relevanten Updates, Patches und Handlungshinweise (Advisories) an Sie als Anwender der Helmholz Produkte. Informieren Sie sich und nutzen Sie die Dienste und die Datenbank des **CERT@VDE** um Ihre Anlagen sicher zu machen und sicher zu halten.

Das Helmholz **„Product Security Incident Response Team“ (PSIRT)** unterstützt Sie proaktiv, um Ihre Maschinen im Rahmen der industriellen Kommunikation bestmöglich zu schützen. Wann immer neue Gefährdungspotentiale auftreten oder uns gemeldet werden, bewerten und bearbeiten wir diese umgehend und versorgen Sie schnellstmöglich mit Handlungsempfehlungen, Patches und Updates, um das Risiko auf ein Minimum zu reduzieren.

Auch Sie können helfen: **Melden Sie Auffälligkeiten** zum Produkt an unser „Product Security Incident Response“ Team unter psirt@helmholz.de oder support@helmholz.de.

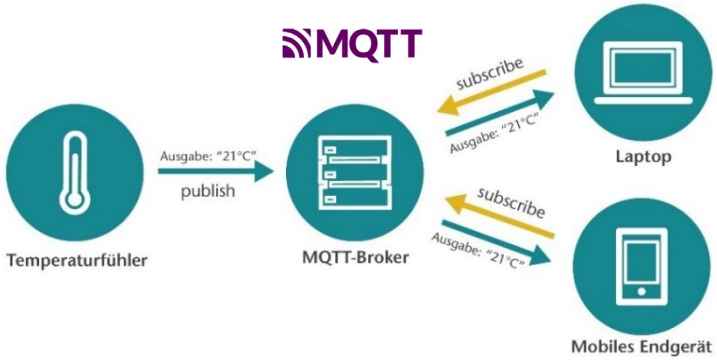
Weitere Informationen zur Thema Security erhalten Sie z.B. hier:

- CERT@VDE
- Sichere-industrie.de
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Allianz für Cyber-Sicherheit

3 Systemübersicht

3.1 Allgemein/Einsatzgebiet

Das MQTT-Protokoll hat sich in den letzten Jahren als einfaches Übertragungsprotokoll für Nachrichten in der IoT-Welt durchgesetzt. MQTT steht für „Message Queue Telemetry Transport Protocol“ und ist ein OASIS-Standard. Informationen zum MQTT-Protokoll sind hier zu finden: mqtt.org



Das MQTT-Protokoll nutzt zur Kommunikation zwischen Geräten immer einen zentralen Broker, der Nachrichten von z.B. einem Sensor empfängt und an interessierte Geräte, z.B. einer Steuereinheit, weiterleitet.

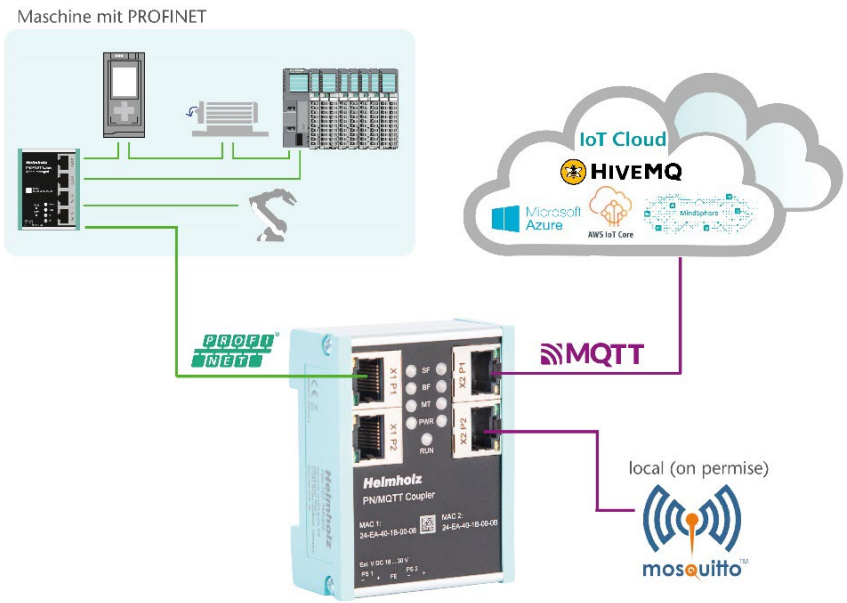
Wenn ein Sensor Daten an den Broker sendet, so nennt man das „Publish“. Benötigt ein Gerät Daten, so muss es diese beim Broker abonnieren („Subscribe“). Der Broker liefert die Daten an alle Subscriber aus, wenn vom Publisher neue Daten eingetroffen sind.

Daten werden immer unter einer frei festlegbaren Kennung - dem „Topic“ - übertragen. Das „Topic“ ist ein beschreibender Text, z.B. „Temperatur“. Um verschiedene gleichartige Topics unterscheiden zu können, werden Gruppierungen verwendet, z.B. „Wohnzimmer/Temperatur“.

Die Gruppierungen werden durch einen Trennstrich aufgeteilt (‚/‘). Somit können die Daten auch in komplexere Strukturen abgebildet werden: „Obergeschoss/Wohnzimmer/Temperatur“ oder „Obergeschoss/Wohnzimmer/Luftfeuchte“.

Die über MQTT gelieferten Daten können im Binärformat, im Textformat oder strukturiert im JSON Format übertragen werden.

Mit dem PN/MQTT Coupler ist eine Übertragung von Werten zwischen einer PROFINET-Maschine (SPS) und einem MQTT-Broker möglich. Es ist sowohl möglich Werte von der SPS über PROFINET an einen Broker zu versenden („Publish“) als auch Werte von einem MQTT-Broker zu abonnieren und in der SPS über PROFINET zu empfangen („Subscribe“).



Die Einbindung in das SPS Engineering-Tool wird durch eine GSDML-Datei ermöglicht, eine extra Konfigurationssoftware ist nicht nötig. Die Konfiguration der auszutauschenden EA-Daten wird im Siemens Engineering-Tool durchgeführt. Alle Einstellungen zur MQTT-Verbindung können auf der Webseite des Gerätes durchgeführt werden.

MQTT-Broker können sowohl lokal angebunden werden („On premise“) als auch über das Internet („Cloud“). Ein lokaler Broker kann z.B. mit der Open-Source Software „Mosquitto“ im Firmennetzwerk auf einem PC/Server oder auch auf einem Kleincomputer, wie z.B. einem Raspberry PI, betrieben werden.

HINWEIS Der PN/MQTT-Coupler kann nur mit einem Broker eine Verbindung aufbauen! Sollen die Daten auch an andere Broker verteilt werden, so muss die Verbindung zwischen den Brokern hergestellt werden (Multi Broker).

In der Cloud können IoT Systeme, wie z.B. HiveMQ, Amazon IoT, Microsoft Azure oder Siemens Mindsphere *(in Vorbereitung)* direkt angebunden werden. Eine Beschreibung für die Anbindung an die verschiedenen Cloudsysteme finden Sie weiter unten in diesem Handbuch oder fragen Sie den Support.

3.2 Eigenschaften des PN/MQTT Coupler

Der „PN/MQTT Coupler“ hat folgende Eigenschaften:

- PROFINET IO Device nach IEC 61158-6-10
- Bis zu 1024 Byte Eingangs- und Ausgangsdaten
- Unterstützt die OASIS MQTT-Standards V3.1.1 und V5
- Einfache Zuordnung der IO-Daten mittels GSDML-Datei
- Bis zu 100 Werte können gleichzeitig zur Übertragung konfiguriert werden (100 Slots)
- Flexible Konfiguration über Webbrowser
- Getrennte Netzwerke für PROFINET und MQTT-Verbindung
- Anbindung an Broker im lokalen Netzwerk oder direkt mit der "Cloud"
- Authentifizierung (Passwort, Zertifikat) und Verschlüsselung (TLS)
- Unterstützt AWS IoT, Microsoft Azure, HiveMQ, IBM Watson, Google IoT, Siemens Mindsphere *(in Vorbereitung)*
- Sehr kompakte Bauform zur Hutschienenmontage
- Redundante Stromversorgung
- Galvanische Trennung der Netzwerke

4 Montage und Demontage

4.1 Zugangsbeschränkung

Das Gerät ist ein offenes Betriebsmittel und darf nur in elektrischen Betriebsräumen, Schränken oder Gehäusen installiert werden.

Der Zugang zu den elektrischen Betriebsräumen, Schränken oder Gehäusen darf nur über Werkzeug oder Schlüssel möglich sein und nur unterwiesenem oder zugelassenem Personal gestattet werden.

4.2 Montage und Mindestabstände

Der PN/MQTT Coupler kann auf eine DIN-Hutschiene montiert werden und kann in beliebiger Lage eingebaut werden. Zum Stecken der Busleitungen muss die Frontplatte zugänglich sein. Es wird empfohlen, bei der Montage Mindestabstände einzuhalten. Durch die Einhaltung der Mindestabstände

- ist das Montieren bzw. Demontieren der Module möglich, ohne andere Anlagenteile demontieren zu müssen.
- ist genügend Raum vorhanden, um alle vorhandenen Anschlüsse und Kontaktierungsmöglichkeiten mit handelsüblichem Zubehör zu verbinden.
- ist Platz für evtl. nötige Kabelführungen vorhanden.

ACHTUNG

Die Montage ist gemäß VDE 0100/IEC 364 und nach geltenden nationalen Normen durchzuführen. Der PN/MQTT Coupler besitzt den Schutzgrad IP20. Wird ein höherer Schutzgrad benötigt, muss der Einbau in ein Gehäuse oder einen Schaltschrank erfolgen.

4.3 Elektrische Installation

Die regional gültigen Sicherheitsbestimmungen sind zu beachten.

4.4 Schutz vor elektrostatischen Entladungen

Um Schäden durch elektrostatische Entladungen zu verhindern sind bei Montage- und Servicearbeiten folgende Sicherheitsmaßnahmen zu befolgen:

- Bauteile und Baugruppen nie direkt auf Kunststoff-Gegenstände (z.B. Styropor, PE-Folie) legen und auch deren Nähe meiden.
- Vor Beginn der Arbeit das geerdete Gehäuse anfassen, um sich zu entladen.
- Nur mit entladenem Werkzeug arbeiten.
- Bauteile und Baugruppen nicht an Kontakten berühren.

4.5 EMV-Schutz

Um die elektromagnetische Verträglichkeit (EMV) in Ihren Schaltschränken und in elektrisch rauer Umgebung sicherzustellen, sind bei der Montage und dem Anschluss die bekannten Regeln des EMV-gerechten Aufbaus zu beachten.

ACHTUNG

Beachten Sie beim Aufbau der Anlage und bei der Verlegung der notwendigen Leitungen alle Normen, Vorschriften und Regeln bezüglich der Abschirmung. Halten Sie die entsprechenden Schriften der PROFIBUS-Nutzerorganisation zum Aufbau von PROFINET genau ein. Arbeiten Sie fachgerecht!
Fehler in der Abschirmung können zu Funktionsstörungen bis hin zum Ausfall der Anlage führen.

4.6 Betrieb

Betreiben Sie den PN/MQTT Coupler nur im einwandfreien Zustand. Die zulässigen Einsatzbedingungen und Leistungsgrenzen müssen eingehalten werden.

Nachrüstungen, Veränderungen oder Umbauten am Gerät sind grundsätzlich verboten.

Der PN/MQTT Coupler ist ein Betriebsmittel zum Einsatz in industriellen Anlagen. Während des Betriebs müssen alle Abdeckungen am Gerät und der Installation geschlossen sein, um den Berührungsschutz zu gewährleisten.

ACHTUNG

Bei der Abschaltung des PN/MQTT Coupler werden Busverbindungen unterbrochen! Stellen Sie vor Beginn jeglicher Arbeiten am PN/MQTT Coupler sicher, dass bei Unterbrechung der Busverbindungen keine unzulässigen Störungen an angeschlossenen Anlagen auftreten.

4.7 Recycling / WEEE

Das Unternehmen Helmholz GmbH & Co. KG ist als Hersteller mit der Marke HELMHOLZ und der Geräteart „Kleine Geräte der Informations- und Telekommunikationstechnik für die ausschließliche Nutzung in anderen als privaten Haushalten“ sowie den folgenden Registrierungsdaten registriert:

Firma Helmholz GmbH &Co. KG,
Ort der Niederlassung/Sitz 91091 Großenseebach,
Anschrift Hannberger Weg 2,
Name des Vertretungsberechtigten: Carsten Bokholt,

Registrierungsnummer **DE 44315750**

Die in diesem Dokument beschriebenen Elektrogeräte sind dem Recycling zuzuführen. Sie dürfen gemäß Richtlinie 2012/19/EU über Elektro- und Elektronik-Altgeräte (WEEE) nicht über kommunale Entsorgungsbetriebe entsorgt werden.

5 Anschluss und Verdrahtung

5.1 Spannungsversorgung

Der PN/MQTT Coupler muss, am Weitbereichseingang DC 18 ... 30 V über den mitgelieferten Anschlussstecker, mit DC 24 V versorgt werden. Die Spannungsversorgung ist redundant ausgelegt, es muss mindestens ein Versorgungspfad PS 1 oder PS 2 angeschlossen werden.

HINWEIS

Das Gehäuse des PN/MQTT Coupler ist nicht geerdet. Bitte verbinden Sie den Funktionserdungs-Anschluss (FE) des PN/MQTT Coupler ordnungsgemäß mit dem Bezugsportal.

5.2 Netzwerk (PROFINET und Ethernet)

Die linken RJ45 Buchsen „X1 P1“ und „X1 P2“ dienen zum Anschluss des PROFINET Netzwerks, die rechten RJ45 Buchsen „X2 P1“ und „X2 P2“ dienen zum Anschluss des Ethernet-Netzwerks, in dem der MQTT-Broker erreichbar ist. Die Ports X1 P1 und X1 P2, sowie X2 P1 und X2 P2 sind intern jeweils mit einem Switch verbunden.

Die Schnittstellen X1 und X2 sind logisch getrennte Netzwerke und nicht physikalisch verbunden. Somit ist eine klare Trennung zwischen den Maschinendaten (PROFINET) und der MQTT-Datenverbindung (Ethernet) möglich. Ein Netzwerkdurchgriff mit anderen Funktionen durch den PN/MQTT Koppler ist nicht möglich.

Die konfigurierten Werte werden im PN/MQTT-Coupler nur als IO-Daten zwischen beiden Netzwerkseiten ausgetauscht.

X1: PROFINET-Stack	Internal Memory	X2: MQTT Client
Outputs	→	Publish
Inputs	←	Subscribe

HINWEIS

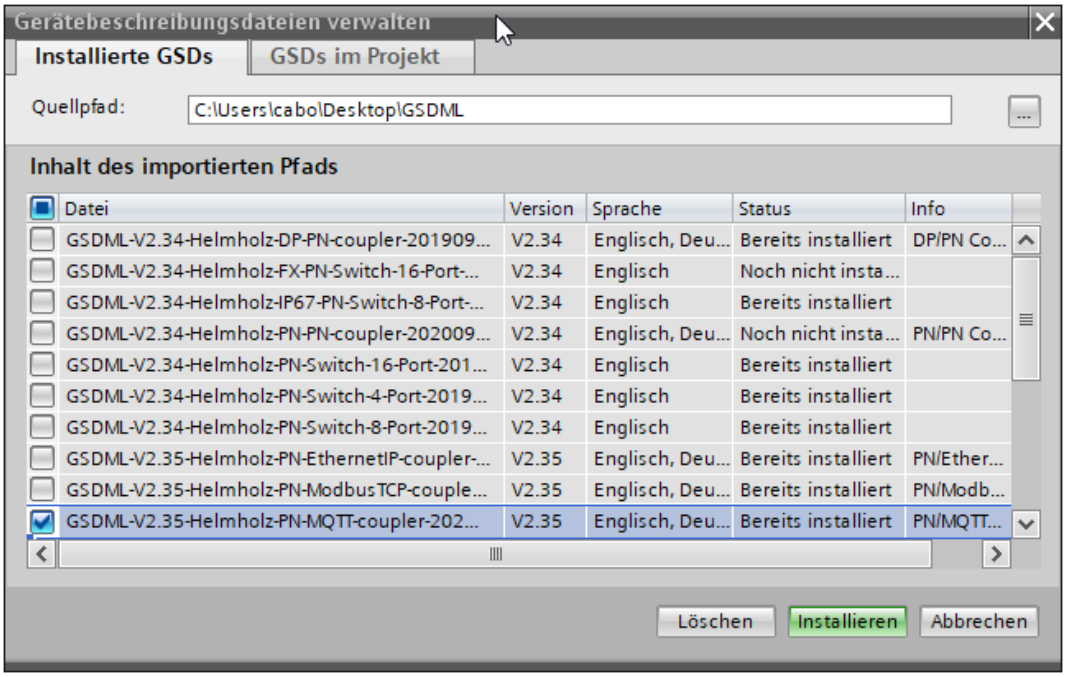
Sollte sich der MQTT-Broker im gleichen Netzwerk (Subnetz) wie die PROFINET-SPS befinden, so kann das Netzwerk X2 mit der gleichen Subnetzmaske wie das Netzwerk X1 konfiguriert werden. Die Schnittstelle X2 benötigt dann eine eigene IP-Adresse in dem Subnetz und muss mit dem Netzwerk X1 mit einem Ethernet-Kabel verbunden sein.

5.3 Netzwerkanschluss

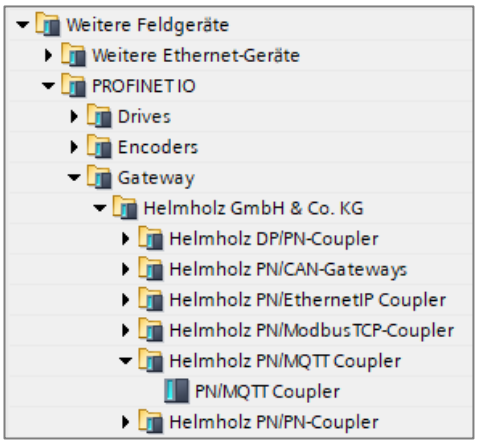
Pin	Signal	RJ45-Stecker	Farbe	Adernpaar
1	TD+	Transmission Data +	Gelb	1
2	TD-	Transmission Data -	Orange	1
3	RD+	Receive Data +	Weiß	2
4	-	-	-	-
5	-	-	-	-
6	RD-	Receive Data -	Blau	2
7	-	-	-	-
8	-	-	-	-

6 GSDML-Datei installieren

Bitte laden Sie die GSDML-Datei („GSDML-V2.35-Helmholz-PN-MQTT-coupler-_____.xml“) unter www.helmholz.de herunter oder scannen Sie den QR-Code. Installieren Sie die GSDML-Datei im TIA-Portal dem Menü „Extras“ / „Geräte-beschreibungsdatei (GSD) verwalten“.

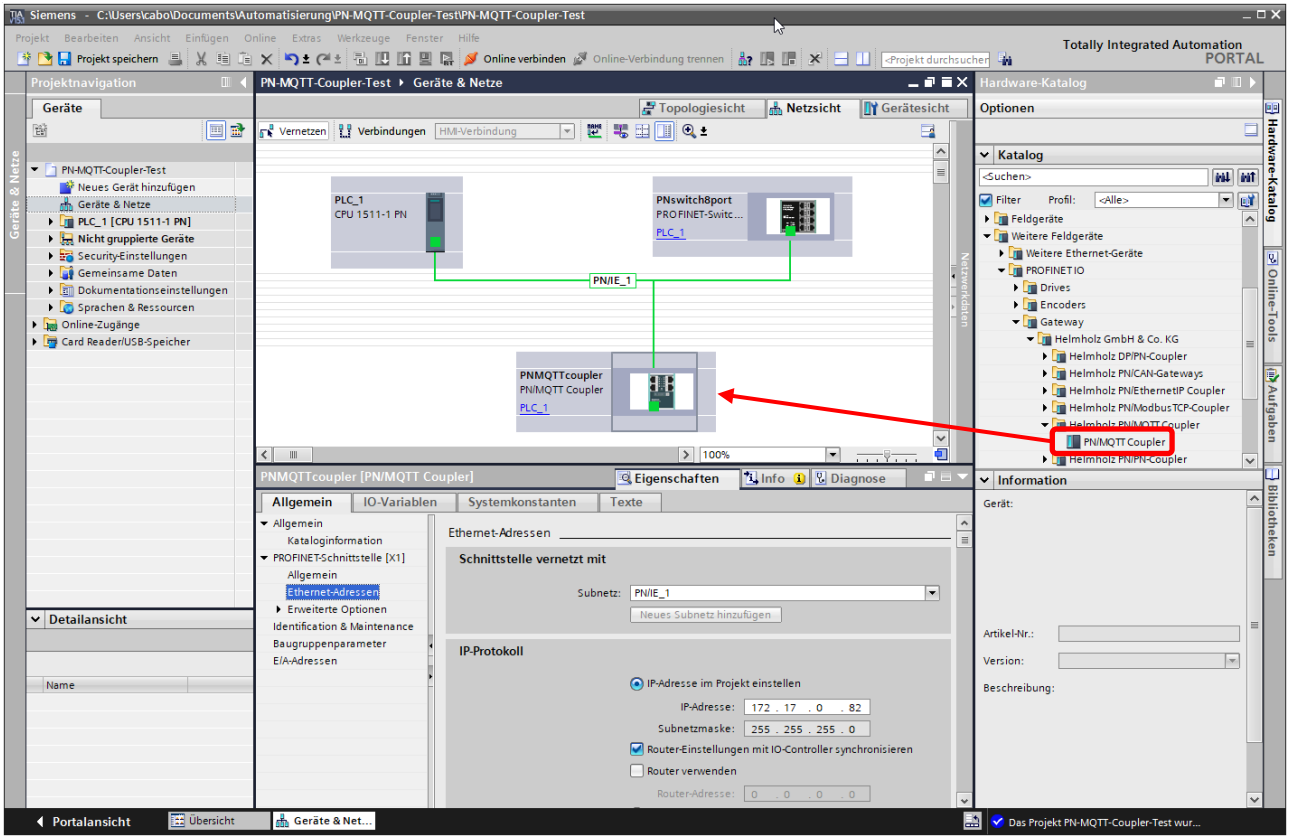


Der PN/MQTT Coupler ist im Hardwarekatalog unter „Weitere Feldgeräte / PROFINET IO / Gateway / Helmholz GmbH & Co. KG“ zu finden.



7 Konfiguration im TIA-Portal

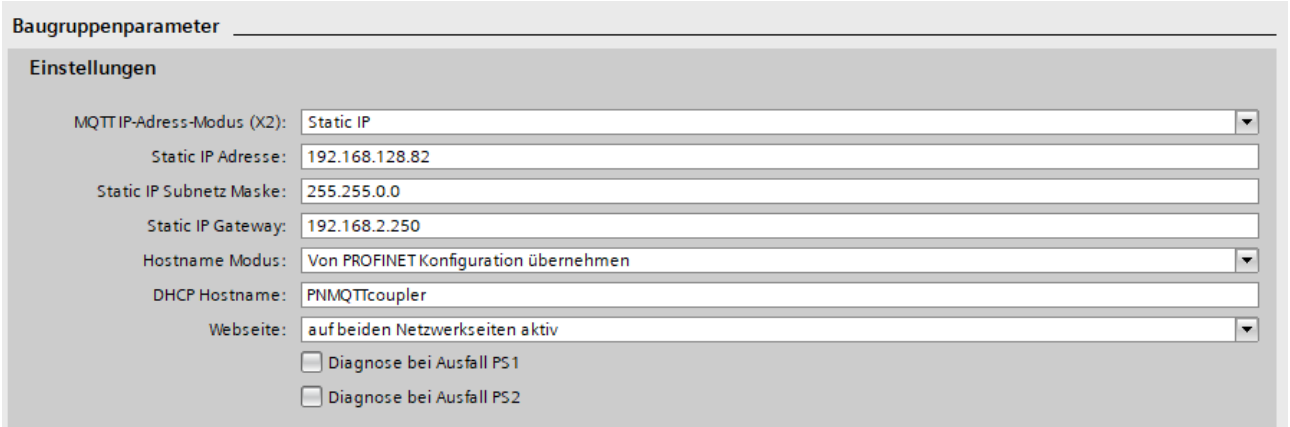
Fügen Sie den PN/MQTT Coupler in das Projekt ein und verbinden Sie den Coupler mit dem PROFINET-Netzwerk.



Vergeben Sie einen Gerätenamen und prüfen Sie die Ethernet-Adresse für das Gerät.

7.1 Parameter des PN/MQTT Coupler

Die Parametrierung des PN/MQTT Coupler wird über den PROFINET Hardware-Konfigurator (z.B. TIA Portal) durchgeführt. Hierbei werden die PROFINET-Parameter und die per MQTT zu übertragenen EA-Daten festgelegt. Die Konfiguration der MQTT-Netzwerkverbindung (Verbindung zum MQTT-Broker) wird dagegen ausschließlich über die Webseite des Gerätes eingestellt.



MQTT IP-Adress-Modus (X2): Festlegung der IP-Adresse für das Netzwerk X2. Mögliche Optionen:

„DHCP“ = Der PN/MQTT Coupler versucht im Netzwerk über einen DHCP-Server eine IP-Adresse sowie ein Gateway und einen DNS-Server zu erhalten.

„Static IP“ = Die Adresse, Subnetzmaske und date Gateway können direkt in den folgenden Feldern fest vorgegeben werden; die Einstellung eines DNS-Server kann – bei Bedarf – zusätzlich auf der Webseite durchgeführt werden.

„IP-Adresse von der Webpage“ = Die IP-Einstellungen des X2-Netzwerks kann über die Webseite durchgeführt werden. Bei der ersten Inbetriebnahme ist der PN/MQTT Coupler nur im Netzwerk X1 (PROFINET) erreichbar. Erst wenn, die IP-Einstellungen für das X2-Netzwerk dort eingestellt wurden, ist der Coupler auch über X2 erreichbar bzw. kann eine Verbindung zum MQTT-Broker aufbauen.

Static IP-Adresse: Wenn der Adress-Modus auf „Static IP“ eingestellt wurde, kann hier die statische IP-Adresse des X2 Netzwerks angegeben werden. Bei „DHCP“ und „IP-Adresse von der Webpage“ hat diese Einstellung keine Funktion.

Static IP-Subnetzmaske: Wenn der Adress-Modus auf „Static IP“ eingestellt wurde, kann hier die Subnetzmaske des X2 Netzwerks angegeben werden. Bei „DHCP“ und „IP-Adresse von der Webpage“ hat diese Einstellung keine Funktion.

Static IP Gateway: Wenn der Adress-Modus auf „Static IP“ eingestellt wurde, kann hier das Gateway des X2 Netzwerks angegeben werden. Bei „DHCP“ und „IP-Adresse von der Webpage“ hat diese Einstellung keine Funktion.

Hostname Modus: „Von der PROFINET Konfiguration übernehmen“ oder „von der Webpage übernehmen“

DHCP-Hostname: Hostname des Gerätes, wird verwendet, wenn die „Hostname Modus“ Option „Von der PROFINET Konfiguration übernehmen“ gewählt wurde.

Webseite: Auf welchen Netzwerkinterfaces soll die Webseite angezeigt werden.

HINWEIS Bitte beachten Sie in der Inbetriebnahmephase in der PROFINET-Konfiguration zumindest die Webseite auf der PROFINET-Netzwerkseite (X1) oder „beide Netzwerkseiten“ zu aktivieren. Ansonsten ist eine vollständige Konfiguration nicht möglich.
Aus Sicherheitsgründen ist es empfehlenswert nach der Inbetriebnahme die Webseiten in der PROFINET-Konfiguration abzuschalten oder zumindest das Webinterface auf der Netzwerkseite abzuschalten, welche mit dem WAN bzw. mit dem Internet verbunden ist.

7.2 Funktionsprinzip des PN/MQTT-Coupler

Der Datenaustausch zwischen der SPS und dem MQTT Broker wird über einzelne Werte organisiert. Ein Wert kann 1, 2 oder 4 Byte groß sein und liegt im EA-Bereich des PROFINET-Controllers. Je nach Datenaustauchrichtung ist der Wert als Ausgänge beschreibbar (MQTT Publish) oder als Eingänge lesbar (MQTT Subscribe).

Es können bis zu 100 verschiedene Werte zwischen dem PROFINET-Controller und dem MQTT-Broker ausgetauscht werden (100 Steckplätze). Die Werte können als Module in die Steckplätze des Couplers nach Bedarf gesteckt werden.

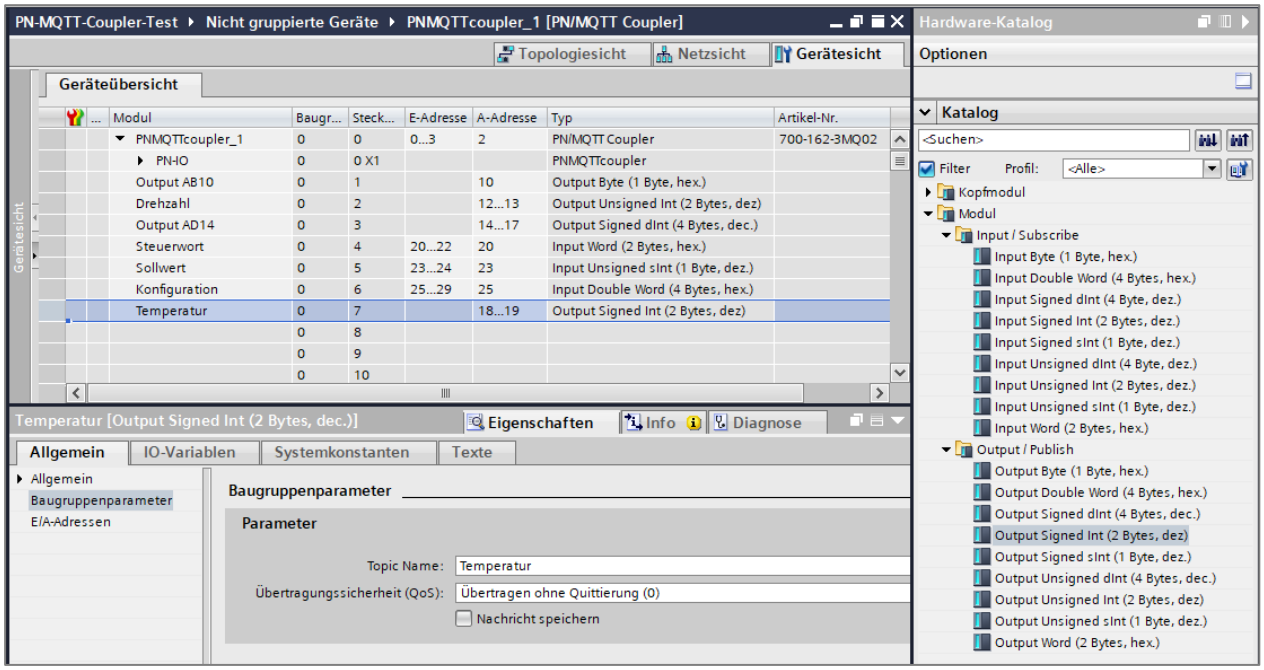
Ein Modul repräsentiert immer genau einen Wert, der über ein MQTT-Topic Namen mit dem Broker ausgetauscht wird. Ein Wert wird über MQTT üblicherweise in einer lesbaren Form gesendet (direkter Text oder JSON formatiert). Aus diesem Grund gibt es für jede Wertgröße (1, 2, 4, 8 Bytes) unterschiedliche Darstellungsformen: hexadezimal, dezimal ohne Vorzeichen, dezimal mit Vorzeichen oder Fließkomma.

Konfigurationsbeispiel:

Slot	Modul	EA	Typ	Richtung	Topic name (Beispiel)	Value (Beispiel)
1	Output Byte (1 Byte, hex.)	1 Byte Ausgang	Byte	Publish →	"Output AB10"	"0x12"
2	Output Unsigned Int (2 Bytes, dez.)	2 Bytes Ausgänge	Unsigned Integer	Publish →	"Drehzahl"	"65534"
3	Output Signed dInt (4 Bytes, dez.)	4 Bytes Ausgänge	Signed double Integer	Publish →	"Output AD14"	"-12345678"
4	Input Word (2 Bytes, hex.)	2 Bytes Eingänge	Word	← Subscribe	„Steuerwort"	„0xFFEE"
5	Input Unsigned sInt (1 Bytes, dez.)	1 Byte Eingänge	Unsigned short Int	← Subscribe	„Sollwert"	„255"
6	Input Double Word (4 Byte, hex.)	4 Bytes Eingänge	Double Word	← Subscribe	„Konfiguration"	„0x11223344"
7	Output Signed Int (2 Byte, dez.)	2 Bytes Ausgänge	Signed Integer	Publish →	„Temperatur"	„25"
...						

Output Module werden einmalig nach Neustart des Kopplers und dann nach jeder Veränderung des SPS-Wertes an den Broker gesendet. Sollten SPS-Werte versendet werden, die sich sehr schnell verändern ist es möglich auf der Konfigurationswebseite ein Sende-Intervall („publish interval") vorzugeben.

Der Wert der Input Module wird nach (Neu-)Start des Kopplers mit 0 initialisiert und bei Empfang eines neuen Wertes über MQTT dauerhaft in den Eingangsbereich übernommen. Ein Bit zeigt den Empfang eines Wertes in der SPS zusätzlich an.



Bei jedem Modul muss in den Baugruppenparametern der **Name des Topics** eindeutig festgelegt werden. Der Name kann z.B. passend zum symbolischen Namen des SPS-Wertes gewählt werden. Es stehen bis zu 40 Zeichen zur Verfügung.

Als weiterer Parameter kann die Methode der **Übertragungssicherheit (QoS)** des Topics festgelegt werden.

Übertragen ohne Quittierung (0): Das Topic wird gesendet ohne eine Quittierung vom Broker („fire-and-forget“)

Übertragen mit Quittierung (1): Das Topic wird gesendet und es wird eine Quittierung („PUBACK“) vom Broker erwartet. Sollte keine Quittierung kommen so wird das Topic nochmals versendet.

Übertragen mit abgesicherter Quittierung (2): Bietet die Garantie, dass eine Nachricht "exakt einmal geliefert" wurde. Um diese Garantie einhalten zu können, verwendet MQTT eine zweistufige Empfangsbestätigung.

Nachricht speichern: Diese Option teilt dem Broker mit, dass die letzte Nachricht bzw. der letzte Wert im Broker gespeichert werden soll, auch wenn die Verbindung zum MQTT-Client ausfällt.

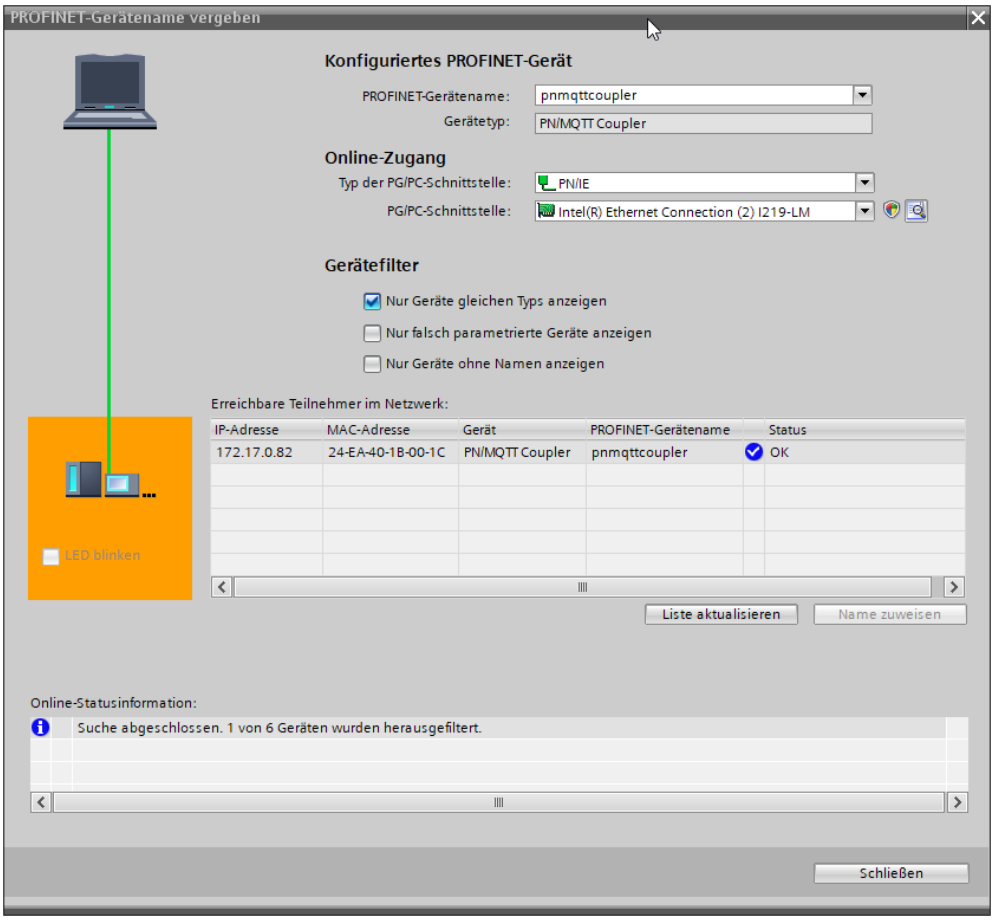
HINWEIS Das Format der Payload (Wertedarstellung) der MQTT Nachrichten ist im Kapitel 8.3 erläutert.

7.3 Dem PN/MQTT Coupler einen Namen zuweisen

Wenn die Konfiguration des PN/MQTT Coupler im Hardwarekonfigurator des Engineering-Tools abgeschlossen ist, kann diese in die SPS eingespielt werden.

Damit der PN/MQTT Coupler vom PROFINET-Controller gefunden werden kann, muss der PROFINET-Gerätename dem PN/MQTT Coupler zugewiesen werden. Dafür verwenden Sie die Funktion „Gerätename zuweisen“ welche Sie mit der rechten Maustaste oder im Menü Online erreichen können, wenn der PN/MQTT Coupler angewählt ist.

Mit dem Button „Liste aktualisieren“ kann das Netzwerk nach PROFINET-Teilnehmern durchsucht werden. Mit „Name zuweisen“ kann der PROFINET-Gerätename dem Gerät zugewiesen werden.



Die eindeutige Identifikation des PN/MQTT Coupler im PROFINET-Netzwerk wird hier durch die MAC-Adresse des Gerätes gewährleistet. Die PROFINET MAC-Adresse ist auf der Gerätefront des PN/MQTT Coupler auf der linken Seite bei X1 („MAC 1“) ablesbar.

Hat der PN/MQTT Coupler den richtigen PROFINET-Namen erhalten, dann wird er durch die SPS erkannt und konfiguriert. Ist die Konfiguration korrekt verlaufen, sollte die PROFINET „BF“-LED aus sein.

Zum Setzen des PROFINET-Namens kann auch das Helmholz IPSet Tool verwendet werden, welches kostenfrei von der Helmholz Webseite heruntergeladen werden kann (oder scannen Sie den nebenstehenden QR-Code).

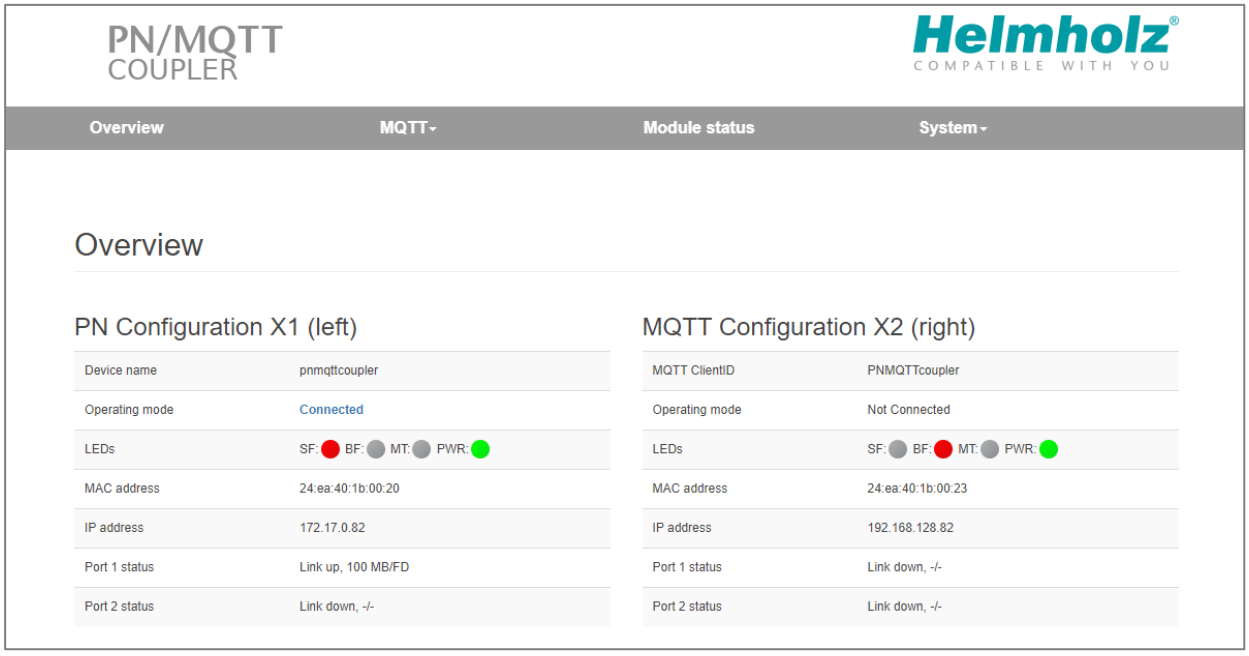
8 Konfiguration der MQTT-Verbindung

8.1 Zugriff auf die Webseite

Sobald der PN/MQTT Coupler über die PROFINET SPS konfiguriert wurde ist die Webseite des Gerätes über das PROFINET-Netzwerk erreichbar. Sollte die IP-Adresse auf der MQTT Netzwerkseite ebenfalls vorhanden sein (Static-IP, DHCP erfolgreich) so ist die Webseite über das MQTT-Netzwerk ebenfalls erreichbar.

HINWEIS Bitte beachten Sie in der Inbetriebnahmephase in der PROFINET-Konfiguration zumindest die Webseite auf der PROFINET-Netzwerkseite (X1) zu aktivieren.

Beim ersten Zugriff auf das Gerät muss für den User “admin“ ein Passwort mit mindestens 8 Zeichen vergeben werden. Nach dem Einloggen ist die „Overview“ Ansicht zu sehen:



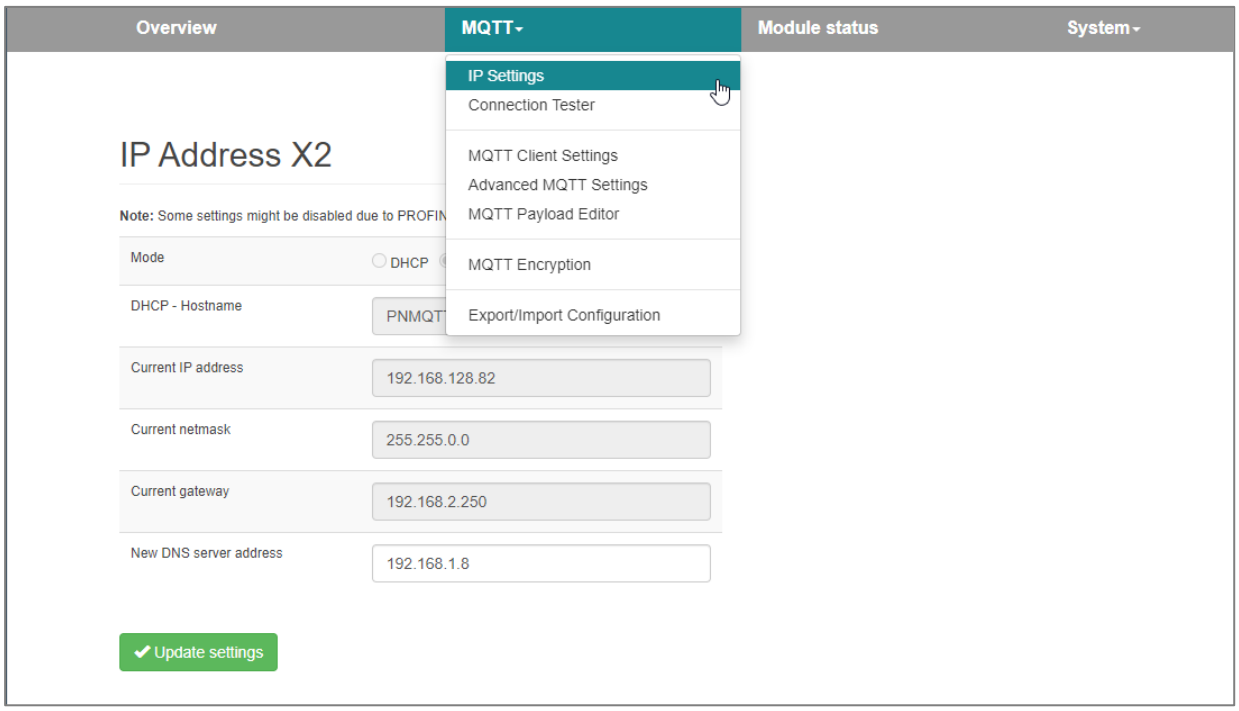
Der PN/MQTT Coupler zeigt auf der „Overview“ Seite in diesem Zustand noch auf dem X2 Interface „Busfehler (BF)“ an, da noch keine Verbindung zum MQTT-Broker konfiguriert worden ist.

Der Fehler „Systemfehler (SF)“ auf der PROFINET-Seite wird ebenfalls aufgrund der nicht konfigurierten MQTT-Verbindung angezeigt.

HINWEIS Sollte die Webseite des Gerätes nicht erreichbar sein, prüfen Sie bitte den Parameter „Webseite“ in der PROFINET-Konfiguration (s. Kap. 7.1), sowie die korrekte Angabe der IP-Adresse und Subnetzmaske passend zu dem Gerät, mit dem Sie die Webseite aufrufen.
Bitte beachten Sie, dass die Webseite einen Inaktivitäts-Timeout hat. Sollten Sie eine Zeit lang nicht auf die Webseite zugreifen, werden Sie ausgeloggt.

8.2 MQTT Grundkonfiguration

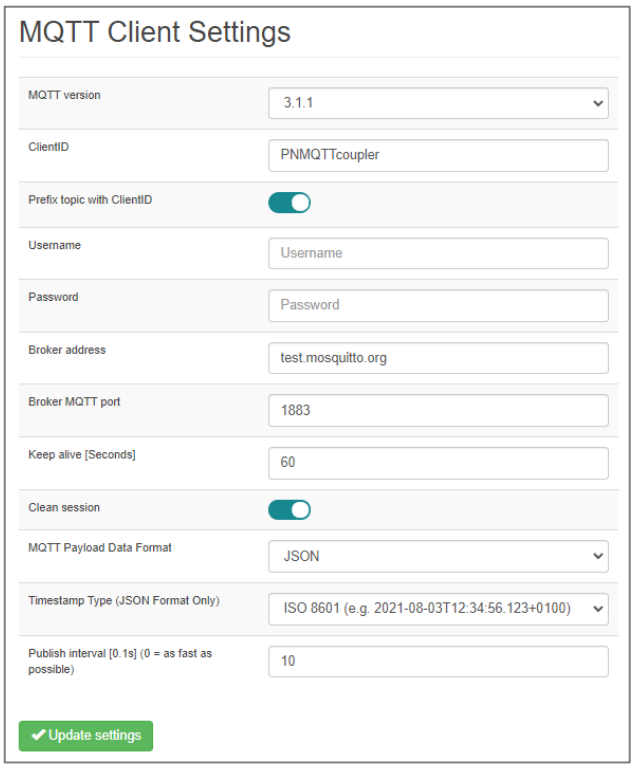
Nach der Konfiguration der PROFINET-Seite muss auf der Webseite des PN/MQTT Coupler noch die Verbindung zum MQTT-Broker konfiguriert werden. Die Konfiguration kann im Menü „**MQTT**“ vorgenommen werden. Wählen Sie zuerst die „**IP Settings**“.



Im Abschnitt „IP Address X2“ wird die IP-Adresse des rechten Netzwerkanschlusses „X2“ des PN/MQTT Coupler angezeigt. Diese kann eingestellt werden, wenn sie nicht über die PROFINET-Konfiguration „Static IP“ schon fest vorgegeben oder per „DHCP“ empfangen wurde.

Über die Schnittstelle X2 wird der MQTT-Broker angesprochen. Sollte sich der MQTT-Broker im gleichen Netzwerk wie die PROFINET-SPS befinden, siehe Hinweis im Kapitel 5.2.

Die notwendigen Informationen zur Verbindung mit dem MQTT-Broker können im Menü „**MQTT**“ unter „**MQTT Client Settings**“ vorgenommen werden.



MQTT version: Der PN/MQTT Coupler unterstützt den MQTT-Standard „3.1.1“ und den neuen Standard „V5“. Da die beiden Standards nicht kompatibel sind, muss die MQTT Version passend zum Broker eingestellt werden.

ClientID: Name des MQTT Clients bei Anmeldung an einem Broker

Prefix topic with ClientID: Mit dieser Option kann jedem Topic die ClientID des Gerätes vorangesetzt werden. Aus dem Topic Namen „Temperatur“ wird dann „<ClientID>/Temperatur“.

Username/Password: Authentifizierung am Broker

Broker address: IP-Adresse oder Domainname des Brokers. Der Broker muss im selben Subnetz sein wie die IP-Adresse des X2 Netzwerks des Kopplers.

Broker TCP Port: Port für die MQTT Verbindung zum Broker. Üblich sind „1883“ für unverschlüsselte und „8883“ für TLS verschlüsselte Verbindungen.

Keep alive: Zeitraster für die zyklische Lebensmeldung des Kopplers an den Broker. Sollte diese Meldung ausbleiben, so geht der Broker von einem Ausfall des Kopplers aus.

Clean session (MQTT V3.1.1): Information an den Broker bei Aufbau der Verbindung, ob alte Nachrichten gelöscht oder gespeichert werden sollen.

Clean start (MQTT V5): Wenn Clean Start aktiviert ist, müssen der Client und der Broker bei Verbindungsaufbau bestehenden Sitzungen verwerfen und eine neue Sitzung starten.
Wenn Clean Start deaktiviert ist und eine Sitzung mit dieser Client-ID verknüpft ist, muss der Broker die Kommunikation mit dem Client basierend auf dem Status der Sitzung wieder aufnehmen. Wenn keine Sitzung mit dieser Client-ID verknüpft ist, muss der Broker eine neue Sitzung erstellen.

Session expiry interval [Seconds] (MQTT 5.0 only): Im Zusammenhang mit „Clean start“, wenn "Session expiry interval" auf 0 gesetzt ist, wird die Sitzung beendet, wenn die Netzwerkverbindung geschlossen wird. Ansonsten wird die Session offen behalten bis die Zeit abgelaufen ist.

MQTT payload data format:
Der Wert eines Topics kann in einfacher Textform („Text“) oder in strukturierter Form („JSON) gesendet werden. Weitere Informationen zur Darstellung der Werte sind im Kapitel 8.3 erläutert.

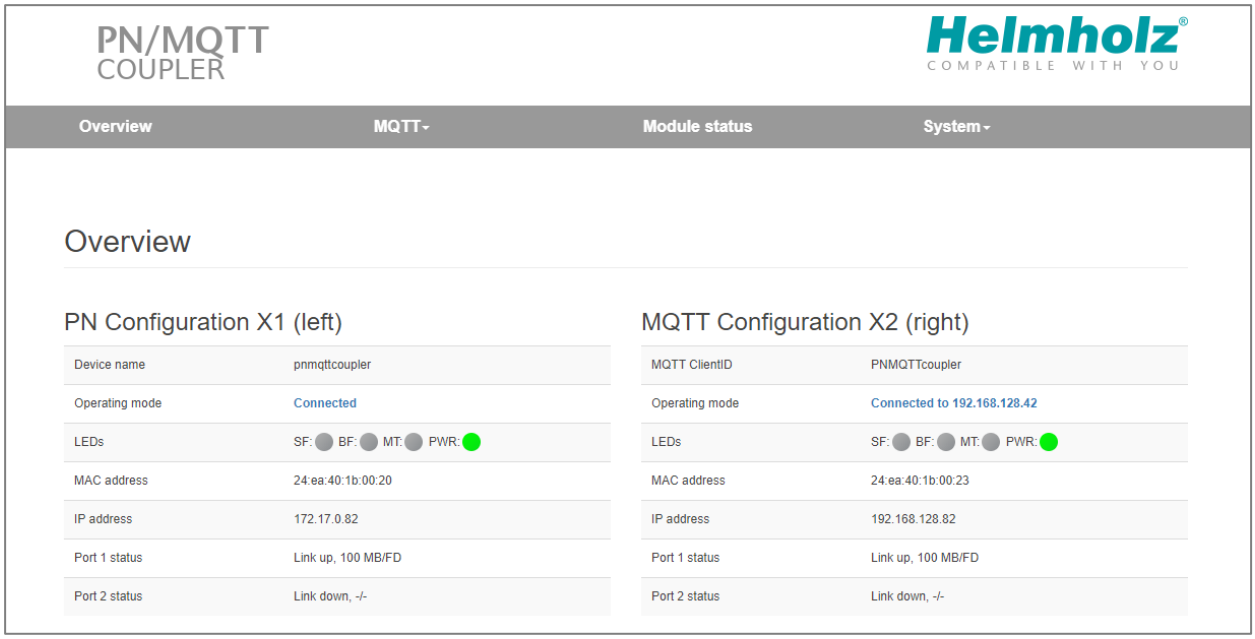
Timestamp Type: Der PN/MQTT Coupler kann (nur bei JSON formatierten Nachrichten) einen Timestamp zur Nachricht hinzufügen.

Publish interval: Eine MQTT Nachricht für einen Slot wird automatisch versendet, sobald der Wert sich verändert. Sollen SPS-Werte versendet werden, die sich sehr schnell verändern, ist es möglich das Sende-Intervall zu begrenzen. Das Publish interval ‚0‘ gibt dem Koppler vor so schnell wie möglich zu senden. Eine Zahl größer als Null gibt vor nicht schneller als **x** * 0,1 Sekunden zu senden.

8.3 MQTT Broker Verbindung aufbauen und prüfen

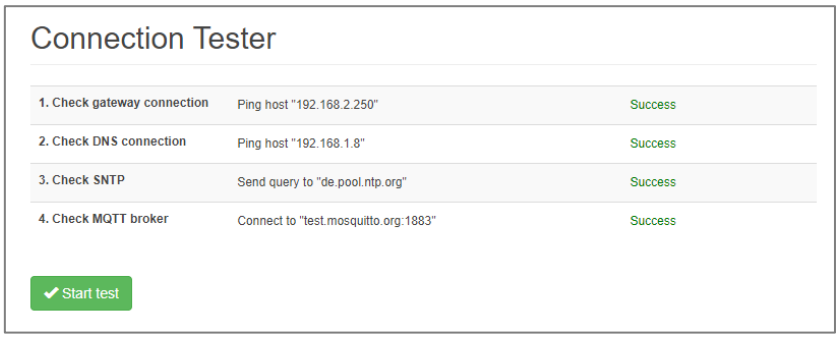
Wurden alle Parameter in der Grundkonfiguration korrekt eingestellt und mit „Update settings“ übernommen, sollte der PN/MQTT Coupler automatisch die Verbindung mit dem MQTT-Broker aufnehmen und die roten LEDs sollten nicht mehr angezeigt werden.

Die „Overview“ Ansicht kann der Zustand überprüft werden:



Im nächsten Schritt können Sie im SPS Programm die EA-Daten ansprechen.

Zum Prüfen der MQTT Broker Verbindung stellt der PN/MQTT Coupler einen „Connection Tester“ im Menü „MQTT“ zur Verfügung.



Der Connection Tester testet in aufbauenden 4 Schritten, ob eine Verbindung mit dem Internet hergestellt werden kann, ob die Namensauflösung und der Zeitserver funktioniert und ob der MQTT Broker Port erreichbar ist.

8.4 MQTT Payload Formate

Der Wert eines Topics kann in einfacher Textform („Text“) oder in strukturierter Form („JSON“) gesendet werden. Die Festlegung kann nur global für alle Topics zusammen unter „MQTT Client Settings“ eingestellt werden.

Beispiel Text:

```
-12345
```

Manche MQTT Anwendungen erwarten eine strukturierte Form im JSON-Format.

Beispiel JSON:

```
{
   "value": -12345
}
```

Die Werte werden je nach Datentyp unterschiedlich dargestellt:

Typ	Größe	Format	Darstellung
Bit	Bit	Text	„0“/„1“, „off“/„on“, „no“/„yes“, „false“/„true“ (parametrierbar, siehe Hinweis)
Byte	1 Byte	Hexadezimal	„0x00“ ... „0xFF“
Unsigned short Int	1 Byte	Dezimal	„0“ ... „255“
Signed short Int	1 Byte	Dezimal	„-127“ ... „128“
Word	2 Bytes	Hexadezimal	„0x0000“ ... „0xFFFF“
Unsigned Int	2 Bytes	Dezimal	„0“ ... „65536“
Signed Int	2 Bytes	Dezimal	„-32767“ ... „32787“
Double Word	4 Bytes	Hexadezimal	„0x00000000“ ... „0xFFFFFFFF“
Unsigned double Int	4 Bytes	Dezimal	„0“ ... „4294967295“
Signed double Int	4 Bytes	Dezimal	„-2147483648“ ... „2147483647“
Real	4 Bytes	Fließkomma	„-123.456789“ (Beispiel)
Long Real	8 Bytes	Fließkomma	„123456.789999“ (Beispiel)

ACHTUNG Module mit Datentyp „Bit“ belegen in der SPS ein ganzes Byte, da PROFINET keine Bits unterstützt. Von dem übertragenen Byte wird nur das unterste Bit ausgewertet.
Wird ein Topic vom Typ Bit empfangen (Topic Subscription) so werden alle o.g. Formate interpretiert und die Groß-/Kleinschreibung ist beliebig.

HINWEIS Benötigen Sie für Ihre Anwendung eine andere Darstellung des MQTT Payloads, so kontaktieren Sie uns. Die Payload Varianten werden ständig erweitert.

9 Status und Steuerung über die SPS

9.1 Status des PN/MQTT Coupler

Der PN/MQTT Coupler stellt einen Status (4 Bytes) über das PROFINET-Eingangsabbild zur Verfügung:

Byte/Bit	7	6	5	4	3	2	1	0
Eingangs-Byte 0	PROFINET Konfiguration OK	0	PS 1 Spannung vorhanden	PS 2 Spannung vorhanden	0	0	X2 Netzwerk IP-Adresse vorhanden	X2 Netzwerk-Kabel erkannt
Eingangs-Byte 1	0	0	0	0	0	0	0	MQTT Broker Verbindung aktiv
Eingangs-Byte 2	Letzter MQTT-Fehlercode (ab MQTT V5) oder Connect Return/Reason-Code							
Eingangs-Byte 3	*reserviert*							

Zur Prüfung der korrekten Funktion des PN/MQTT Coupler in der SPS sollten das Bit „PROFINET Konfiguration OK“ sowie „MQTT Broker Verbindung aktiv“ gelesen werden.

9.2 Steuerung des PN/MQTT Coupler

Über folgende Steuerbits (1 Byte) im PROFINET-Ausgangsabbild kann der PN/MQTT Coupler gesteuert werden:

Byte/Bit	7	6	5	4	3	2	1	0
Ausgangs-Byte 0	MQTT-Error Code löschen		-	-	-	-	MQTT Verbindung trennen	MQTT Datenaus-tausch sperren

9.3 „Subscribe“ Module

Die Subscriber Module haben neben den Eingangsdaten für den eigentlichen Wert noch jeweils ein Status- und ein Steuerbyte.

Statusbits der Subscribe Module:

Byte/Bit	7	6	5	4	3	2	1	0
Eingangs-Byte 0	1 = neue Daten wurden empfangen	Empfangszähler						

Steuerung der Subscribe Module:

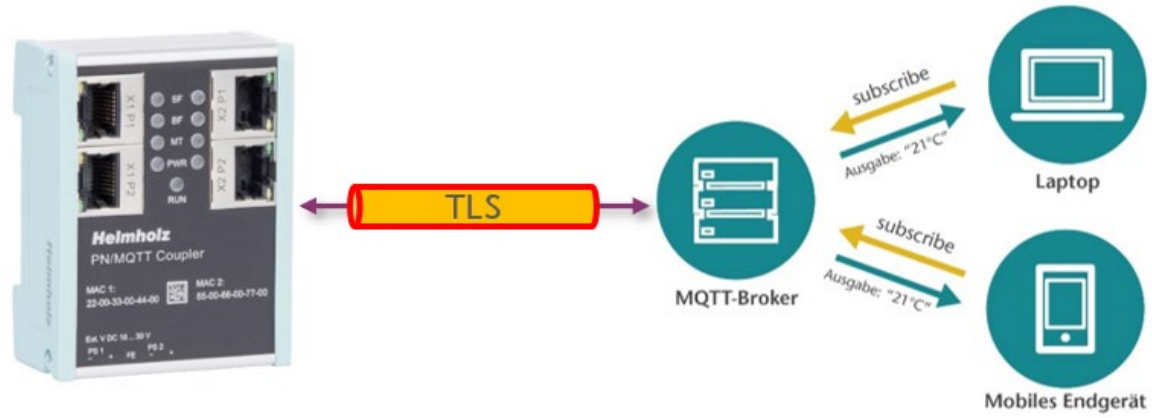
Byte/Bit	7	6	5	4	3	2	1	0
Ausgangs-Byte 0	1 = Datenempfangs-Bit zurücksetzen	-	-	-	-	-	-	-

Um den Empfang von MQTT Nachrichten erkennen zu können kann das Empfangs-Bit 7 verwendet werden, welches im Ausgangsbyte des Moduls immer zurückgesetzt werden muss. Alternativ kann der Empfangszähler auf Veränderung geprüft werden.

Achtung: der Empfangszähler läuft bis 0x7F und wird dann auf 0x00 zurückgesetzt.

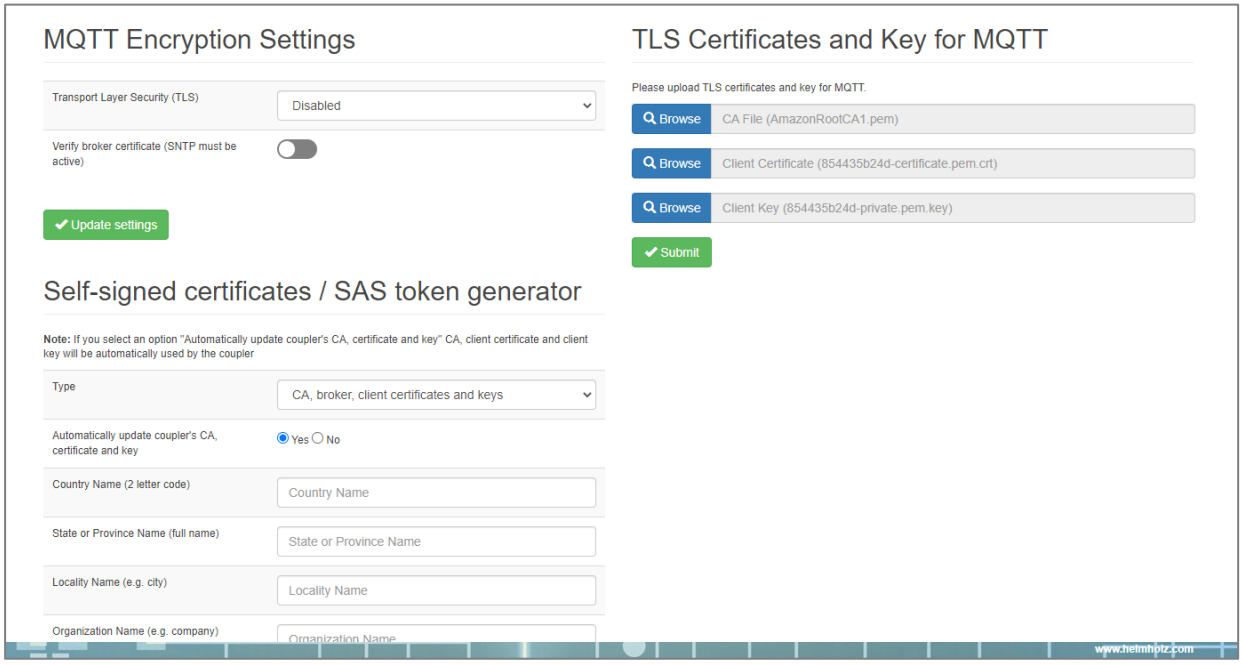
10 MQTT Verschlüsselung und Authentifizierung

Die Übertragung zwischen dem Client und dem Broker kann verschlüsselt werden und die Geräte können sich gegenseitig Authentifizieren also Ihre Identität überprüfen.

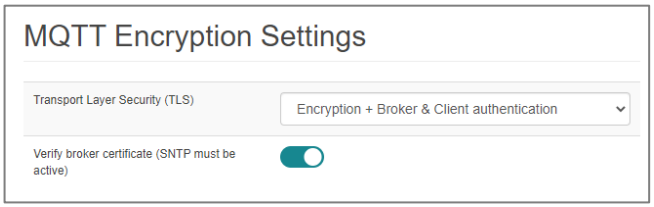


Die Verschlüsselung verhindert, dass ein Dritter die Daten mitlesen kann. Die Authentifizierung stellt sicher, dass nur die „richtigen“ Geräte miteinander Daten austauschen können.

Im Menü „MQTT“ unter „MQTT Encryption“ kann die Verschlüsselung aktiviert, Zertifikate hinterlegt, aber auch selbstgenerierte Zertifikate erstellt werden.



Transport Layer Security (TLS):
Disabled: unverschlüsselter Datenaustausch zwischen Client und Broker. Es werden keine Zertifikate oder Keys benötigt.



Enabled – Encryption only: Aktiviert die Verschlüsselung ohne Authentifizierung. Diese Option erfordert weder ein CA- noch Client-Zertifikat oder Client-Key.

Encryption + Broker authentication: Aktiviert die Verschlüsselung mit Broker-Authentifizierung durch den Client. Bei dieser Option muss eine CA zur Broker-Verifizierung hochgeladen werden (s.u.).

Encryption + Broker & Client authentication: ermöglicht die Verschlüsselung mit gegenseitiger Broker- und Client-Authentifizierung. Bei dieser Option ist ein CA- und Client-Zertifikat erforderlich. Zusätzlich zur Broker-Verifizierung durch den Client kann der Broker auch den Client verifizieren, da er sein Zertifikat während des TLS-Handshakes sendet.

Verify broker certificate: Zertifikate enthalten ein Ablaufdatum und müssen regelmäßig aktualisiert werden. Durch diese Option wird geprüft, ob das Broker Zertifikat noch gültig ist.

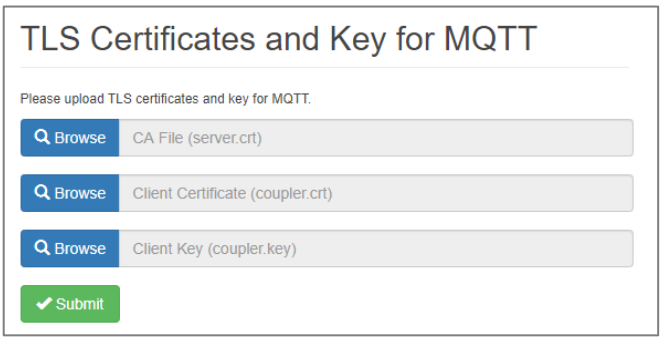
ACHTUNG Bei der Verwendung von Zertifikaten zur Authentifizierung muss die Zeitsynchronisierung des PN/MQTT Couplers mittels SNTP aktiviert sein.

Für die Verschlüsselung und Authentifizierung müssen dem PN/MQTT Coupler Zertifikate und Keys mitgegeben (hochgeladen) werden.

CA File: Zertifikat des Brokers oder übergeordnete Zertifikatsdatei

Client Certificate: Zertifikat für den PN/MQTT-Coupler

Client Key: Private Key für den PN/MQTT-Coupler



10.1 Generator für Zertifikate und SAS Token

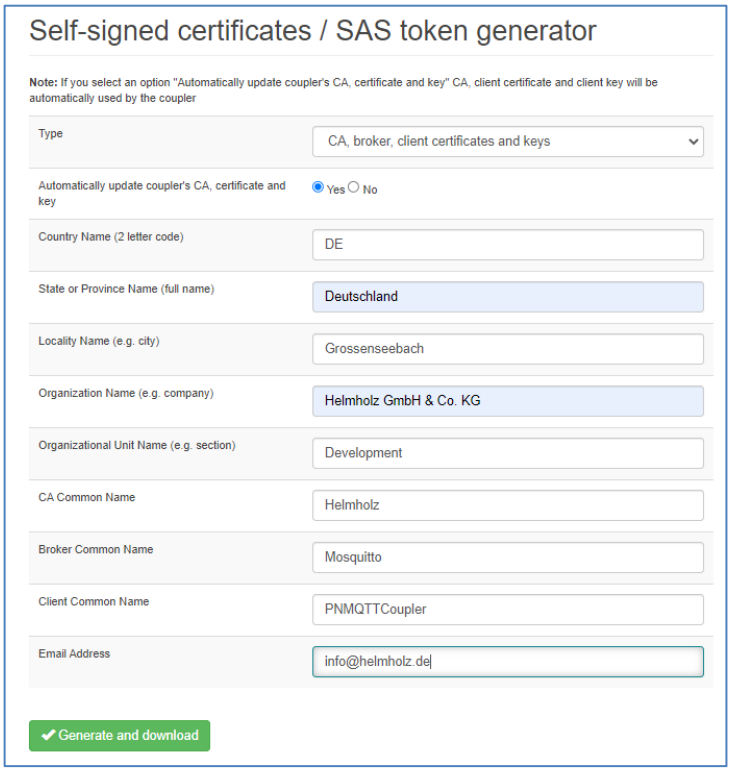
Für eine verschlüsselte und authentifizierte Verbindung mit einem Broker – egal ob „on premise“ oder in der Cloud - sollte das Zertifikat des Brokers und das Zertifikat der übergeordneten Zertifizierungsstelle (‚CA‘) herunterladbar oder von der IT für das eigene Netzwerk generiert werden.

Das Zertifikat für den Client sollte dann auch entweder von der Broker-Anwendung generiert werden (Beispiel „Amazon IoT“, siehe Kapitel 17) oder ebenfalls von der IT erstellt werden.

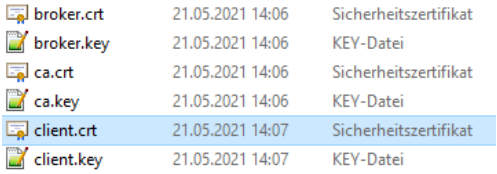
Um die Arbeit mit Zertifikaten bei internen Tests zu erleichtern, beinhaltet der PN/MQTT Coupler einen eingebauten Generator für selbst-signierte Zertifikate. Für die Anwendung mit Microsoft Azure steht zusätzlich ein SAS Token Generator zur Verfügung (siehe Kapitel 18).

Soll für einen Testaufbau mit einem lokalen Broker (z.B. Mosquitto) eine verschlüsselte und authentifizierte Verbindung hergestellt werden, so kann der PN/MQTT Koppler mit der Option **„CA, broker, client certificates and keys“** die Zertifikate und die Private-Keys sowohl für den PN/MQTT-Coupler selbst als auch für den Broker erstellen. Das Zertifikat der lokalen Zertifizierungsstelle (‚CA‘) mit dem die anderen beiden Zertifikate signiert wurden, wird ebenfalls mitgeliefert.

Die Eingabefelder werden inhaltlich in die Zertifikate übernommen, haben aber eher informativen Charakter.

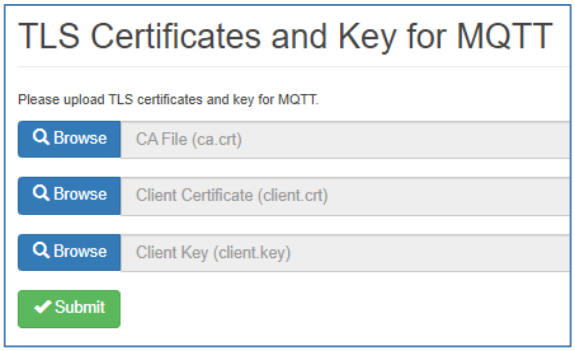


Nach dem Drücken des Buttons „Generate and Download“ werden die Zertifikate generiert und es wird eine ZIP-Datei mit den Zertifikaten heruntergeladen:



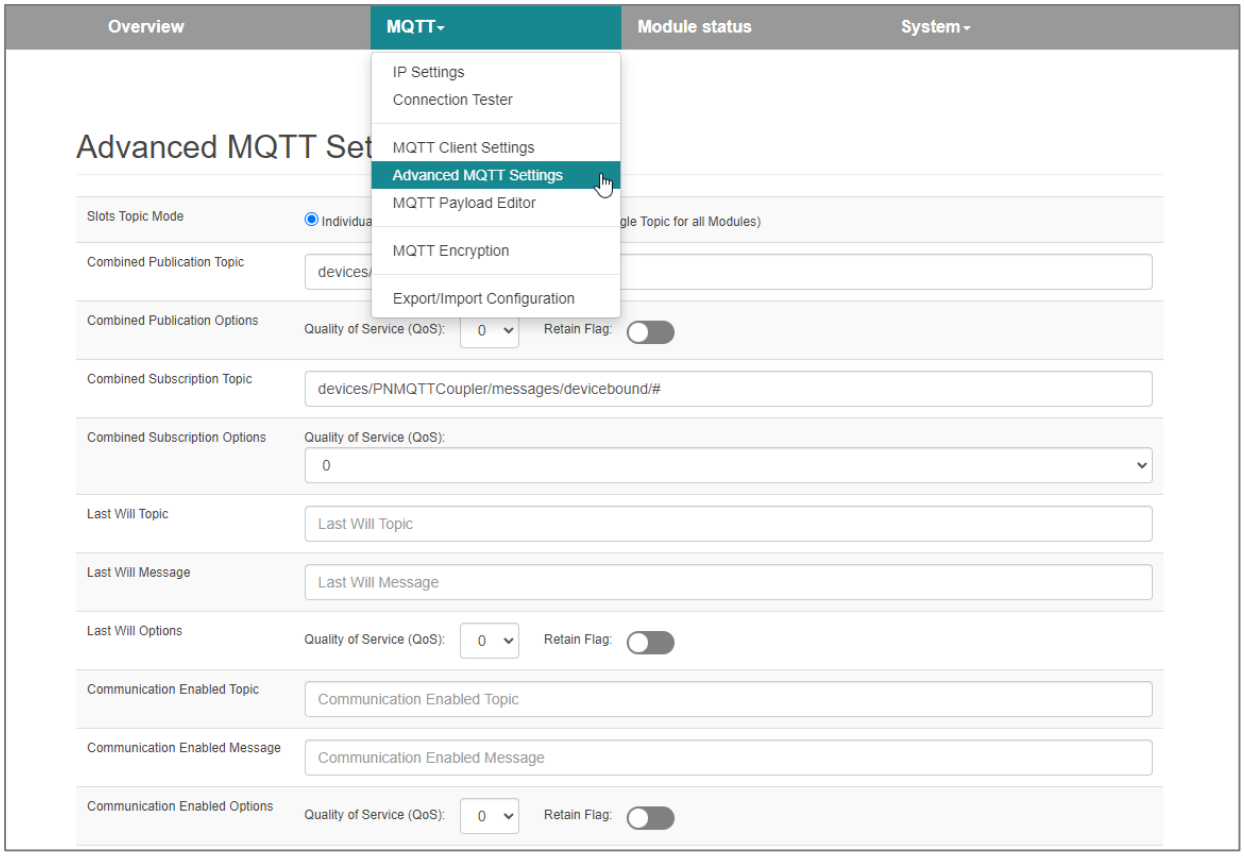
Die Option „Automatically update coupler's CA, certificate and key“ übernimmt die relevanten Dateien direkt in den PN/MQTT-Coupler.

Im Broker kann jetzt ebenfalls sein private Key, sein Zertifikat und die CA-Datei verwendet werden.



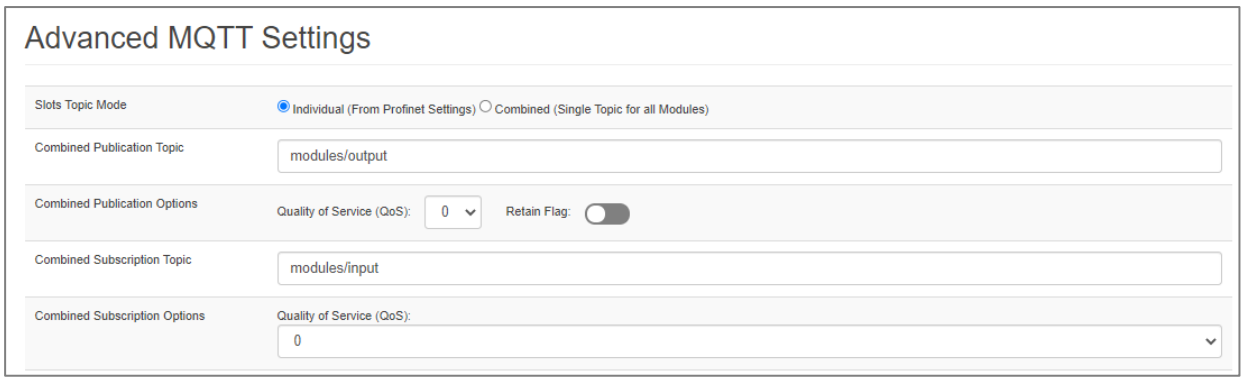
11 Weitere MQTT Einstellungen

Unter dem Menu „Advanced MQTT Settings“ können weitere Einstellungen zum MQTT Verhalten des PN/MQTT Coupler vorgenommen werden.



11.1 Topic Mode

Der Topic Mode bestimmt wie alle konfigurierten Topic Messages gesendet werden sollen. Üblicherweise wird jedes Topic (jedes konfigurierte Modul) einzeln als MQTT Message versendet oder empfangen → Topic Mode *„Individual“*.



Für bestimmte Anwendungen, z.B. zur Verbindung mit der Microsoft Azure Cloud (siehe Kapitel 18), darf ein Gerät nur unter einer MQTT Nachricht alle Daten versenden oder empfangen → Topic Mode *„Combined“*.

Für den Anwendungsfall Combined kann in den folgenden Einstellungen der Topic Name für das Publishing und der Topic Name für die Subscription sowie die zugehörige QoS- und Retain-Eigenschaft festgelegt werden.

Beispiel für Topic Mode „Individual“:

Message 1 für Topic „Temperature“:

```
{
   "value": 23
}
```

Message 2 für Topic „Humidity“:

```
{
   "value": 40
}
```

Beispiel für Topic Mode „Combined“:

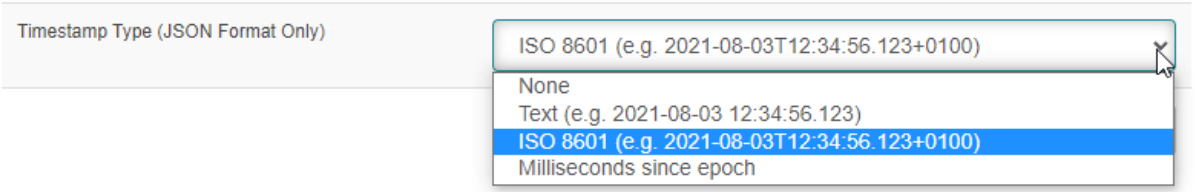
Message für Topic „modules/output“:

```
{
   "Temperature": 23
   "Humidity": 40
}
```

11.2 Timestamp in Topic Nachrichten (nur JSON)

In vielen Anwendungen ist es wichtig mit der Dateninformation in der Nachricht auch eine Zeitinformation mitgeliefert zu bekommen um den zum Datum gehörigen Zeitpunkt mit speichern zu können.

Im Menü MQTT Client Settings kann – ausschließlich für JSON Nachrichten – eingestellt werden, dass ein Zeitstempel in der Nachricht mitgesendet wird.



Es stehen 3 verschiedene Zeitstempelformaten zur Verfügung.

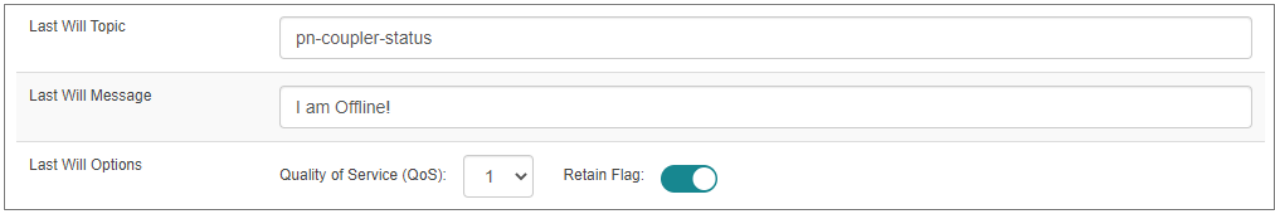
Beispiel mit ISO 8601 Zeitstempel:

```
{
   "timestamp": "2021-10-19T11:49:41.809+0200",
   "value": 235243
}
```

HINWEIS Für komplexere MQTT Nachrichten kann der MQTT Payload Editor verwendet werden. Siehe Kapitel 11.5.

11.3 Last Will Message

Die „Last Will Message“ ist eine MQTT Nachricht, um andere Clients über einen nicht ordnungsgemäß getrennten Client zu informieren. Der PN/MQTT Coupler sendet seine Nachricht des „letzten Willens“ an den Broker, wenn er eine Verbindung zu dem Broker herstellt. Unter dem Menu „Advanced MQTT Settings“ kann die Last Will Message eingestellt werden.



Die Nachricht des „letzten Willens“ ist eine normale MQTT-Nachricht mit einem beliebigen Topic und einem beliebigen Payload. Der Broker speichert die Nachricht, bis er feststellt, dass der Client die Verbindung unfreiwillig getrennt hat. Als Reaktion auf die unvorhergesehene Verbindungstrennung sendet der Broker die „Last-Will“ Nachricht an alle abonnierten Clients des „Last-Will“-Topics.

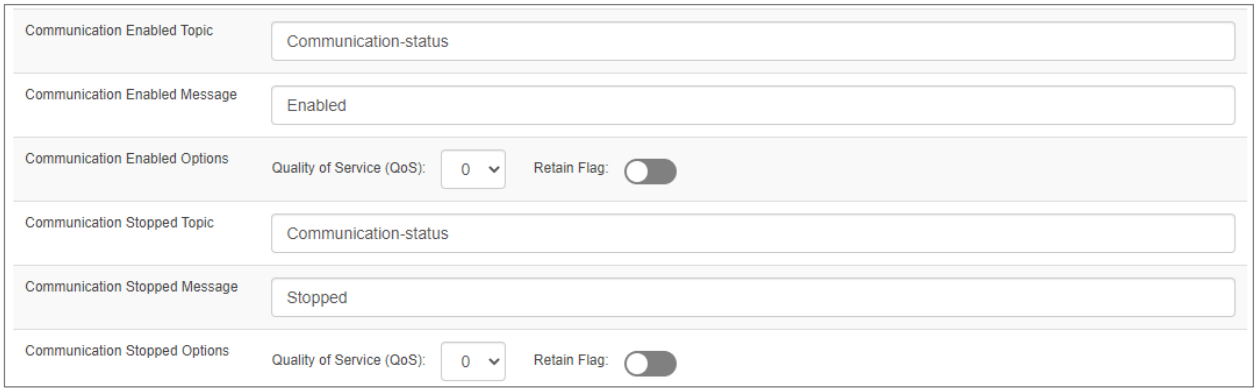
Wenn der Client die Verbindung ordnungsgemäß trennt, verwirft der Broker die gespeicherte „Last Will Message“.

HINWEIS Nicht alle Broker unterstützen die Last Will Message.

11.4 „Communication Enable“ und „Communication Stopped“ Messages

Die „Communication Enable“ Message wird vom PN/MQTT-Coupler immer dann gesendet, wenn der Koppler betriebsbereit ist. Dazu muss der Koppler über PROFINET konfiguriert sein und die SPS im RUN sein.

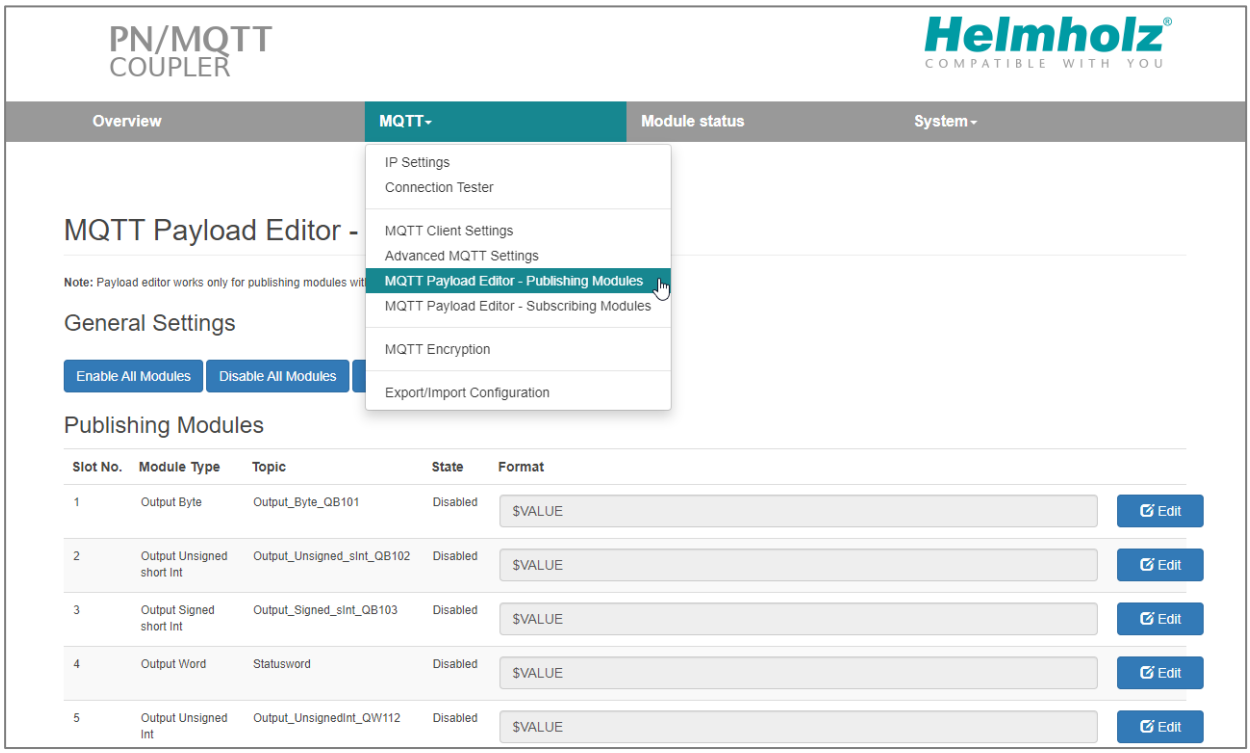
Die „Communication Stopped“ Message wird vom PN/MQTT-Coupler immer dann gesendet, wenn der Koppler nicht mehr betriebsbereit ist. Gründe hierfür sind eine Netzwerkunterbrechung, eine Umkonfiguration oder wenn die SPS in Stopp gegangen ist.



11.5 Payload Editor

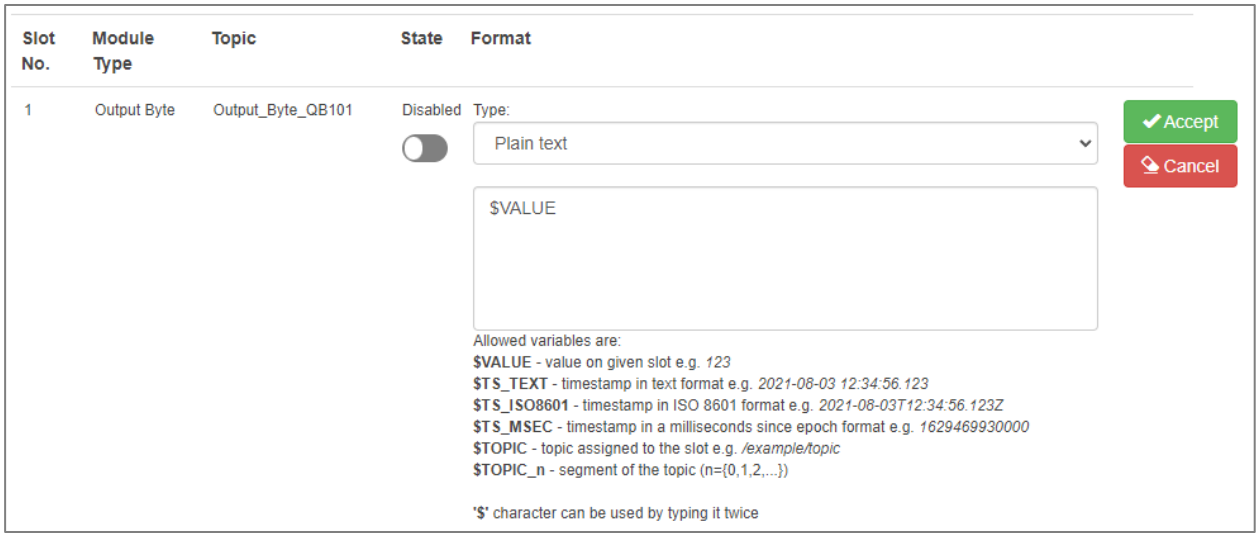
Der Inhalt einer MQTT Nachricht kann abhängig von der Anwendung einen komplexen Aufbau erfordern. Der PN/MQTT Coupler stellt hierfür einen Payload Editor bereit.

Für jedes Publish Topic kann mit dem „MQTT Payload Editor“ getrennt und unabhängig das Format der versendeten Nachricht frei definiert werden. Der Payload Editor steht sowohl für das Senden als auch für den Empfang zur Verfügung.



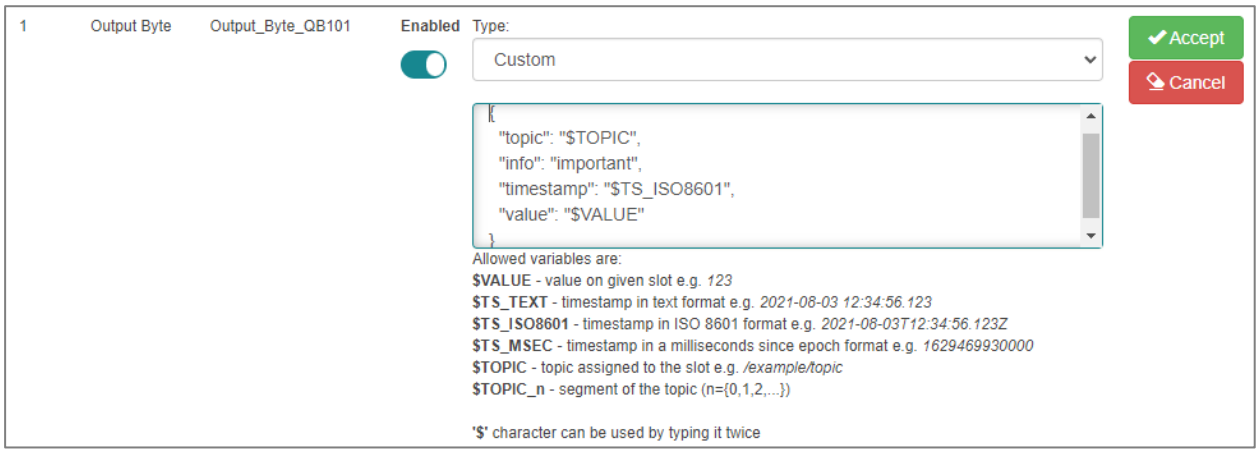
Im Grundzustand ist der Payload Editor für alle Topics abgeschaltet (State = „Disabled“). In diesem Zustand wird die Payload des Topic so versendet wie es in den “MQTT Client Settings“ eingestellt wurde.

Um für ein Topic eine individuelles Payload Format einzustellen, muss der Button „Edit“ gedrückt werden:



Unter „Type“ kann ausgewählt werden, ob die Payload als „Plain Text“, „JSON“ oder „Custom“ (frei editierbar) formatiert aufgebaut werden soll. Mit der Einstellung „Custom“ kann in dem Feld unter „Type“ die Nachricht in einem Editor frei aufgebaut werden.

Hier ein Beispiel für eine frei aufgebaute JSON Nachricht:

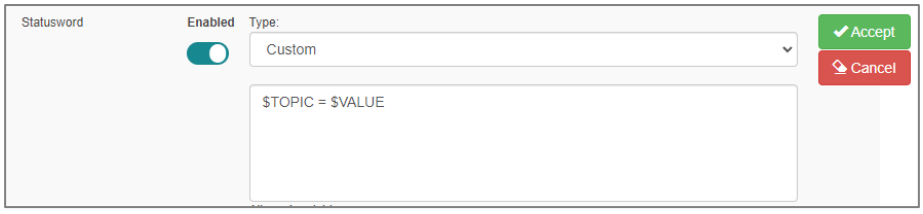


Mit dem Schalter links neben „Type“ kann das im Payload Editor eingestellte Nachrichtenformat aktiviert („Enabled“) oder ignoriert („Disabled“) werden.

Hier eine Beispiel Aussendung des Topics „Output_Byte_QB101“:

```
{
  "topic" : "Output_Byte_QB101",
  "info" : "important",
  "timestamp" : "2021-10-26T08:50:47.128+0200",
  "value" : "0x00"
}
```

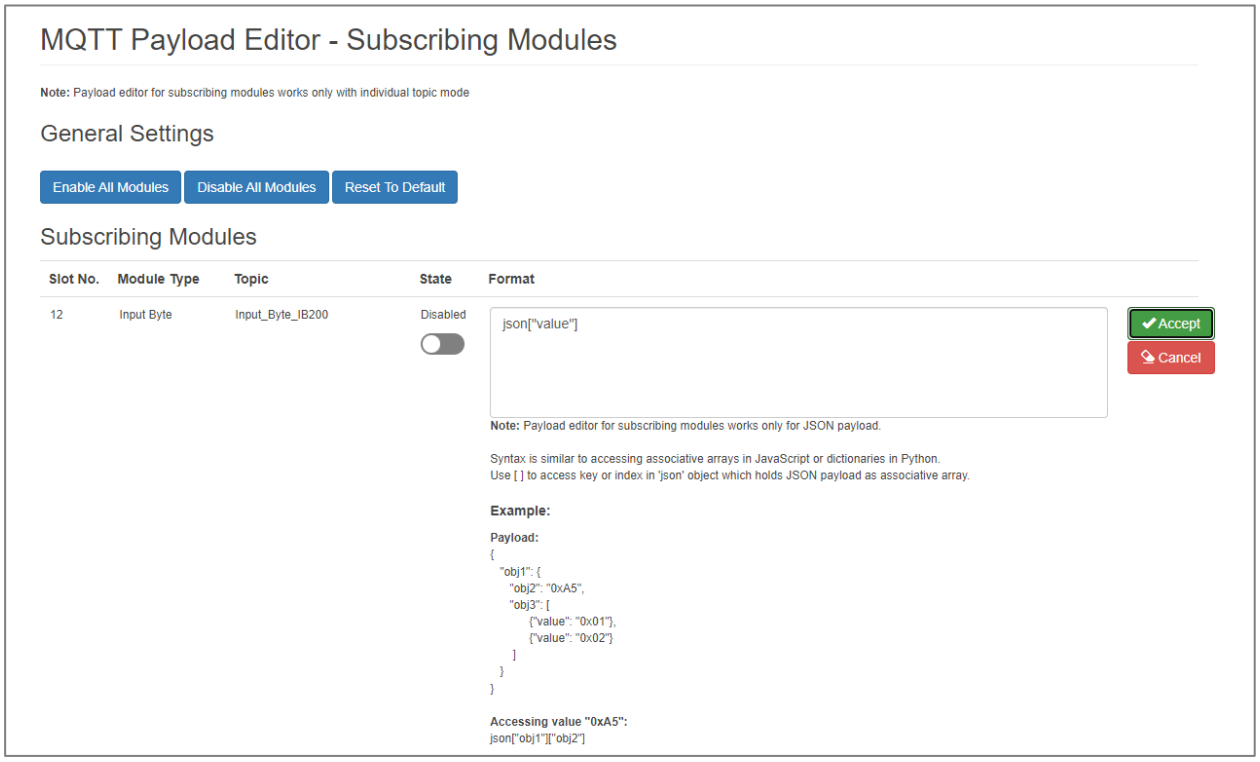
Der Payload Editor können auch beliebig formatierte Nachrichten gesendet werden. Ein Beispiel:



→ `Statusword = 0x1234`

HINWEIS Benötigen Sie für Ihre Anwendung eine bestimmte Darstellung des MQTT Payloads, so kontaktieren Sie uns. Wir unterstützen Sie gerne.

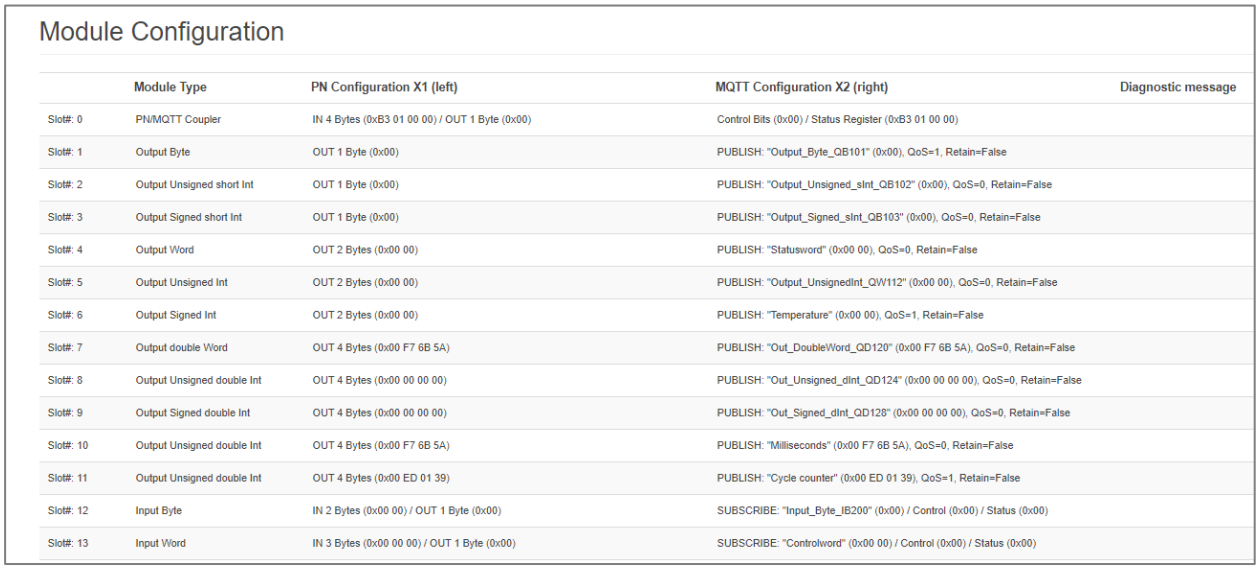
Der Payload Editor für empfangene Nachrichten (Subscribing Modules) arbeitet nach einem ähnlichen Konzept. Die Angaben im Payload Editor haben jetzt aber die Funktion aus einer komplexen Nachricht den gewünschten Wert herauszuholen. Der Payload-Editor geht zwingend davon aus, dass die empfangene Nachricht JSON formatiert ist. In der empfangenen JSON Struktur kann jetzt der Wert über das benannte Objekt innerhalb der Struktur ausgewählt werden.



12 Weitere Funktionen im Webinterface

12.1 Modul-Status

Auf der Webseite „Modul-Status“ wird die projektierte Modul-Konfiguration und die aktuellen IO-Daten angezeigt. Sollte ein Konfigurationsfehler vorliegen so wird der Fehler in der Spalte „Diagnostic message“ angezeigt.



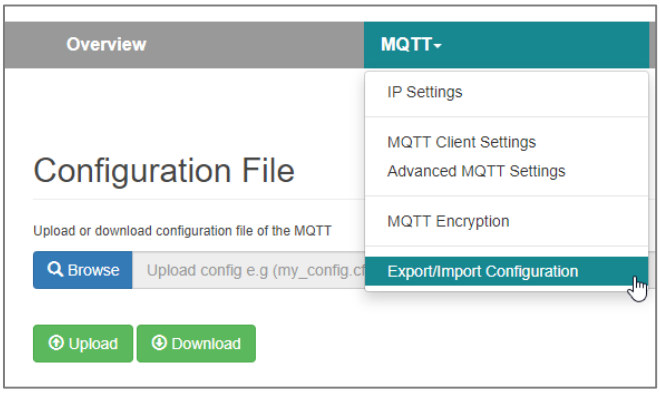
Module Configuration

	Module Type	PN Configuration X1 (left)	MQTT Configuration X2 (right)	Diagnostic message
Slot#: 0	PN/MQTT Coupler	IN 4 Bytes (0xB3 01 00 00) / OUT 1 Byte (0x00)	Control Bits (0x00) / Status Register (0xB3 01 00 00)	
Slot#: 1	Output Byte	OUT 1 Byte (0x00)	PUBLISH: "Output_Byte_QB101" (0x00), QoS=1, Retain=False	
Slot#: 2	Output Unsigned short Int	OUT 1 Byte (0x00)	PUBLISH: "Output_Unsigned_sInt_QB102" (0x00), QoS=0, Retain=False	
Slot#: 3	Output Signed short Int	OUT 1 Byte (0x00)	PUBLISH: "Output_Signed_sInt_QB103" (0x00), QoS=0, Retain=False	
Slot#: 4	Output Word	OUT 2 Bytes (0x00 00)	PUBLISH: "Statusword" (0x00 00), QoS=0, Retain=False	
Slot#: 5	Output Unsigned Int	OUT 2 Bytes (0x00 00)	PUBLISH: "Output_UnsignedInt_QW112" (0x00 00), QoS=0, Retain=False	
Slot#: 6	Output Signed Int	OUT 2 Bytes (0x00 00)	PUBLISH: "Temperature" (0x00 00), QoS=1, Retain=False	
Slot#: 7	Output double Word	OUT 4 Bytes (0x00 F7 6B 5A)	PUBLISH: "Out_DoubleWord_QD120" (0x00 F7 6B 5A), QoS=0, Retain=False	
Slot#: 8	Output Unsigned double Int	OUT 4 Bytes (0x00 00 00 00)	PUBLISH: "Out_Unsigned_dInt_QD124" (0x00 00 00 00), QoS=0, Retain=False	
Slot#: 9	Output Signed double Int	OUT 4 Bytes (0x00 00 00 00)	PUBLISH: "Out_Signed_dInt_QD128" (0x00 00 00 00), QoS=0, Retain=False	
Slot#: 10	Output Unsigned double Int	OUT 4 Bytes (0x00 F7 6B 5A)	PUBLISH: "Milliseconds" (0x00 F7 6B 5A), QoS=0, Retain=False	
Slot#: 11	Output Unsigned double Int	OUT 4 Bytes (0x00 ED 01 39)	PUBLISH: "Cycle counter" (0x00 ED 01 39), QoS=1, Retain=False	
Slot#: 12	Input Byte	IN 2 Bytes (0x00 00) / OUT 1 Byte (0x00)	SUBSCRIBE: "Input_Byte_IB200" (0x00) / Control (0x00) / Status (0x00)	
Slot#: 13	Input Word	IN 3 Bytes (0x00 00 00) / OUT 1 Byte (0x00)	SUBSCRIBE: "Controlword" (0x00 00) / Control (0x00) / Status (0x00)	

12.2 Export/Import der Konfiguration

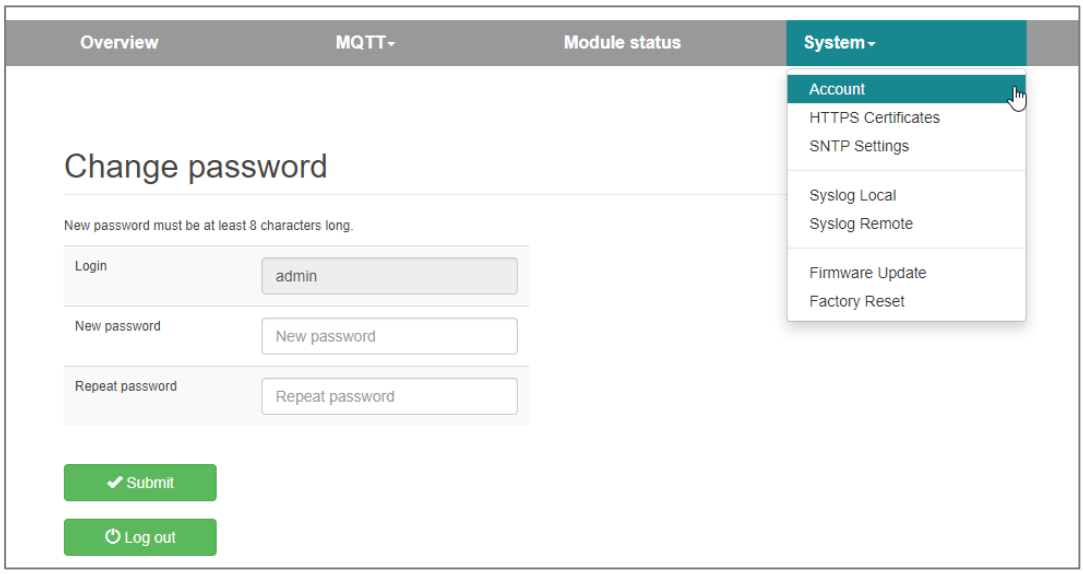
Die auf der Webseite vorgenommenen Einstellungen können zur Sicherung, für die Serienproduktion oder zur manuellen Bearbeitung der Gerätekonfiguration in einem editierbaren Format am PC gespeichert werden (Download).

Bei Bedarf kann die Datei zur Konfiguration eine Gerätes dann wieder hochgeladen werden (Upload).



12.3 Account

Im Menü „System“ unter „Account“ kann das Passwort des Users „admin“ geändert werden.

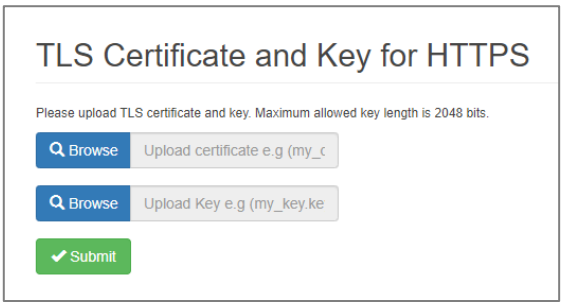


Zurzeit enthält der PN/MQTT Coupler nur diesen User, der Name ist nicht änderbar.

12.4 TLS Zertifikate für HTTPS hinterlegen

Für den sicheren Zugriff auf die Webseite des PN/MQTT Coupler kann im Menü „System“ unter „HTTPS Certificates“ ein firmeneigenes Zertifikat hinterlegt werden.

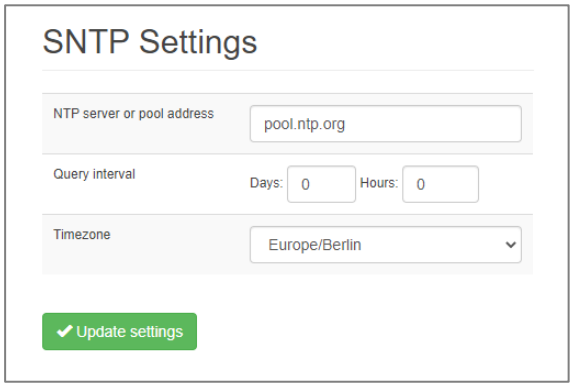
Damit kann sichergestellt werden, dass der Aufruf der PN/MQTT Coupler Konfigurationswebseite neben der HTTPS-Verschlüsselung auch vertrauenswürdig ist.



12.5 SNTP Einstellungen

Der PN/MQTT Coupler kann über die MQTT Netzwerkschnittstelle (X2) per SNTP Protokoll seine Uhrzeit aktualisieren.

Die Uhrzeit wird für das Prüfen der Zertifikate, für das Logging oder ggf. für Timestamps in den MQTT Topics verwendet.



12.6 Firmwareupdate

Die Firmware des PN/MQTT Coupler kann über die Webseite sehr einfach aktualisiert werden. Die Firmware erhalten Sie von der Helmholz Webseite unter www.helmholz.de.

Link zur aktuellsten Firmware:
http://www.helmholz.de/goto/700-162-3MQ02#tab-software

Die Firmwaredatei kann an der Dateiendung "HUF" (Helmholz Update File) erkannt werden und ist verschlüsselt, um diese vor einer Veränderung zu schützen.

Legen Sie die Firmwaredatei auf Ihrem PC ab, wählen den Speicherort mit "Browse" aus und starten Sie das Firmwareupdate mit „Submit“. Danach wird die Firmwaredatei übertragen, entschlüsselt und überprüft. Ist der Inhalt korrekt wird die Firmware in den Programmspeicher gebrannt und ein Neustart des PN/MQTT Coupler durchgeführt.

ACHTUNG Während dem Updatevorgang ist der Betrieb des PN/MQTT Coupler unterbrochen. Schalten Sie das Gerät während dem Updatevorgang nicht aus!

HINWEIS Die Konfiguration des PN/MQTT Coupler wird bei einem Update auf eine höhere Version, soweit es technisch möglich ist, beibehalten. Ein "Downgrade" auf eine ältere Firmwareversion kann aber zu Konfigurationsfehlern führen. Es wird empfohlen nach einem Downgrade ein Werksrücksetzen durchzuführen.

12.7 Rückstellen auf Werkseinstellung

Das Rückstellen des PN/MQTT Coupler auf Werkseinstellung kann über die Webseite oder über die PROFINET-Funktion durchgeführt werden .

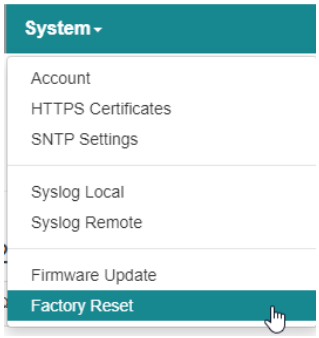
Es wird beim Rücksetzen des PN/MQTT Coupler die Konfiguration unwiederbringlich gelöscht und die Einstellungen auf den Auslieferzustand gesetzt. Die Firmware bleibt dabei auf dem aktuellen Stand.

ACHTUNG Bitte beachten Sie, dass das Gerät nach dem Rückstellen auf Werkseinstellung nicht mehr im Netzwerk verfügbar ist. Der PROFINET-Name und die IP-Adressen werden gelöscht, die Kommunikation mit der SPS wird gestoppt und die SPS erkennt einen Konfigurationsfehler und geht ggf. auch in Stopp.

12.7.1 Rückstellen auf Werkseinstellung über Webseite

Wählen Sie im den Menü „System“ den Menüpunkt „Factory Reset“.

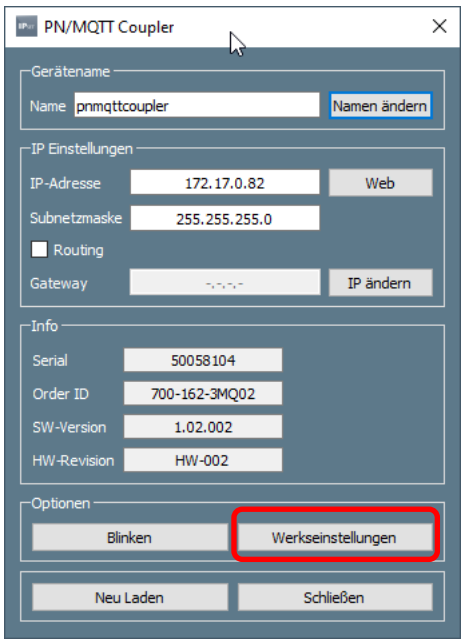
Drücken Sie den Button „Set factory defaults und reboot“ und bestätigen Sie die Sicherheitsabfrage.



12.7.2 Rückstellen auf Werkseinstellung über „IPSet“ Tool

Zum Rücksetzen des PN/MQTT Coupler kann über das PROFINET Netzwerk auch das Helmholz Tool „IPSet“ verwendet werden.

Das Helmholz IPSet Tool kann kostenfrei von der Helmholz Webseite heruntergeladen werden (oder scannen Sie den QR-Code).



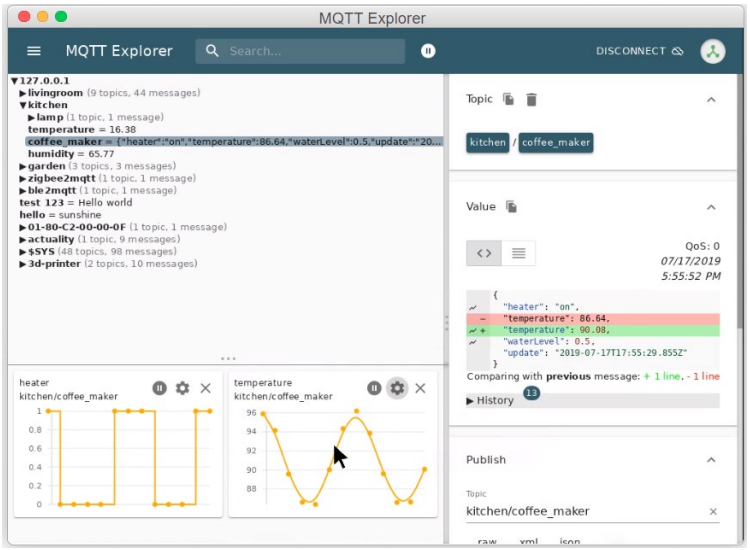
13 Diagnose über LEDs

	X1 PROFINET (linke Seite)	X2 MQTT-Netzwerk (rechte Seite)
SF (rot)		
Aus	Konfiguration korrekt	Konfiguration korrekt
Ein	Es liegt ein PROFINET-Diagnosealarm vor	PROFINET Seite nicht konfiguriert oder ausgefallen
blinkend	PROFINET-Funktion „LED blinken“ zum Auffinden des Gerätes wird ausgeführt	-
BF (rot)		
Aus	Es besteht eine Verbindung zum PROFINET-Controller	Es besteht eine Verbindung mit dem MQTT-Broker
Ein	Das Gerät hat keine Konfiguration, der PROFINET-Gerätename ist nicht korrekt oder es besteht keine Verbindung zum PROFINET Controller.	Es kann keine Verbindung zum MQTT-Broker aufgebaut werden
Blinkend	PROFINET-Funktion „LED blinken“ zum Auffinden des Gerätes wird ausgeführt	-
MT (gelb)		
Blinkend	Ein Firmwareupdate wird durchgeführt	Ein Firmwareupdate wird durchgeführt
Blinkend mit SF und BF	PROFINET-Funktion „LED blinken“ zum Auffinden des Gerätes wird ausgeführt.	-
PWR (grün)		
Ein	PS1 Spannungsversorgung vorhanden	PS2 Spannungsversorgung vorhanden
RUN (grün)		
Aus	Firmware oder Gerät defekt. Bitte wenden Sie sich an den Support	
Ein	Das Gerät ist betriebsbereit	
RJ45 LEDs	X1 P1/P2 und X2 P1/P2	
Grün (Link)	Verbunden	
Orange (Act)	Datenübertragung am Port	

14 Client-Tools für den MQTT Datenaustausch

Um den Datenaustausch über den PN/MQTT-Coupler bereits testen zu können, wenn die Anwendung auf der Gegenseite noch nicht vorhanden ist oder um die vom PN/MQTT Coupler gesendeten Daten neben der Anwendung beobachten zu können, bietet sich der Einsatz von MQTT Client Testprogrammen an. In diesem Kapitel werden 3 MQTT Clients exemplarisch vorgestellt, es gibt aber noch viele weitere Tools.

14.1 MQTT Explorer

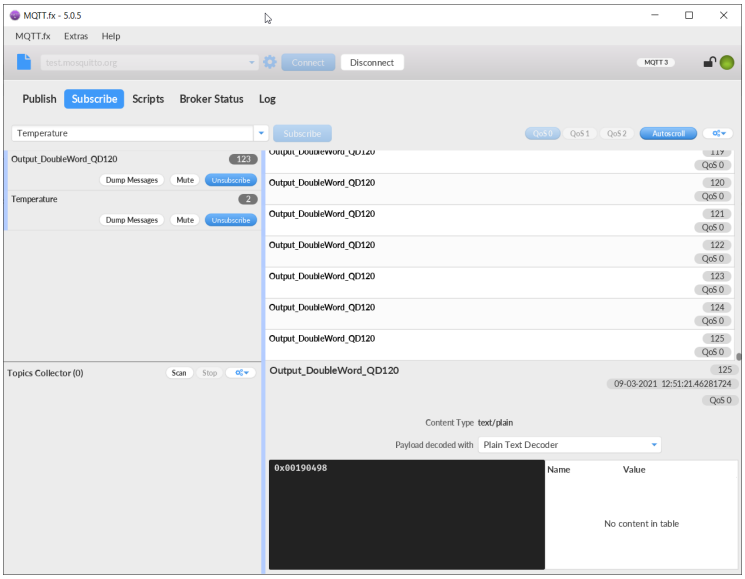


Der „MQTT Explorer“ von Thomas Nordquist (http://mqtt-explorer.com/) ist ein sehr praktisches kleines Tool für Windows, Mac und Linux.

Neben einer aufgeräumten Oberfläche, hierarchischer Darstellung der Topics und der Möglichkeit Werte in Graphen anzuzeigen arbeitet das Programm sehr schnell und ist kompakt.

GitHub:

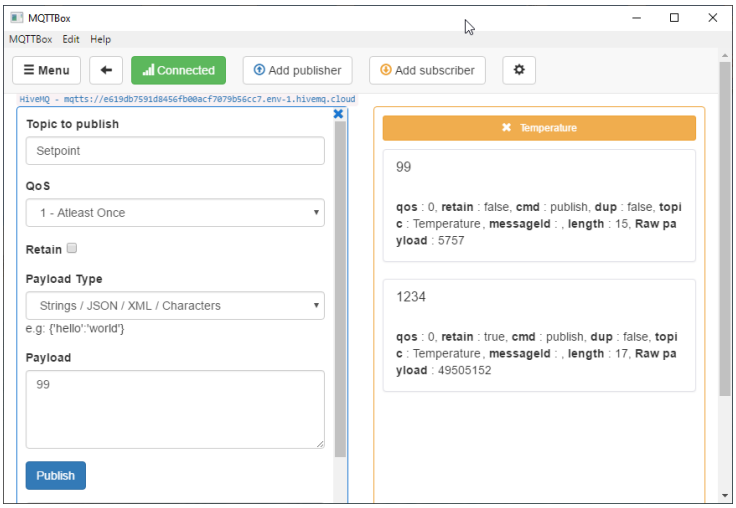
14.2 MQTT.fx V5



MQTT.fx bietet in der kostenpflichtigen Variante ab Version V5 einen sehr umfangreichen Funktionsumfang an.

Insbesondere die erweiterbaren Payload Decoder erleichtern das Testen mit MQTT.

14.3 MQTT Box



MQTT Box (http://workswithweb.com/mqttbox.html) ist als Linux, Macintosh oder Windows APP einfach installierbar.

15 Anwendungsbeispiel „mosquitto“

Eclipse Mosquitto (mosquitto.org) ist ein Open Source MQTT Broker für MQTT V3.1.1 und MQTT V5.

Mosquitto gibt es sowohl für Linux – u.a. für den Raspberry PI – als auch für den PC. Das Mosquitto Projekt enthält auch einen Kommandozeilen MQTT-Client für Tests.

15.1 Mosquitto Test-Host

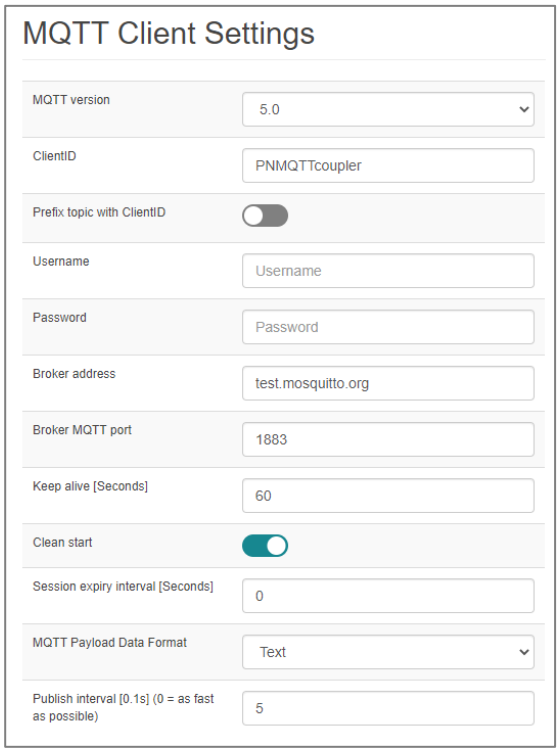
Eclipse Mosquitto betreibt einen Mosquitto Test-Broker unter test.mosquitto.org.

Der Test-Broker kann sowohl mit MQTT V3.1.1 als auch mit MQTT V5 angesprochen werden.

Der Test-Broker kann am einfachsten unverschlüsselt (Port 1883) erreicht werden.

Details zu Verwendung sind auf der Webseite des Mosquitto Test-Brokers erläutert.

Hinweis: Um den Domainnamen des Test-Brokers auflösen zu können, muss bei den IP-Settings ein gültiger DNS-Server angegeben werden!



15.2 Mosquitto lokal installieren und verwenden

Mosquitto kann sowohl unter Linux, auf einem Windows-PC (64-Bit und 32Bit) und auf einem Macintosh laufen. Unter Linux werden die verschiedensten Derivate unterstützt: Raspberry PI, Debian, Ubuntu, usw.

Die entsprechenden Pakete können hier heruntergeladen oder mit einem Paketmanager installiert werden.

16 Anwendungsbeispiel „HiveMQ“

HiveMQ (https://www.hivemq.com) ist ein professioneller, skalierbarer MQTT Broker, der sowohl lokal am PC (Windows oder Linux) läuft, als auch in der Cloud hoch-performant und hochverfügbar nutzbar ist. HiveMQ kann als Broker zwischen der Device-Ebene und den Cloud-anwendungen (AWS, Azure, SAP, etc.) eingesetzt werden.

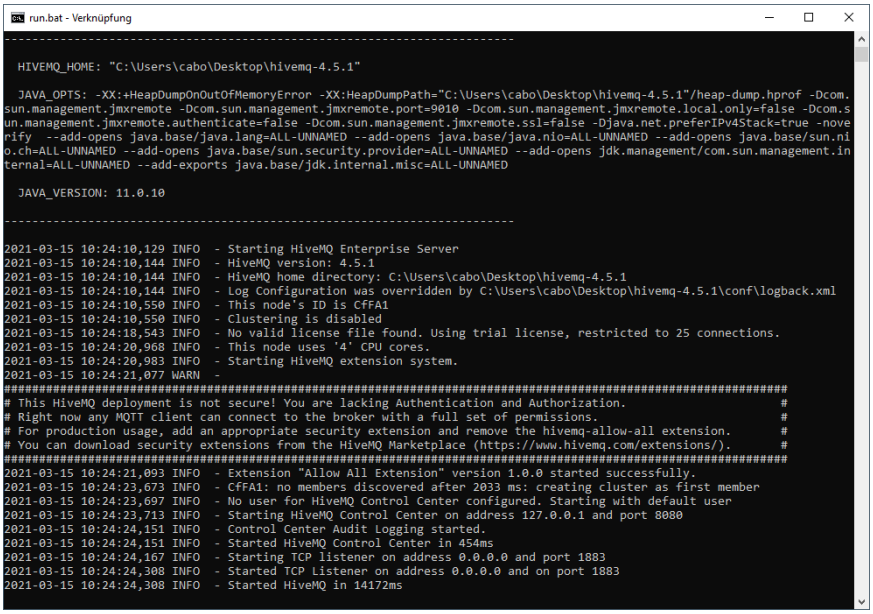
HiveMQ steht in 3 Varianten zur Verfügung: „Community“ (Open Source auf GitHub), „Professional“ und „Enterprise“. Die letzten beiden Versionen können auf eigenen Servern betrieben (on premise) oder als Cloud-Dienst von HiveMQ genutzt werden.

16.1 HiveMQ in einer virtuellen Maschine nutzen

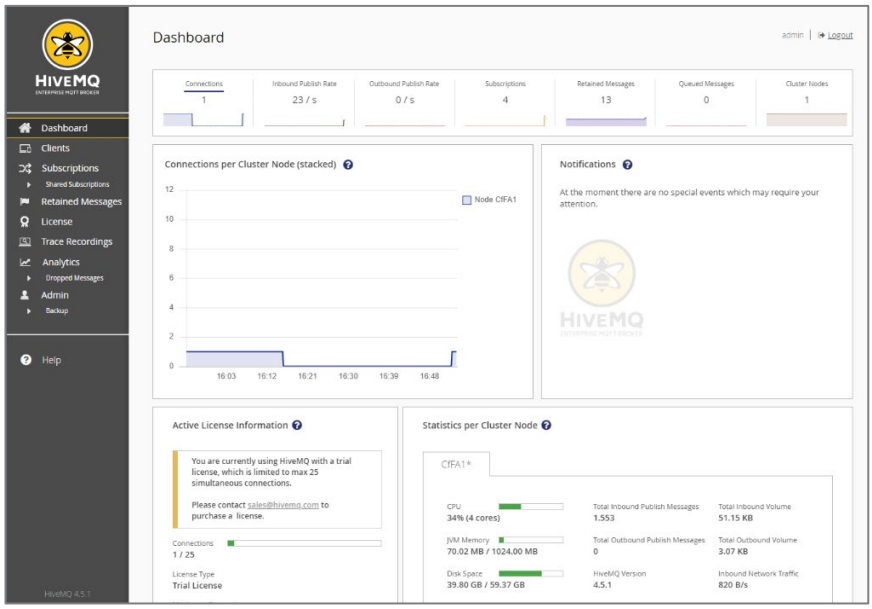
Unter https://www.hivemq.com/downloads/ kann eine „out-of-the-box“ Trial-Version der Enterprise-Version HiveMQ Lösung heruntergeladen und gestartet werden. Die Version kann unter Windows oder Linux gestartet werden. Eine Docker-Version oder eine direkt in AWS startbare Variante ist ebenfalls verfügbar.

Die Trial-Version kann direkt vom PN/MQTT Coupler unter der IP-Adresse des PCs angesprochen werden unter der sie gestartet wurde.

Der MQTT Port 1833 ist aktiv, es wird keine Verschlüsselung oder „user/password“ verwendet.

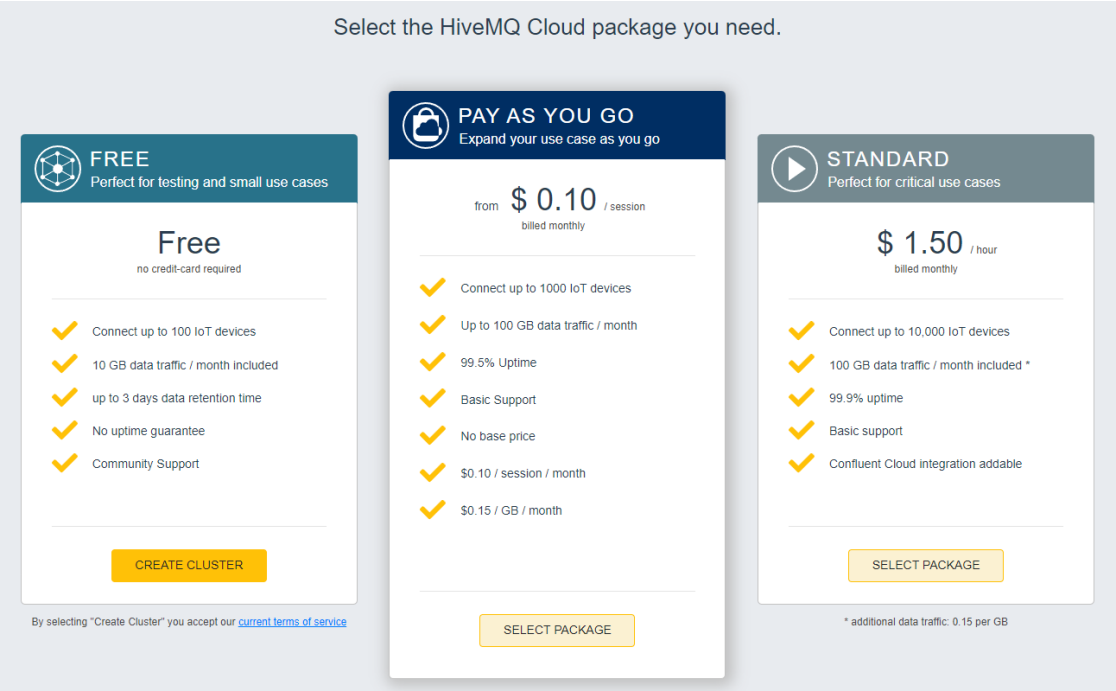


Die Trial-Version enthält auch ein umfangreiche Informations-Webseite.

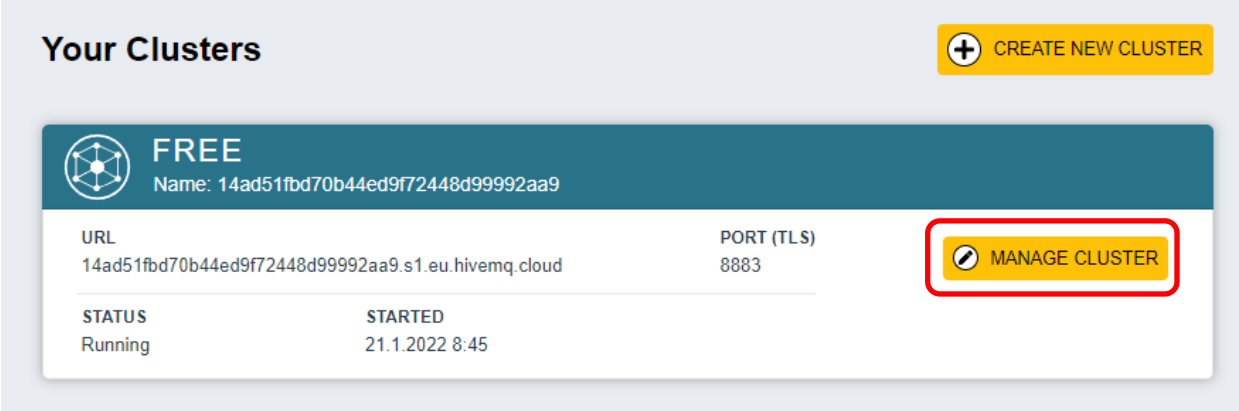


16.2 HiveMQ Cloud

Unter https://www.hivemq.com/cloud/ kann ein Account für die HiveMQ Cloud angelegt werden und eigene „Cluster“ (MQTT Broker) betrieben werden.

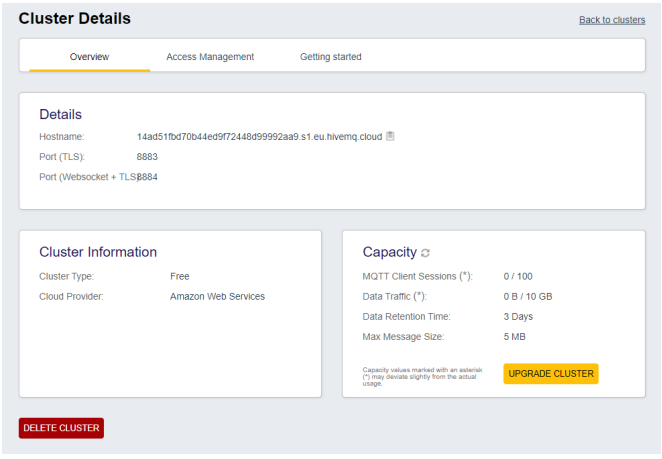


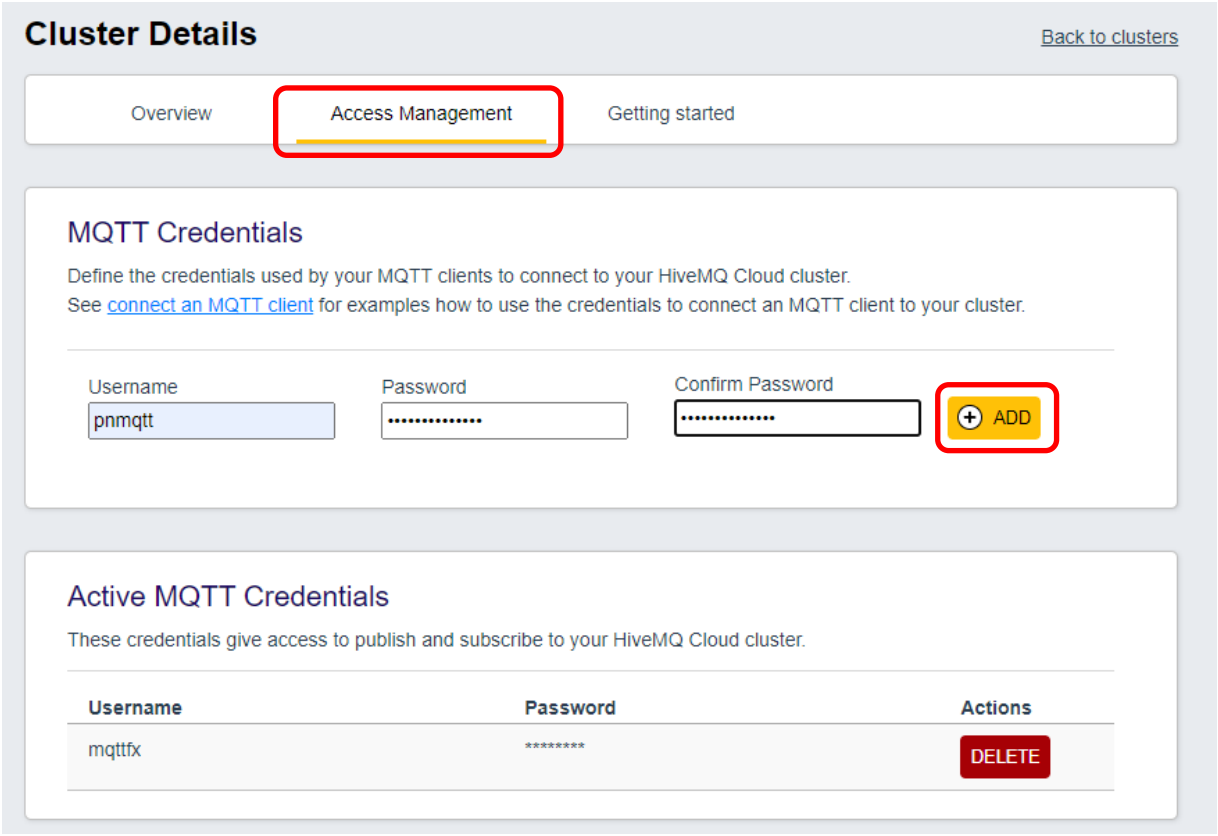
HiveMQ bietet zum Test und für kleine Anwendungsfälle die Einrichtung eines kostenfreien Clusters im Modell „Free“ an. Daneben kann aus zwei kostenpflichtigen Modellen für professionellen Betrieb gewählt werden.



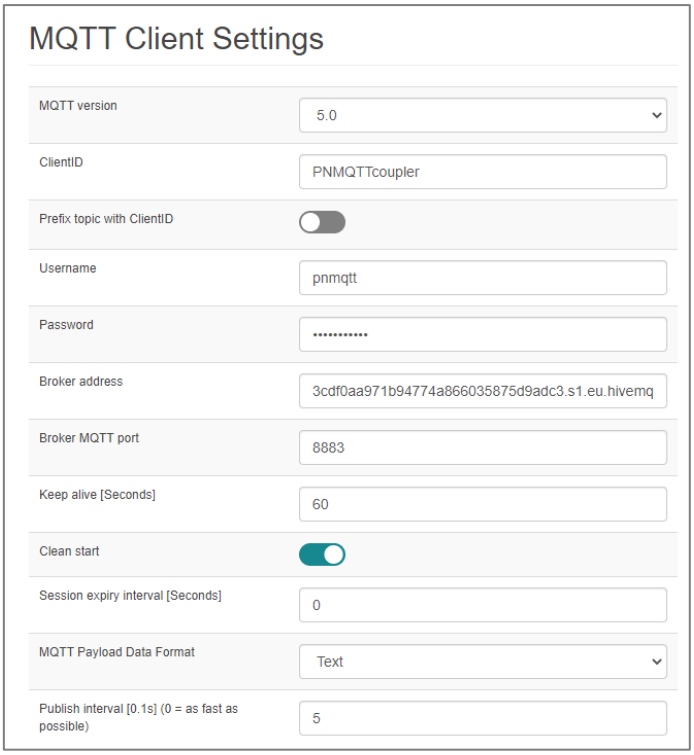
Über „Manage Cluster“ gelangt man zu den „Cluster Details“.

In diesem Dialog ist der Reiter „Access Management“ anzuklicken, und unter „MQTT Credentials“ mit „Add“ einen neuen MQTT Client Zugriff („Username“/ “Password“) anzulegen.





Hiermit sind alle notwendigen Einstellung gemacht und der PN/MQTT Coupler kann auf den HiveMQ Broker zugreifen. Im PN/MQTT Coupler sind nun unter „MQTT Client Settings“ folgende Einstellungen zu übernehmen:



HiveMQ unterstützt sowohl **MQTT Version** 3.1.1 als auch Version 5.

Die **ClientID** kann beliebig sein.

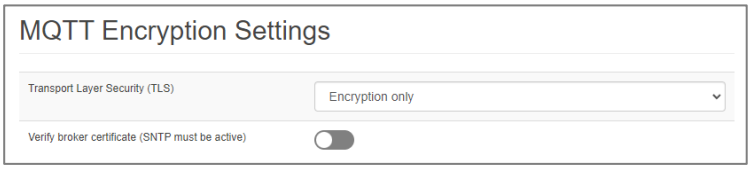
Unter **Username** und **Password** die in den MQTT Credentials eingegeben Werte übernehmen.

Unter **Broker address** die HiveMQ URL kopieren.

Den **Broker Port** auf 8883 stellen.

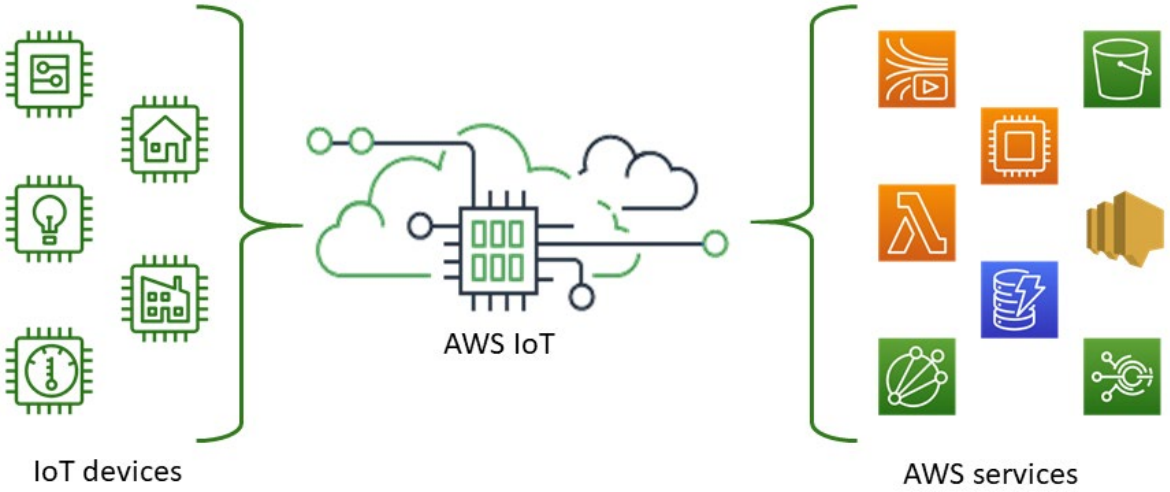
Die restlichen Einstellungen sind beliebig zu wählen.

Transport Layer Security (TLS) sollte auf „Encryption only“ eingestellt werden.

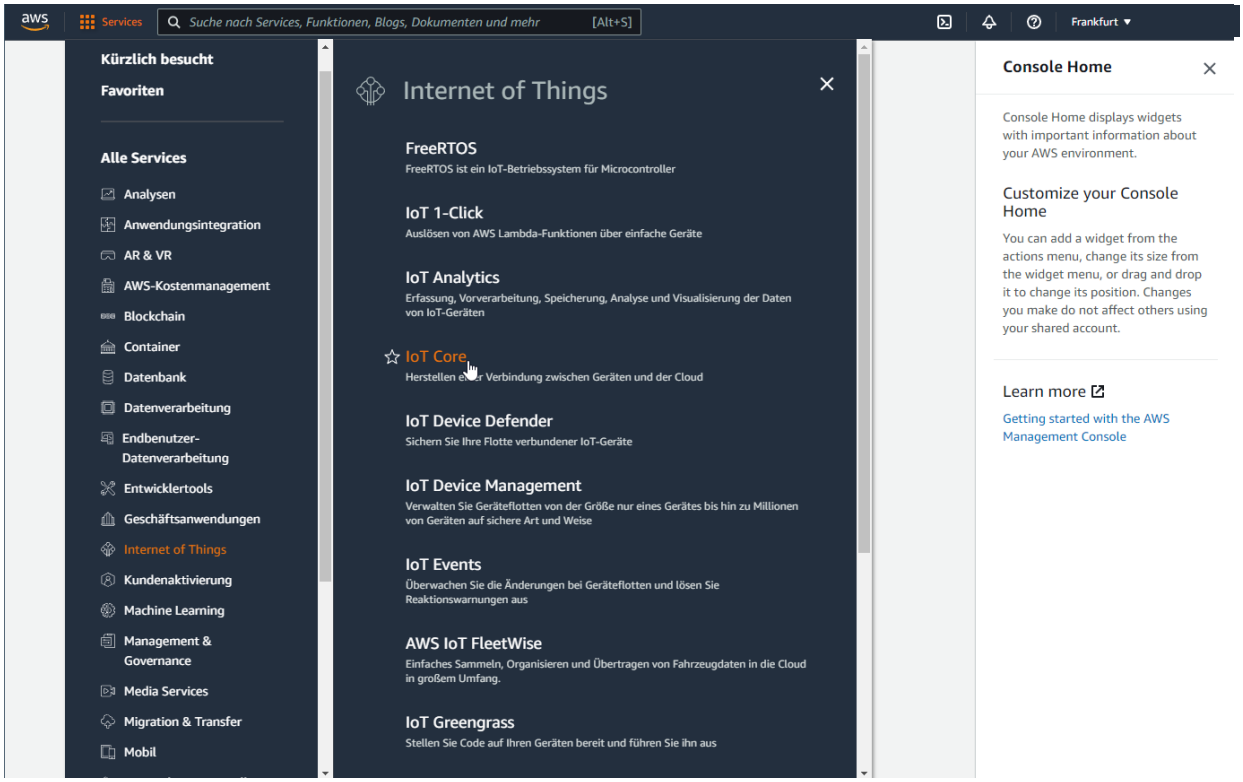


17 Anwendungsbeispiel „Amazon IoT Core“

Mit dem PN/MQTT Coupler können sehr einfach Daten direkt in die Amazon Cloud (AWS) übertragen werden. Die AWS IoT Core Komponente ist ein MQTT-Broker in der AWS Cloud. MQTT Nachrichten können direkt an AWS IoT Core gesendet werden und dann in den anderen AWS Services weiterverarbeitet werden.

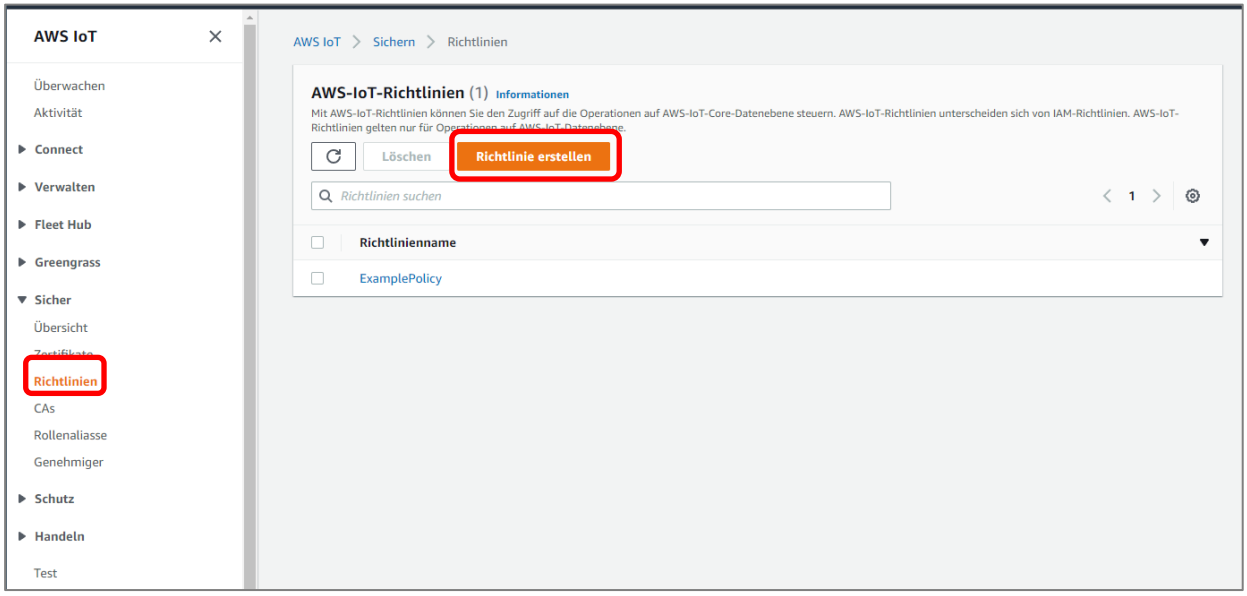


Öffnen Sie in Ihrem AWS Konto das Modul „Internet of Things / IoT Core“.

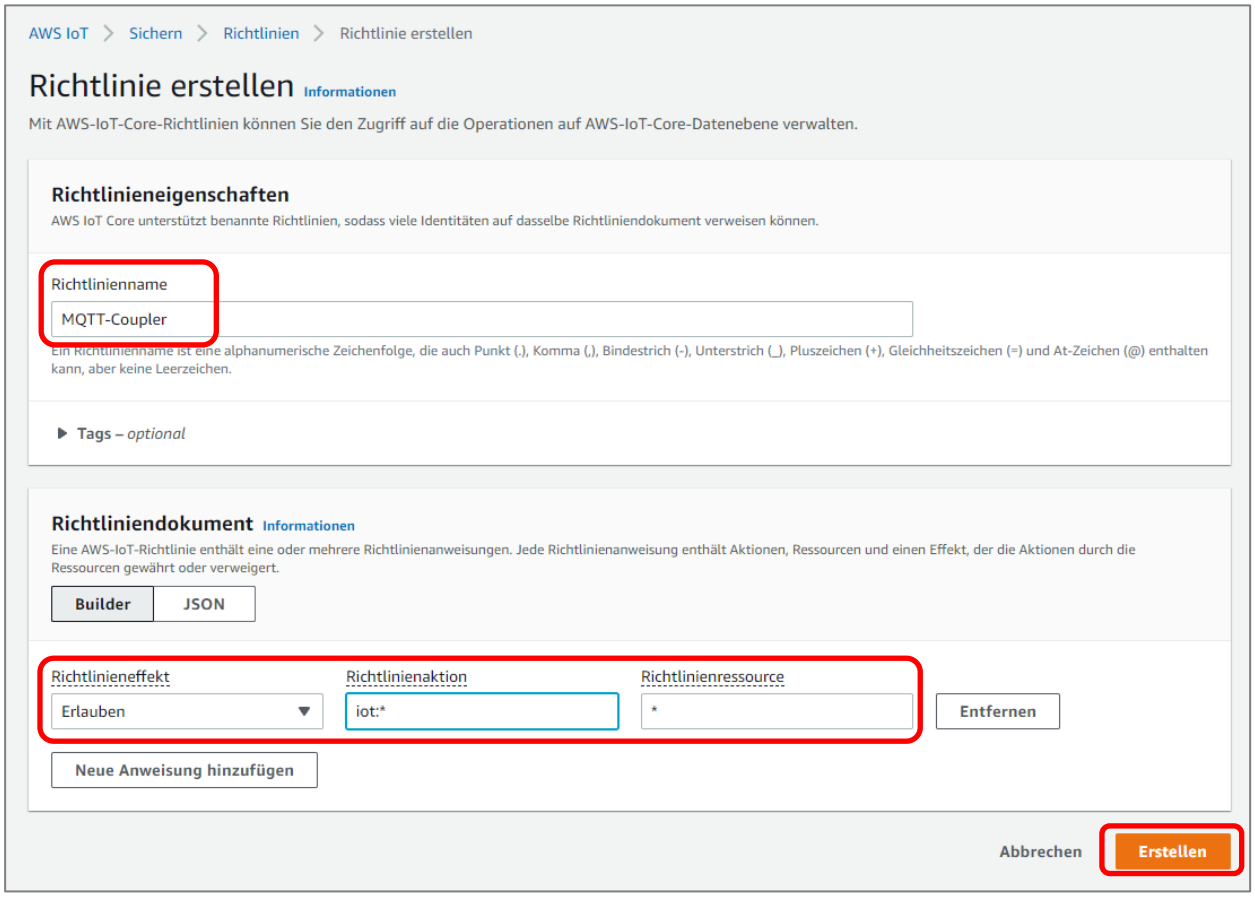


17.1 Policy anlegen

Legen Sie unter „Sicher/Richtlinien“ eine neue Richtlinie (Regelwerk für die Zugriffsrechte) für den PN/MQTT Coupler an und vergeben Sie einen Namen für die Policy.

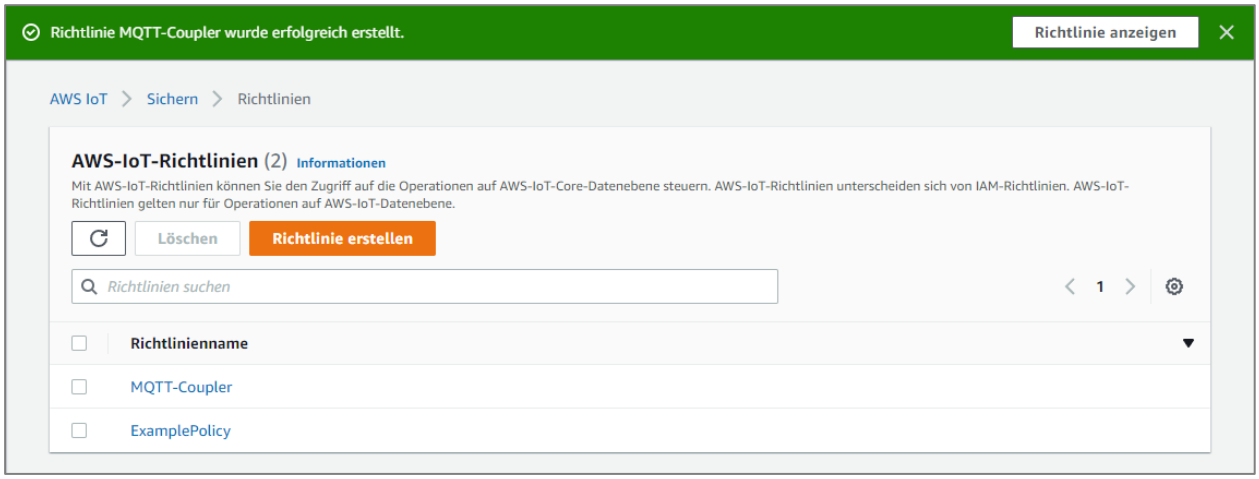


Vergeben Sie der Richtlinie einen Namen, setzen Sie bei „Richtlinieneffekt“ den Haken „Erlauben“, geben bei Richtlinienaktion „iot:*“ ein und bei Richtlinienressource „*“.



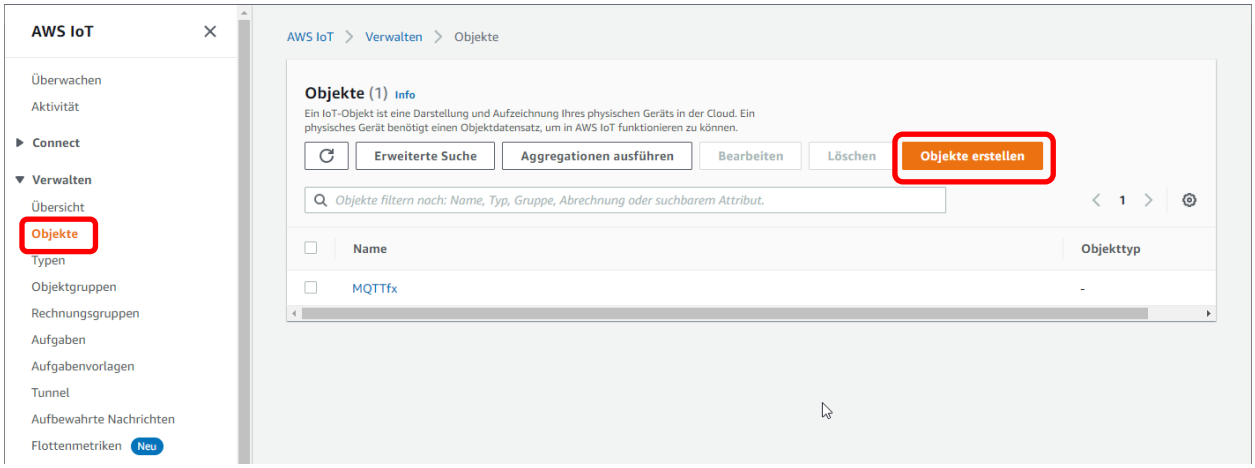
Damit haben Sie vollen Zugriff auf „Subscriptions“ und „Publikationen“ (kann später angepasst werden).

Die Richtlinie wird mit „Erstellen“ (rechts unten) angelegt und erscheint in der Übersicht.

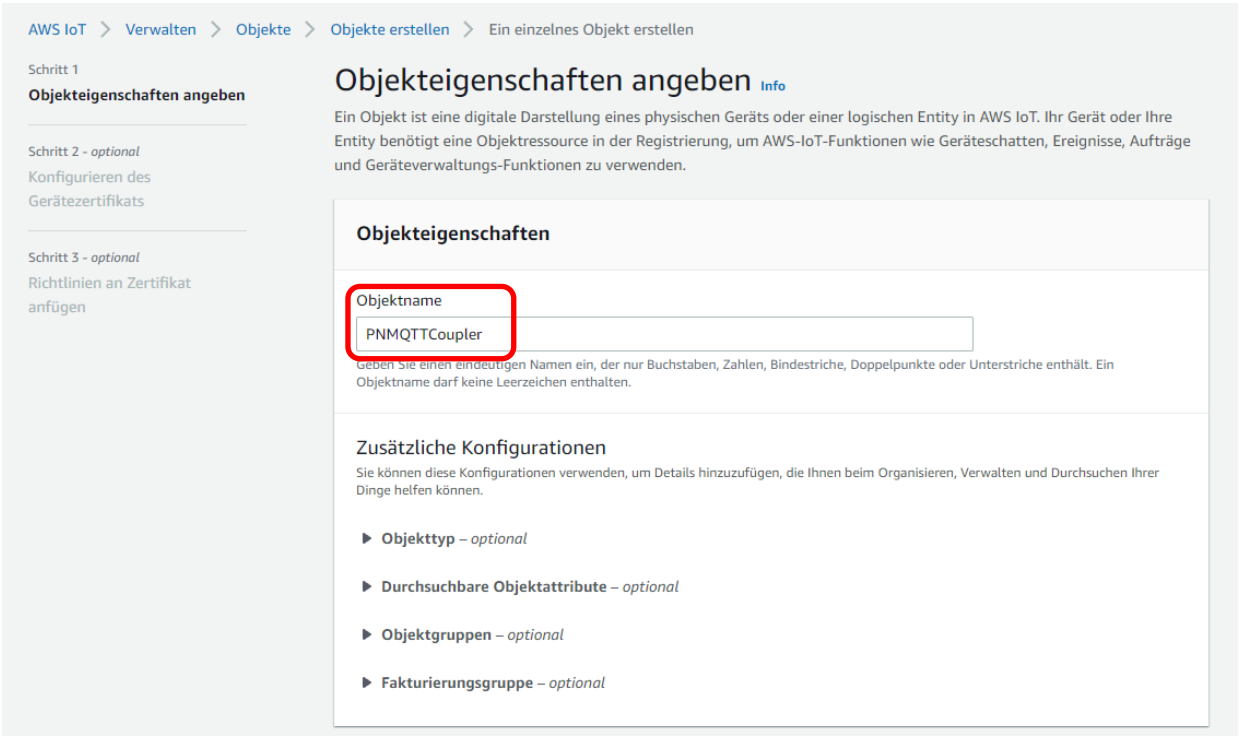


17.2 Erstellen eines „Objekts“

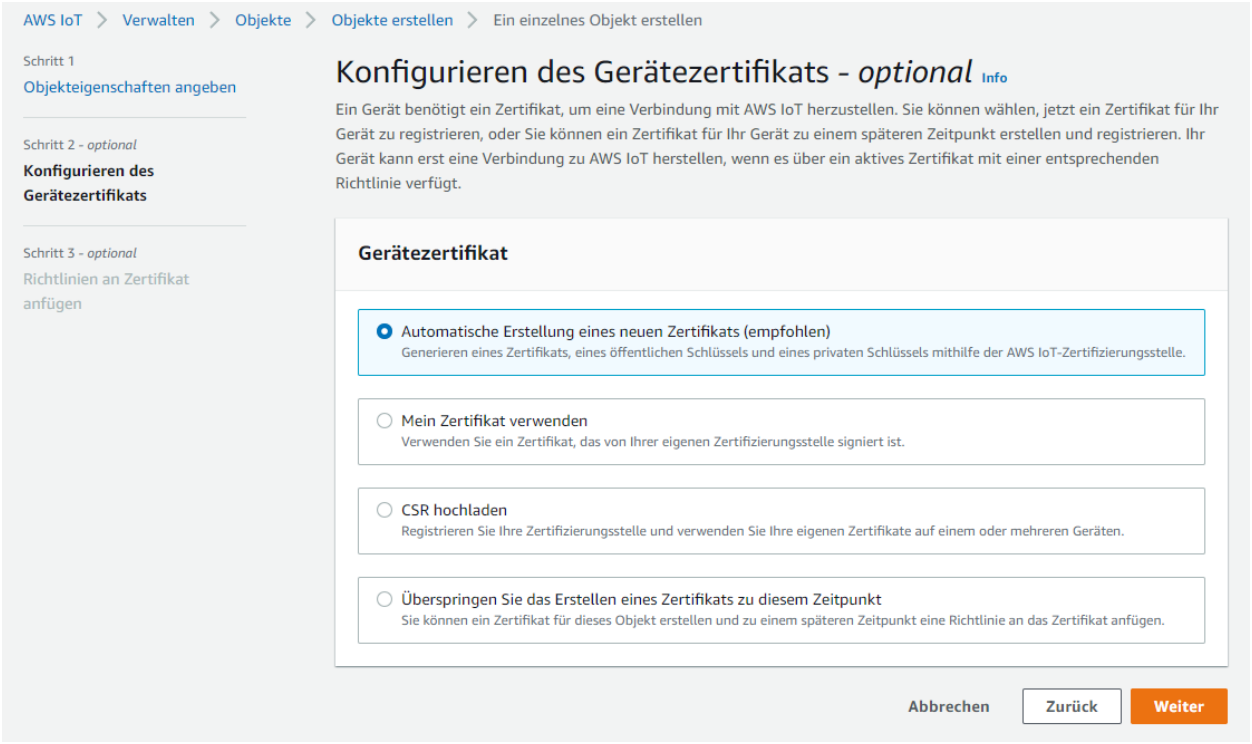
Wählen Sie unter „Verwalten/Objekte“ die Funktion „Objekt erstellen“ aus.



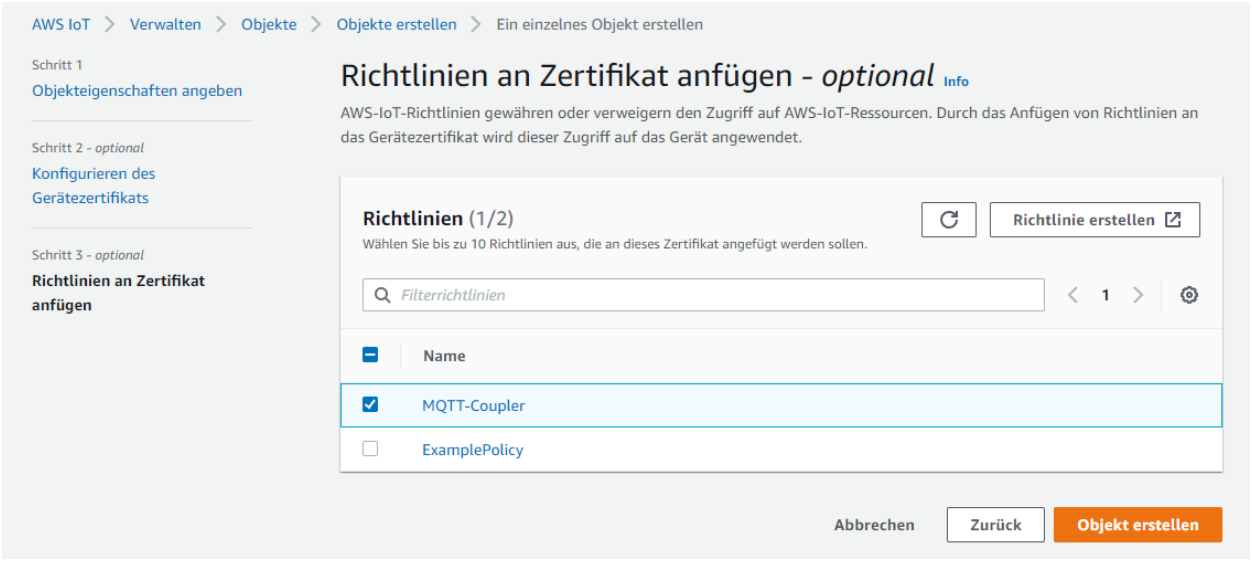
Geben Sie dem Objekt einen Namen.



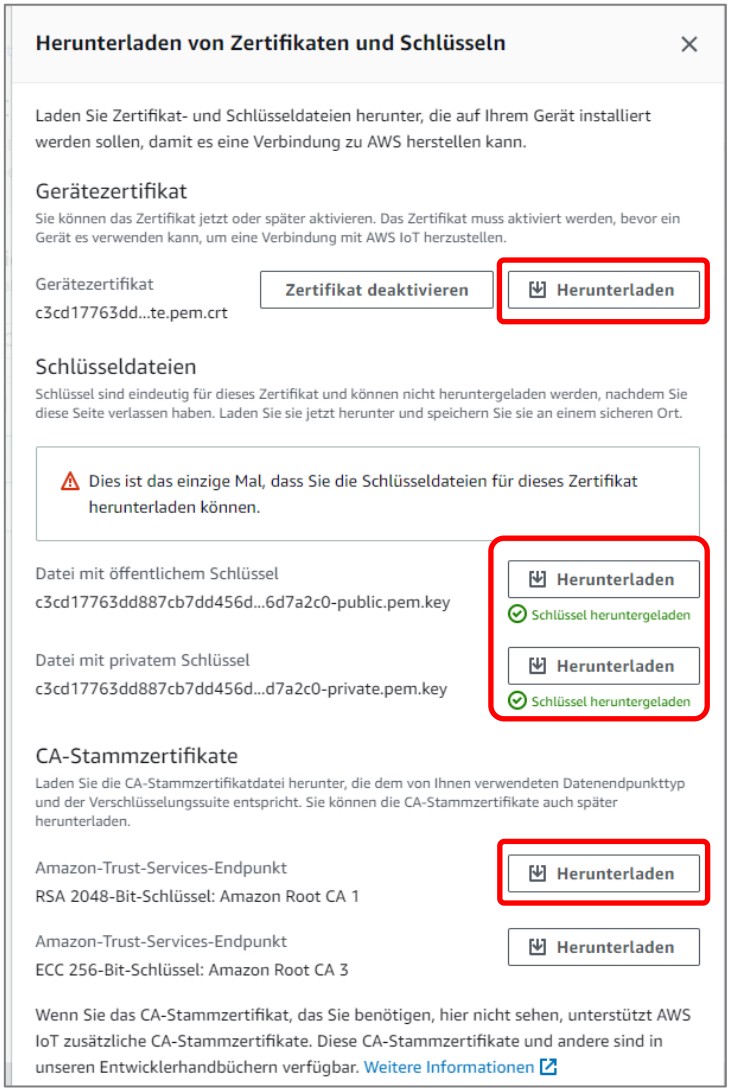
Für das Objekt können nun die Gerätezertifikate erstellt werden.



Mit dem erstellten Zertifikat des Objektes wird nun die oben angelegte Richtlinie verbunden, um dem Objekt die notwendigen Zugriffsrechte zu geben.

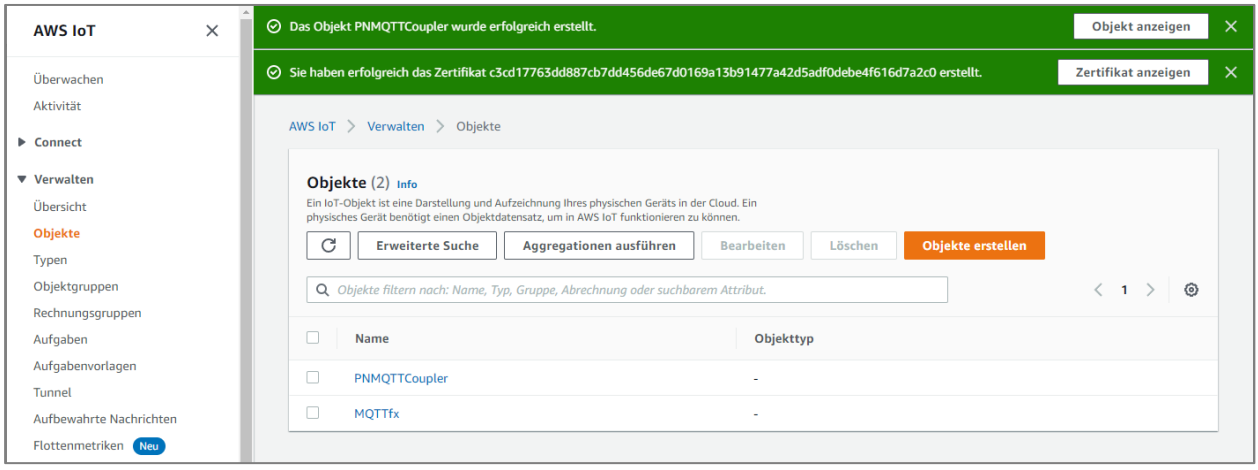


Laden Sie das „Gerätezertifikat“ und die „Schlüsseldateien“ herunter und bewahren Sie diese an einem sicheren Ort auf. Die Schlüsseldateien können nicht nochmal heruntergeladen werden.

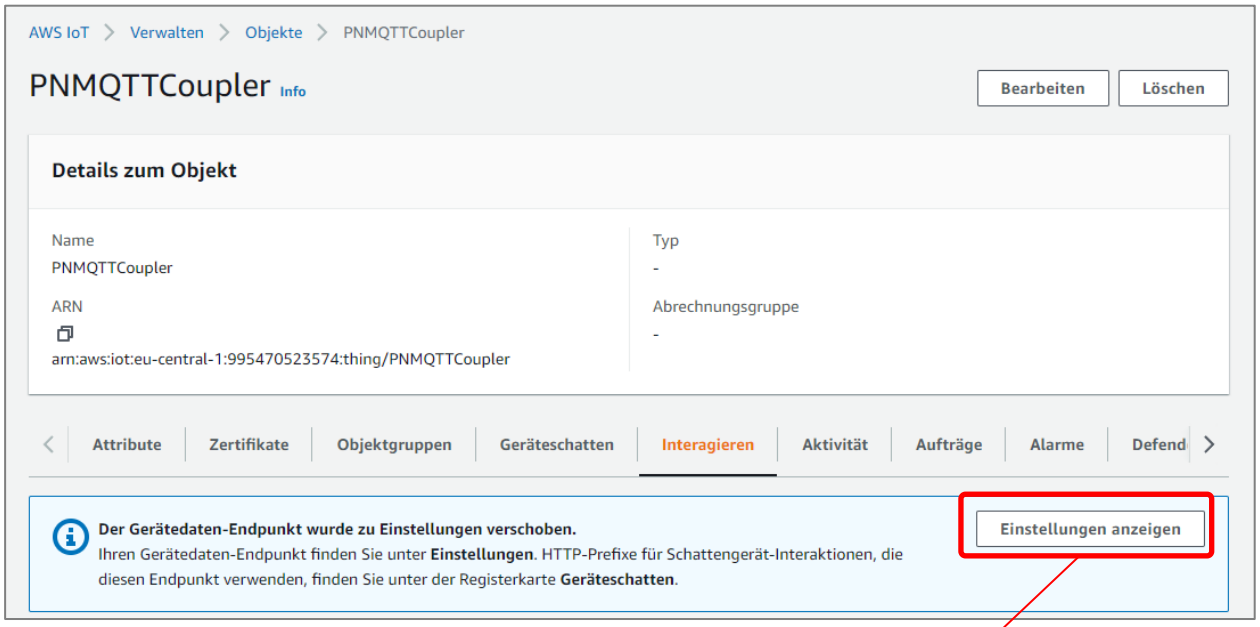


Laden Sie zusätzlich noch das Root Zertifikat („root CA“) von AWS herunter. Für dieses Anwendungsbeispiel verwenden Sie den „RSA 2048-Bit-Schlüssel: Amazon Root CA 1“.

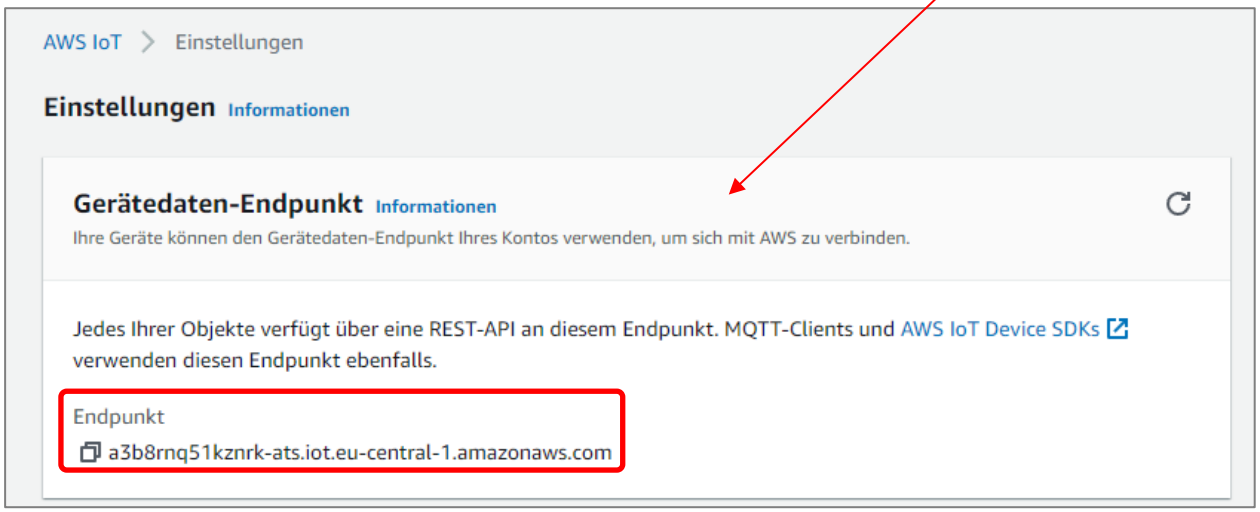
Das Objekt für den PN/MQTT Coupler ist nun erstellt und wir haben das Zertifikat und die Schlüsseldateien heruntergeladen, welche wir gleich in den PN/MQTT Coupler einspielen werden.



Zum Schluss benötigen wir noch die Adresse des Gerätedaten-Endpunktes. Wählen Sie das eben angelegte Objekt an und gehen in den Reiter „Interagieren“.



Mit „Einstellungen anzeigen“ kommen Sie zum Gerätedaten-Endpunkt.



Kopieren sie die Endpunkt Adresse.

17.3 PN/MQTT Coupler für den AWS Zugriff konfigurieren

Konfigurieren Sie den PN/MQTT Coupler im PROFINET Engineering Tool (z.B. TIA Portal) wie im Kapitel 7 beschrieben. Beachten Sie beim Parametrieren der MQTT Topic-Module, dass AWS nur QoS ‚0' und ‚1' unterstützt und bei den Publisher Modulen kein „Retain"-Flag gesetzt werden darf!

ACHTUNG AWS IoT Core hat einige Einschränkungen bei den MQTT-Nachrichten:

1. Das „Retain-Flag" darf nicht verwendet werden!
2. „QoS 2" kann mit AWS nicht verwendet werden!
3. „Keep-alive" muss zwischen 30 und 1200 Sekunden liegen!

Für die Verbindung mit AWS IoT Core ist zwingend ein Gateway und ein DNS-Server in den IP Settings anzugeben.

Auf der Webseite des PN/MQTT Coupler müssen nun im Menü „MQTT" unter „MQTT Client Settings" folgende Einstellungen durchgeführt werden:

AWS IoT Core unterstützt aktuell nur **MQTT Version 3.1.1**.

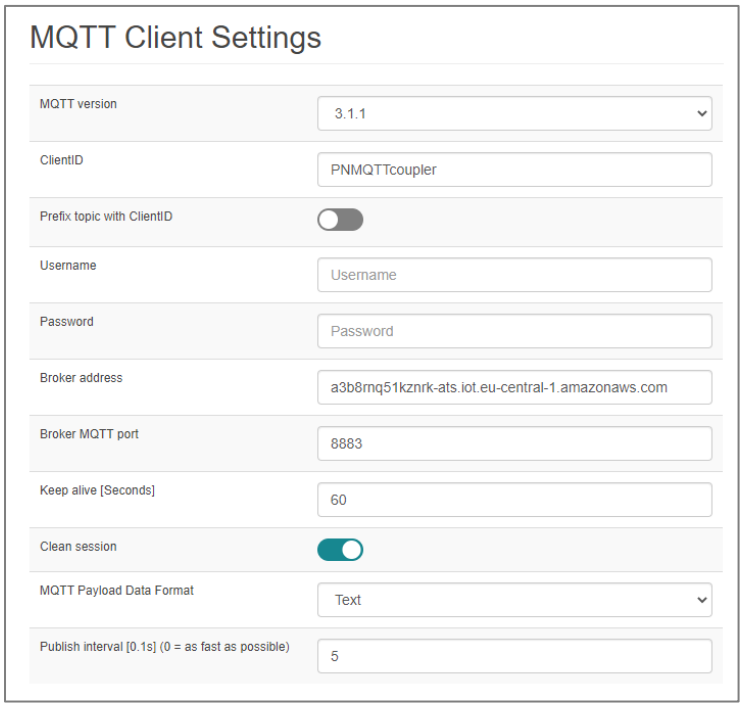
Die **ClientID** kann beliebig sein.

Username und **Password** werden nicht benötigt.

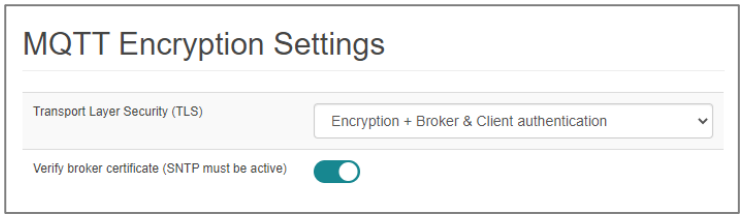
Unter **Broker address** muss die auf der vorherigen Seite kopierte Endpoint-URL eingefügt werden.

Der **Broker port** muss auf 8883 gestellt.

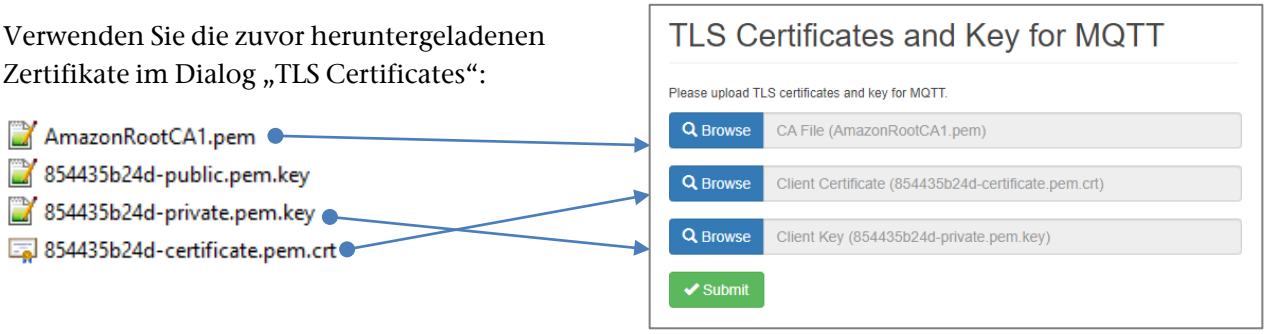
Keep alive muss für AWS zwischen 30 und 1200 Sekunden eingestellt werden.



Transport Layer Security (TLS) muss auf „Encryption +Broker & Client authentication" eingestellt werden.



Verwenden Sie die zuvor heruntergeladenen Zertifikate im Dialog „TLS Certificates":



Für das CA-File verwenden Sie die „AmazonRootCA1.pem“ Datei.

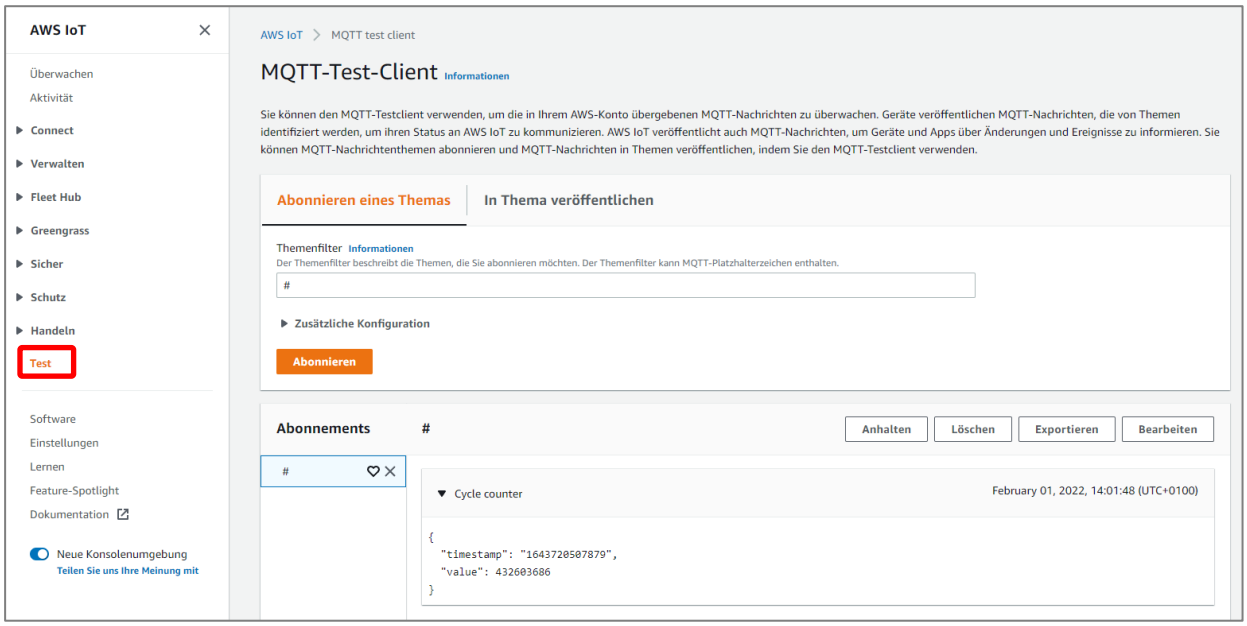
Das Client Certificate ist die „xxx-certificate.pem.crt“ Datei, sie enthält sowohl das Zertifikat als auch den Public Key des Clients.

Als letztes benötigen Sie noch den private Key des Clients („xxx-private.pem.key“).

Damit ist die Konfiguration abgeschlossen und der PN/MQTT Coupler sollte mit der AWS IoT Core Verbindung aufnehmen.

17.4 Testen der MQTT Verbindung in AWS

Um zu prüfen, ob der Datenaustausch mit dem PN/MQTT Coupler über MQTT funktioniert, kann MQTT Test-Client im AWS IoT Core aufgerufen werden. Wählen Sie links im Menü „Handeln/Test“.



In dem folgenden Dialog könne Sie unter „Abonnieren eines Themas“ die Anzeige eines vom PN/MQTT Coupler gesendeten Topics aktivieren und unter „In Thema veröffentlichen“ Daten an den PN/MQTT Coupler senden.

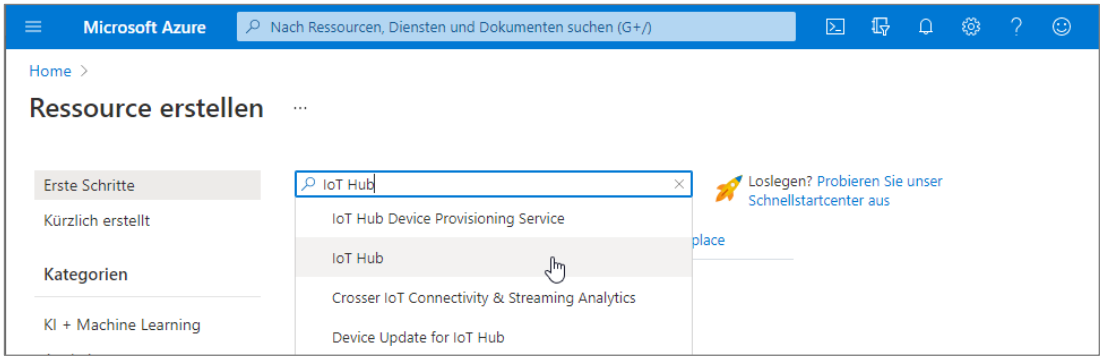
Ist der Test erfolgreich, so ist die Konfiguration abgeschlossen!

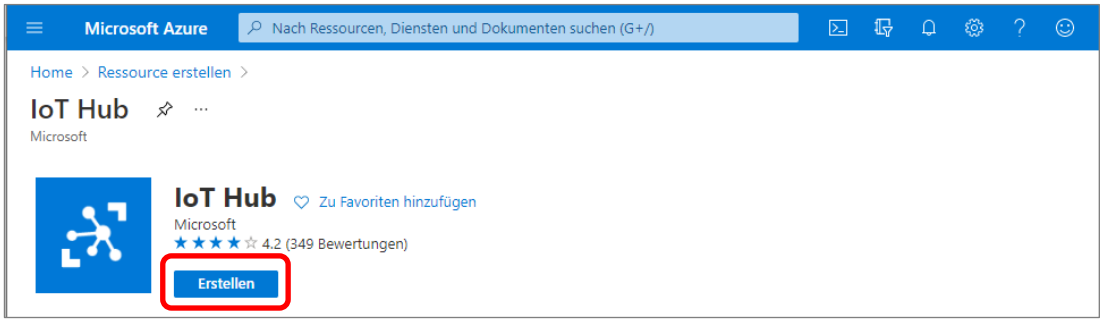
ACHTUNG Für die Verbindung mit Amazon AWS ist zwingend ein Gateway und ein DNS-Server in den IP Settings anzugeben. Zur Prüfung der Aktualität der Zertifikate ist die Uhrzeitsynchronisierung per SNTP zu aktivieren.

18 Anwendungsbeispiel „Microsoft Azure“

18.1 Gerät in Azure anlegen

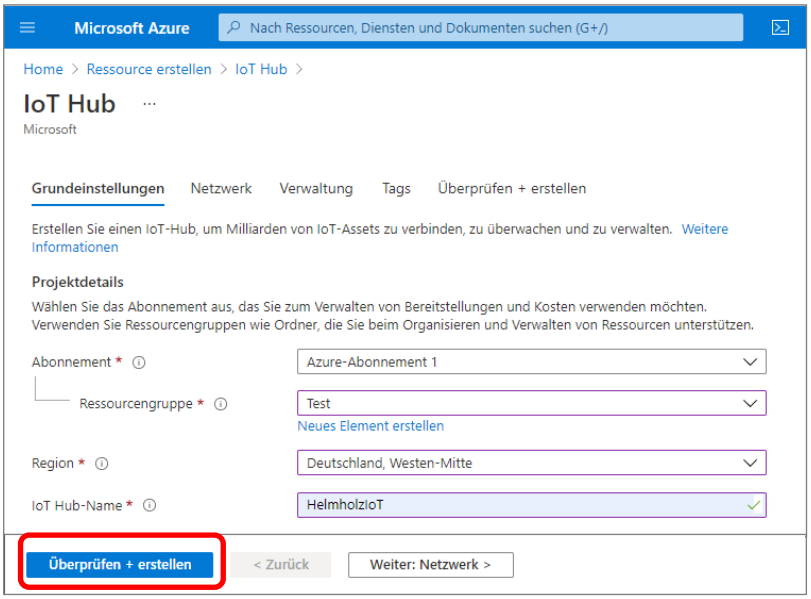
Unter Microsoft Azure muss zuerst ein IoT Hub angelegt werden.





Wählen Sie ein passendes Abonnement. Bei einem neuen AWS Account kann ggf. die „Kostenlose Testversion“ genutzt werden.

Der IoT Hub-Name kann beliebig gewählt werden.

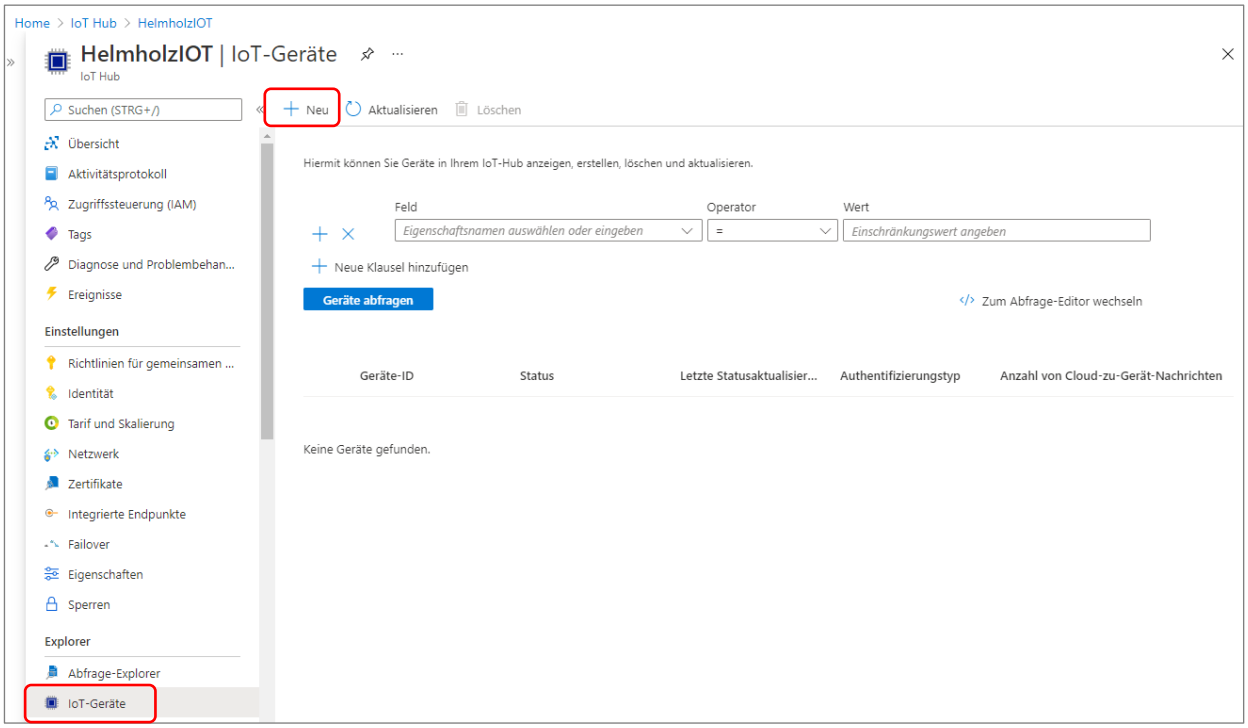


Im nächsten Dialog können die Angaben nochmal überprüft werden und mit „Erstellen“ wird die Bereitstellung der IoT Hub Komponente in Azure gestartet.

Die Bereitstellung kann ein paar Minuten dauern.

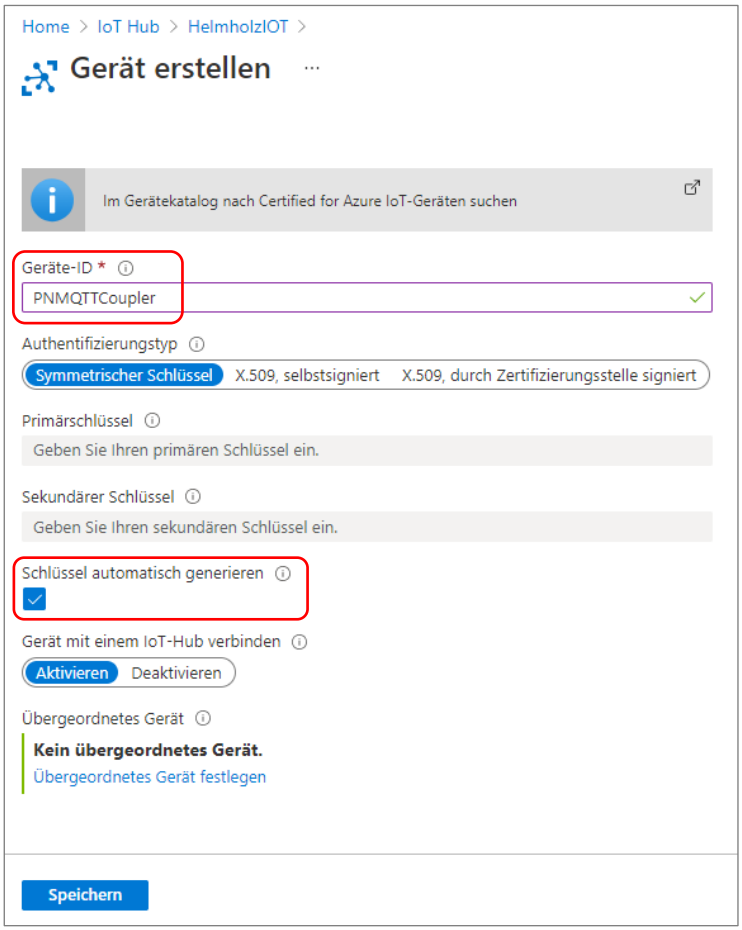
Wählen Sie dann den neu erstellten IoT Hub aus.

Im Menü Baum links unten „IoT-Geräte“ auswählen und oben mit „Neu“ ein neues Gerät anlegen.

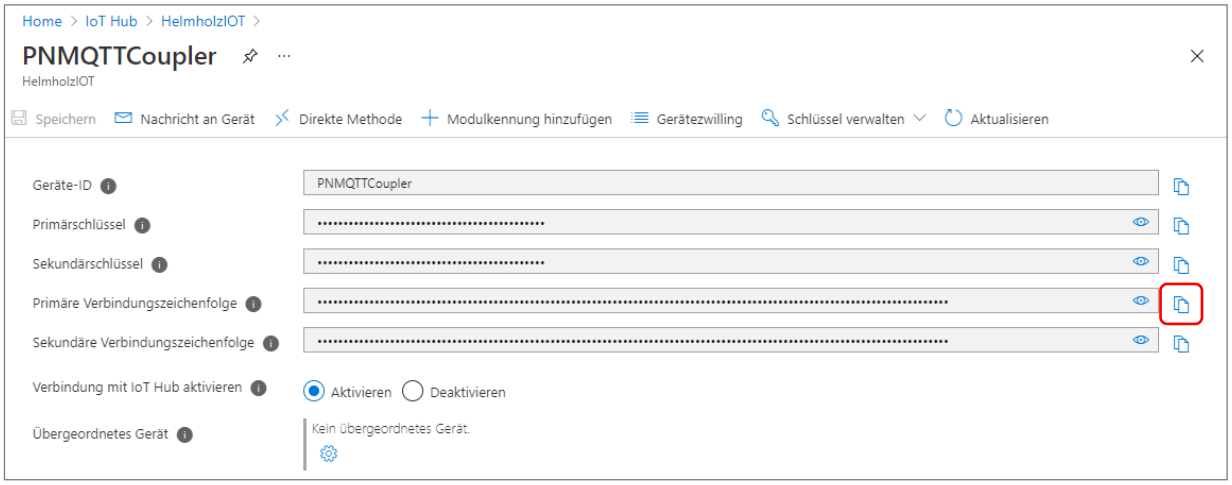


Im folgenden Dialog kann man dem Gerät eine Geräte-ID geben.

Die anderen Einstellungen können unverändert übernommen werden, wichtig sind die Optionen“ Symmetrischer Schlüssel“ und Schlüssel automatisch generieren.



Wählen Sie das Gerät an.

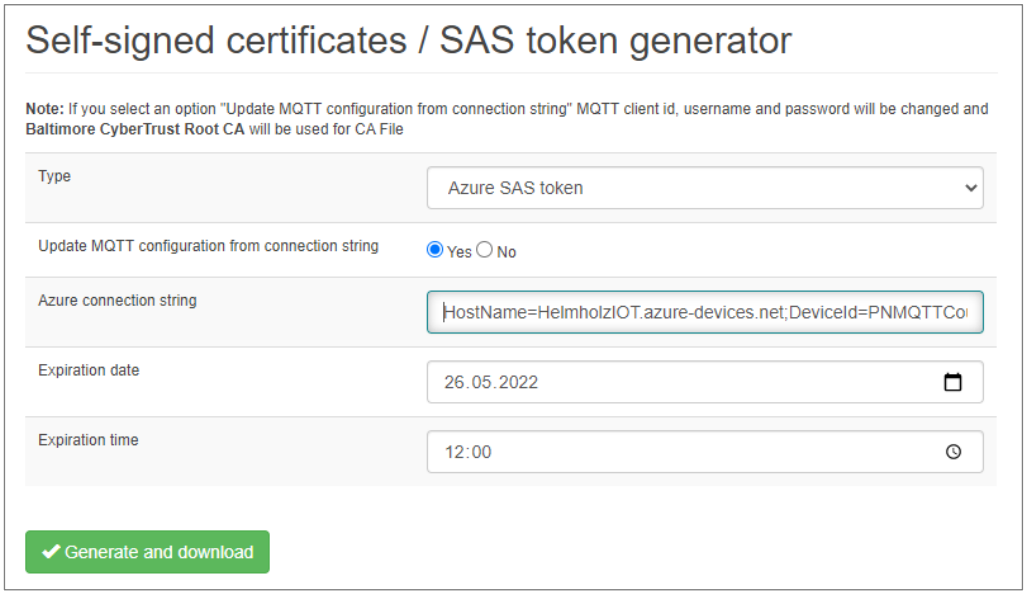


Kopieren Sie die „Primäre Verbindungszeichenfolge“ in die Zwischenablage.

18.2 PN/MQTT-Coupler für Azure konfigurieren

Der PN/MQTT-Coupler muss über PROFINET bereits konfiguriert sein und auf der MQTT Netzwerkseite eine IP-Adresse haben und Verbindung mit dem Internet aufbauen können (Gateway und DNS-Server sind verfügbar).

Als erstes muss im PN/MQTT Coupler im Menü „MQTT“ unter „MQTT Encryption“ ein „Azure SAS Token“ für den Coupler erstellt werden.

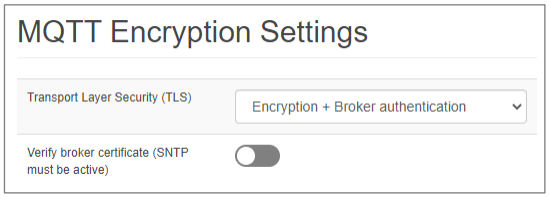


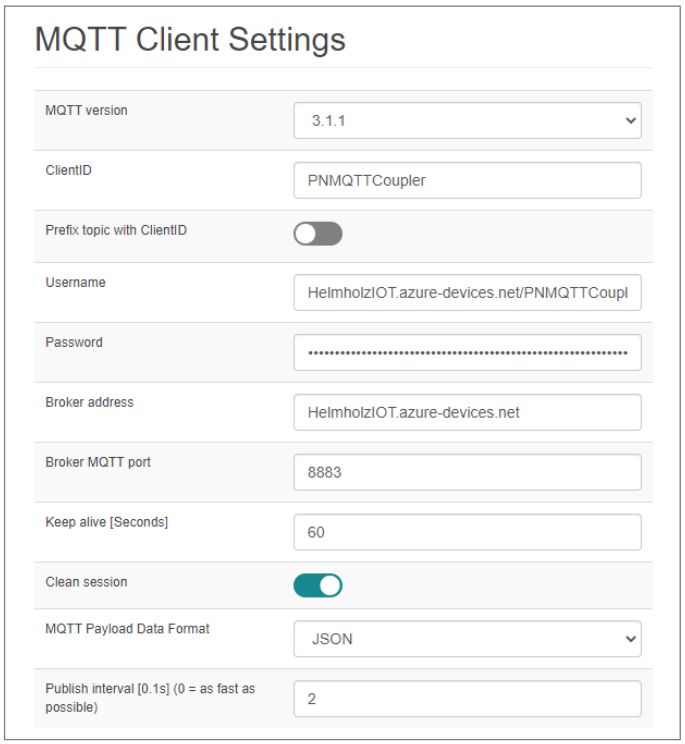
Als „Azure connection string“ muss die „Primäre Verbindungszeichenfolge“ aus der Zwischenablage (siehe vorherige Seite) eingetragen werden. Als „Expiration date“ und „Expiration time“ muss eine Zeit in der Zukunft eingetragen werden.

Mit „Update MQTT configuration from connection string“ werden die Verbindungseinstellungen automatisch in die „MQTT Settings“ übernommen. Dazu gehören „Username“, „Password“ und die „Broker address“.

Überprüfen Sie in den „MQTT Client Settings“ die restlichen Einstellungen, wie rechts angezeigt. Als Broker Port muss 8883 eingestellt sein.

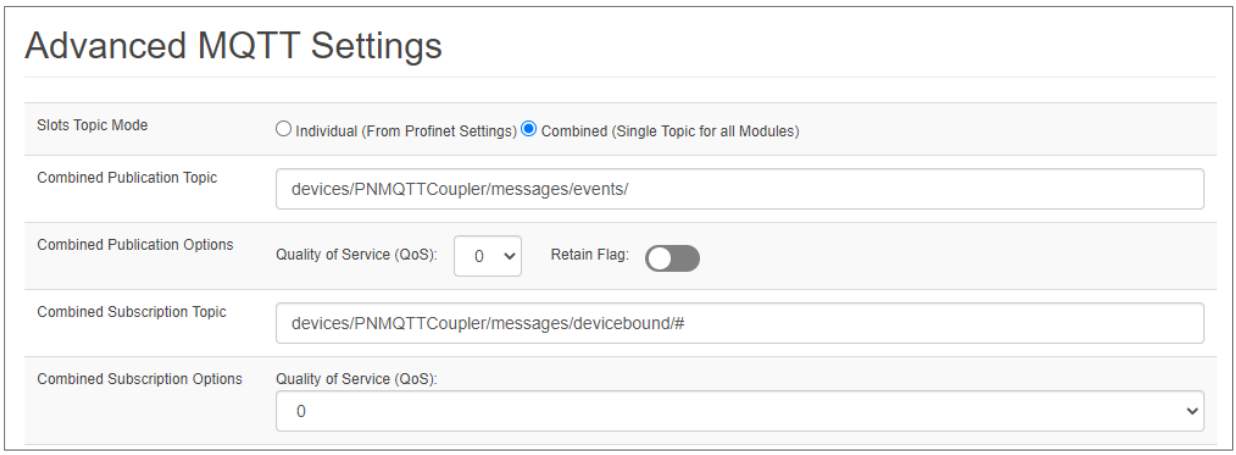
Die MQTT Encryption muss auf „Encryption + Broker authentication“ eingestellt sein.





Da Microsoft Azure von jedem Gerät nur ein zentrales Topic empfangen kann, müssen alle konfigurierten Werte aus der SPS in einem kombiniertes Topic zusammen gesendet werden.

Wählen Sie „MQTT / Advanced MQTT settings“ und überprüfen Sie, ob der „Combined Topic mode“ aktiviert ist.



Das „Combined Publication Topic“ muss für Microsoft Azure auf folgendes Format eingestellt werden:

```
devices/<Geräte-ID>/messages/events/
```

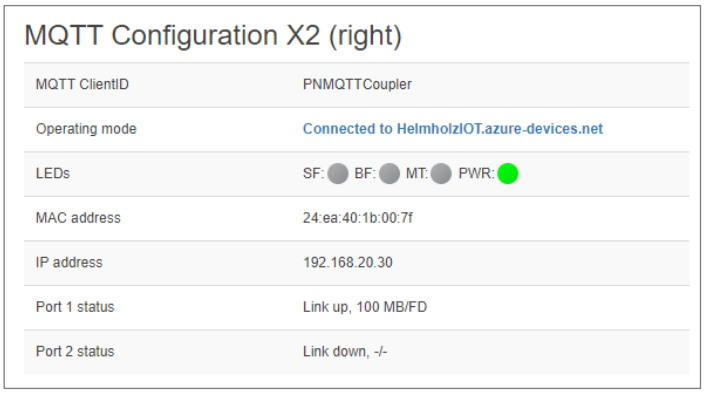
Das „Combine Subscription Topic“ muss für Microsoft Azure auf folgendes Format eingestellt werden:

```
devices/<Geräte-ID>/messages/devicebound/#
```

Die *Geräte-ID* des in Azure angelegten Gerätes muss hier korrekt angegeben werden, z.B.:

```
devices/PNMQTTCoupler/messages/events/
```

Sind alle Einstellungen korrekt, so sollte der PN/MQTT Coupler die Verbindung zu Microsoft Azure selbstständig aufbauen.



ACHTUNG Microsoft Azure hat einige Einschränkungen:

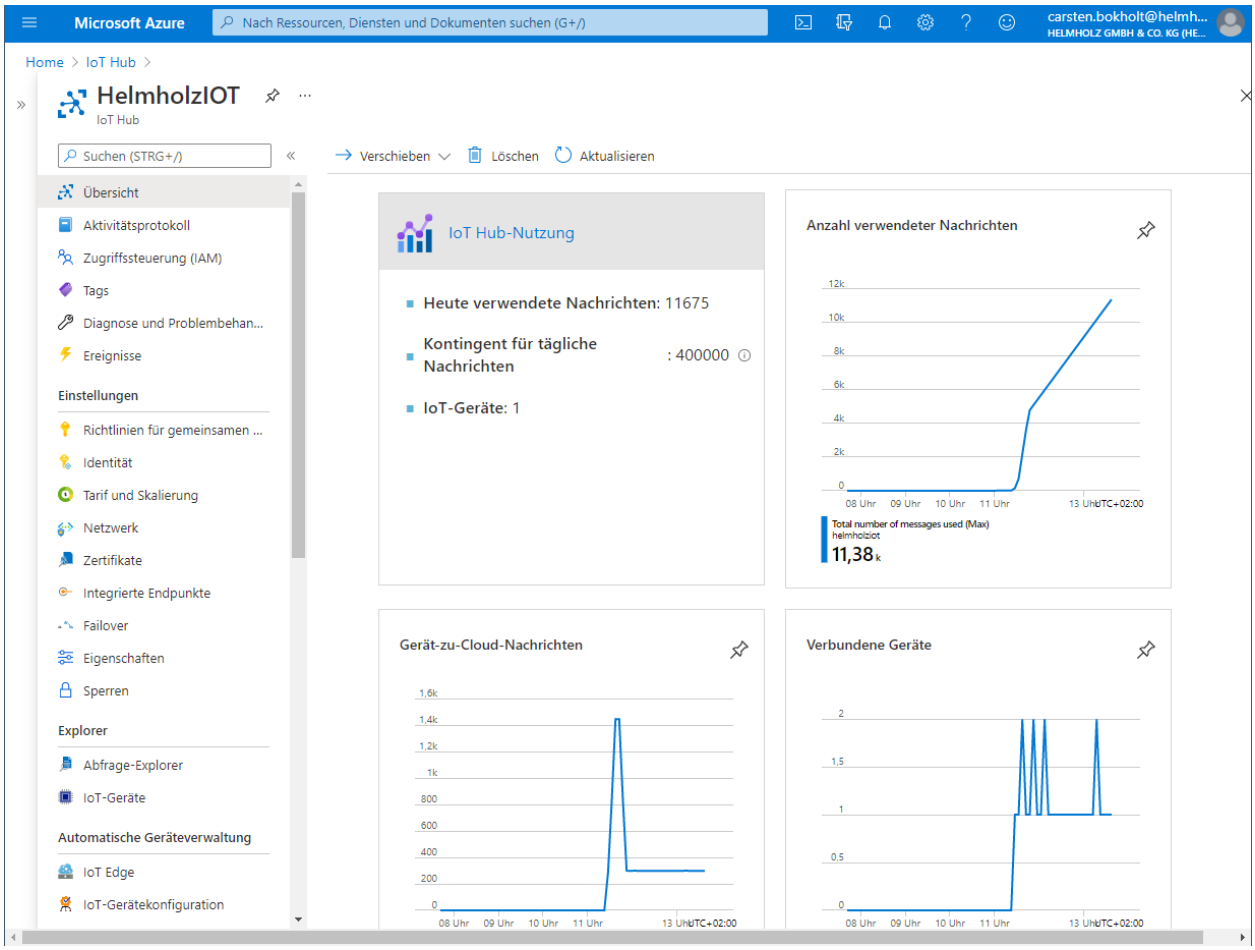
1. Das „Retain-Flag“ darf nicht verwendet werden!
2. „QoS = 2“ kann mit Azure nicht verwendet werden!
3. Keep Alive ist auf maximal 19 min beschränkt (1140 Sekunden).
4. „Communication enable“ & „Communication stopped“ Nachrichten dürfen nicht verwendet werden.

Für die Verbindung mit Microsoft Azure ist zwingend ein Gateway und ein DNS-Server in den IP Settings anzugeben.

Zur Prüfung der Aktualität der Zertifikate ist die Uhrzeitsynchronisierung per SNTP zu aktivieren.

18.3 Prüfen der Datenübertragung in Microsoft Azure

Ob eine aktive Verbindung des PN/MQTT Coupler mit dem IoT Hub besteht kann man in der IoT Hub Übersicht unter „IoT Hub Nutzung“ sehen. Dort werden die aktiven Verbindungen und die Anzahl der verwendeten Nachrichten angezeigt.

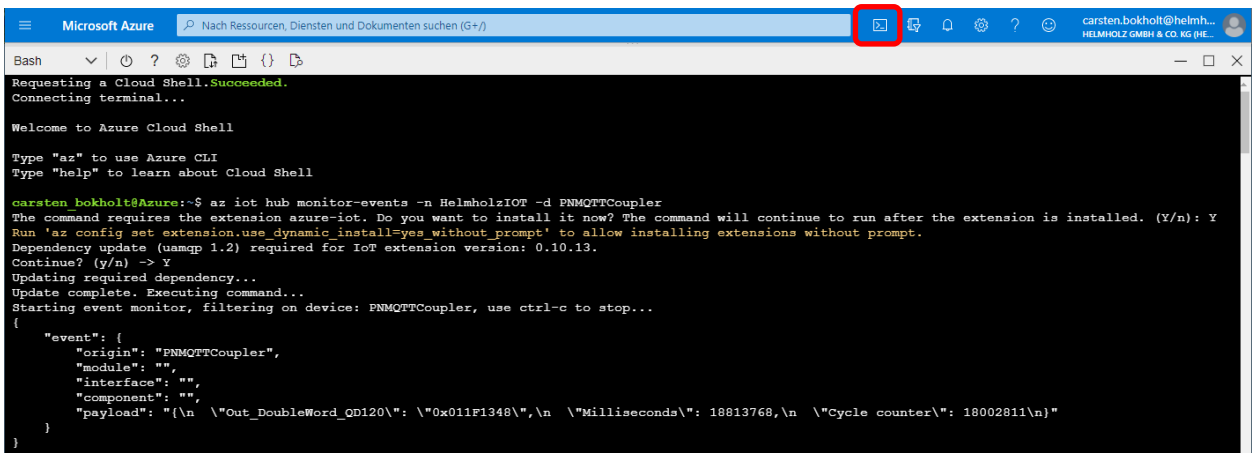


Zusätzlich kann man sich die empfangenen Nachrichten in der Azure Console anschauen. Das folgende Kommando startet das MQTT Event Monitoring:

```
az iot hub monitor-events -n <Hub-Name> -d <Geräte-ID>
```

z.B.:

```
az iot hub monitor-events -n HelmholzIOT -d PNMQTTCoupler
```



19 Technische Daten

Artikelnummer	**700-162-3MQ02**
Name	PN/MQTT Coupler
PROFINET-Schnittstelle	
Anschluss	2x RJ45, integrierter Switch
Protokoll	PROFINET IO Device nach IEC 61158-6-10
Übertragungsrate	100 Mbit/s Voll Duplex
E/A-Abbild Größe	Bis zu 1024 Byte Eingangs- und Ausgangsdaten
Anzahl projektierbare Slots	100
Features	PROFINET Conformance Class B, Medienredundanz (MRP-Client), Automatische Adressierung, Topologieerkennung (LLDP, DCP), Diagnosealarme
MQTT Schnittstelle (X2)	
Anschluss	2x RJ45, integrierter Switch
Protokoll	MQTT V3.1.1 & V5
Übertragungsrate	10/100 Mbits/s, voll-/halbduplex
Statusanzeige	9 LEDs Funktions-Status, 8 LEDs Ethernet-Status
Spannungsversorgung	DC 24 V (18 - 28 V DC)
Stromaufnahme	max. 210mA
Verlustleistung	Max. 5 W
Abmessungen (T x B x H)	32,5 x 58,5 x 76 mm (ohne Spannungsversorgungsstecker)
Gewicht	ca. 135 g
Zulassungen	PROFINET Conformance Class B
Umgebungsbedingungen	
Schutzart	IP 20
Relative Feuchte	95% ohne Betauung
Einbaulage	beliebig
Zulässige Umgebungstemperatur	0° C bis 60° C
Transport- und Lagertemperatur	-20° C bis 80° C
Störfestigkeit	DIN EN 61000-6-2 „EMV-Störfestigkeit“
Störaussendung	DIN EN 61000-6-4 „EMV-Störaussendung“
Vibration und Schockfestigkeit	DIN EN 60068-2-6:2008 „Schwingung“ DIN EN 60068-2-27:2010 „Schock“