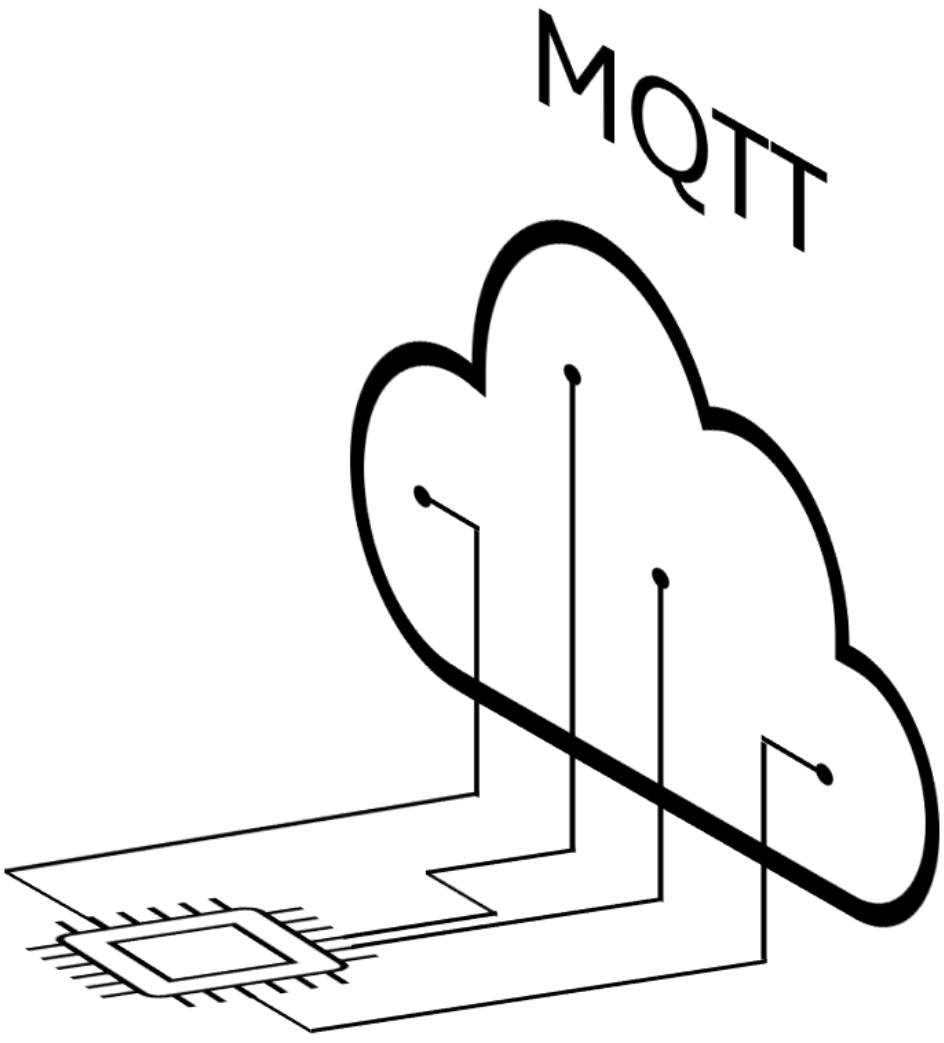
–weishaupt–

manual

Datenpunktliste Zusatzblatt



Konfiguration MQTT (WEP)

83818101 ▪ 1/2026-10

1 MQTT 3
2 Voraussetzungen für die Inbetriebnahme 4
3 Anmelden am MQTT-Webserver 5
4 MQTT-Webserver 6
5 MQTT-Einstellungen 7
6 MQTT-Broker-Einstellungen 9

1 MQTT

MQTT (Message Queuing Telemetry Transport) ist ein leichtgewichtiges Protokoll zum Austausch von Daten zwischen IoT-Geräten. Es verwendet eine publish-subscribe-Architektur, bei der Clients Daten an einen Broker senden und wiederum andere Clients diese von einem Broker beziehen können (Abbildung 1). Das System kann sehr gut skaliert werden, so dass es möglich ist, mehrere Millionen IoT-Geräte zu verwalten.

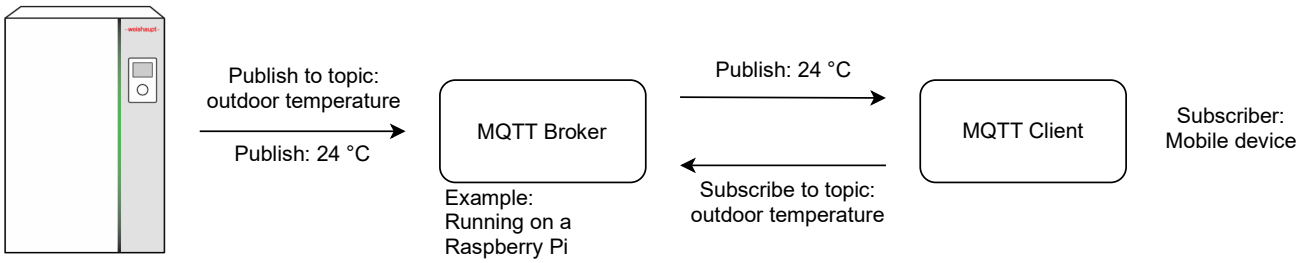


Abbildung 1: MQTT Publish/Subscribe Architecture based on: https://mqtt.org/

Nachrichten werden immer an eine sogenannte *topic* gesendet bzw. eine *topic* wird von einem Client abonniert. Erhält der Broker eine neue Nachricht, wird diese an alle Geräte gesendet, welche die *topic* dieser Nachricht abonniert haben.

2 Voraussetzungen für die Inbetriebnahme

Damit die MQTT-Schnittstelle des WEP-Systems in Betrieb genommen werden kann, muss diese zunächst am Bediengerät aktiviert werden. Dies kann im Menüpunkt *User/Settings/MQTT Protocol* eingestellt werden. Dort kann die Schnittstelle kurzzeitig für 30 min oder dauerhaft aktiviert werden.

Anschließend wird in diesem Menüpunkt ein Pin angezeigt, welcher benötigt wird, um sich auf den MQTT-Webserver des WEP-Systems anzumelden. Dieser Pin wird bei jedem Neustart des Gerätes neu generiert und sollte nicht an Dritte weitergegeben werden.

Um den MQTT-Webserver erreichen zu können, ist die Seriennummer des Gerätes notwendig. Diese kann entweder vom Typenschild abgelesen werden oder über das Bediengerät unter dem Menüpunkt *User/Settings/Portal*. Es handelt sich in jedem Fall um eine zwölfstellige Nummer, z. B. *245100000115*.

Daneben ist ein MQTT-Broker notwendig, an den die Daten gesendet werden sollen. Dieser kann z. B. lokal auf einem Raspberry Pi eingerichtet werden oder es werden externe Dienste genutzt. Für die lokale Nutzung auf einem Raspberry Pi ist z. B. der *Eclipse Mosquitto (https://mosquitto.org/)*, eine open-source-Variante, welche genutzt werden kann.

Außerdem ist ein weiterer MQTT-Client notwendig, welcher die Daten vom Broker ausliest und entsprechend weiterverarbeitet. Zum Testen der Verbindung und einzelner Datenpunkte kann *MQTT Explorer (https://mqtt-explorer.com/)* verwendet werden.

3 Anmelden am MQTT-Webserver

Für die Konfiguration der MQTT-Schnittstelle des WEP-Systems muss auf den MQTT-Webserver zugegriffen werden. Dazu muss in einem beliebigen Webbrowser nun folgende URL eingegeben werden:

`https://ze<Seriennummer>.local:8443/config`

Der Tag `<Seriennummer>` muss durch die eigentliche Seriennummer ersetzt werden, sodass die URL für die oben angegebene Seriennummer folgendermaßen lautet:

`https://ze245100000115.local:8443/config`

Da die Weboberfläche ein eigenes Zertifikat verwendet, welches dem Browser unbekannt ist, wird die Seite als gefährlich oder unsicher eingestuft. In diesem Fall kann bzw. muss die Warnung ignoriert werden und bestätigt werden, dass fortgefahren werden soll.

- Google Chrome:
  Auf *Erweitert* klicken und anschließend *Weiter zu https://ze<Seriennummer>.local (unsicher)* wählen
- Microsoft Edge:
  Auf *Erweitert* klicken und *Weiter zu … (unsicher)* wählen
- Mozilla Firefox
  Auf *Erweitert -> Risiko akzeptieren* und *fortfahren* klicken

Auf dem folgenden Anmeldebildschirm kann nun der vierstellige Pin, welcher auf dem Systemgerät unter *User/Settings/MQTT Protocol* angezeigt wird, eingegeben werden.

4 MQTT-Webserver

Die Ansicht der Weboberfläche ist in unterschiedliche Abschnitte untergliedert, welche abhängig vom aktuellen Betriebszustand sichtbar sind und teilweise bearbeitet werden können. Zunächst wird der *Client Status (*Abbildung 2*)* angezeigt, welcher den aktuellen Betriebszustand sowie den Verbindungsstatus zum MQTT-Broker darstellt.

Im Abschnitt *Network Information* (Abbildung 3) werden die aktuellen Netzwerkdaten des Gerätes (IP-Adresse, Netzwerkmaske sowie Gateway) und des Brokers (IP-Adresse und Port) angezeigt. Diese Einstellungen zeigen nur den aktuellen Zustand und können hier nicht verändert werden.

Als nächstes werden im Abschnitt *Current MQTT Configuration* (Abbildung 4) die aktuellen Einstellungswerte des geräteseitigen MQTT-Clients angezeigt. Dazu zählen die Art der Verbindung, die Art der Authentifizierung ggf. hinterlegter Benutzer und Passwort sowie hochgeladene Zertifikate.

Unter *Change MQTT Configuration* (Abbildung 5) können die Einstellungen für den MQTT-Client geändert und abgespeichert werden. Hierzu gehört der MQTT-Mode, die Verschlüsselung, die Authentifizierung und ein benutzerdefiniertes Topic-Prefix.

Schließlich kann unter *Broker Configuration* (Abbildung 6) die Einstellung für den MQTT-Broker vorgenommen werden. Dazu zählen die IP-Adresse und der Port des MQTT-Brokers sowie das Hochladen von Zertifikatsdateien, wenn eine Verschlüsselung oder die Authentifizierung mit Zertifikat gewählt wurde.

5 MQTT-Einstellungen

In **Tabelle 1** können die möglichen MQTT-Client-Einstellungen eingesehen werden. Teilweise können nur Einstellungen vorgenommen werden, wenn andere Einstellungen aktiviert wurden. Wird der *MQTT* Mode auf *off* gestellt, so werden alle weiteren Einstellungen deaktiviert. Bei der Einstellung *external server* wird eine TLS-Verschlüsselung vorausgesetzt. Eine unverschlüsselte Verbindung kann nur aufgebaut werden, wenn ein lokaler Server genutzt wird, der sich im gleichen Subnetz wie das Gerät befindet. Es wird eine Sicherheitswarnung angezeigt, wenn keine Verschlüsselung oder Authentifizierung eingestellt wurde. Außerdem können zertifikatsbasierte Authentifizierungsmaßnahmen nur angewendet werden, wenn eine TLS-Verschlüsselung aktiviert wurde. Die Eingabe eines Nutzers und eines Passwords ist nur möglich, wenn als Authentifizierungsmethode *Password* oder *Certificate & Password* ausgewählt wurde. Schließlich kann ein *Custom Prefix* nur eingegeben werden, wenn auch der *Topic-Prefix-Mode* auf *Custom* gestellt wurde.

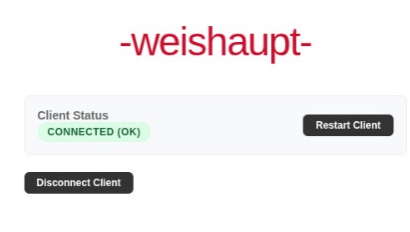


Abbildung 2: Client Status

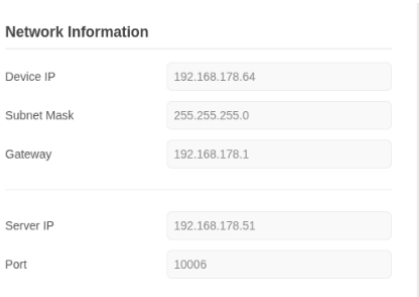


Abbildung 3: Network Information

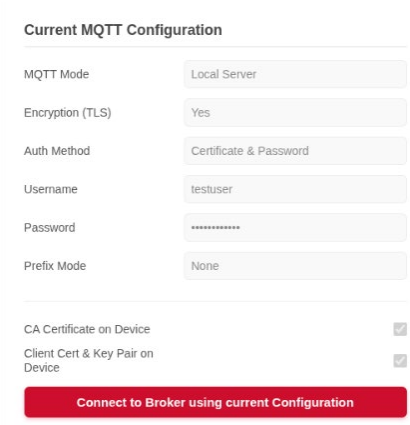


Abbildung 4: Current MQTT Configuration

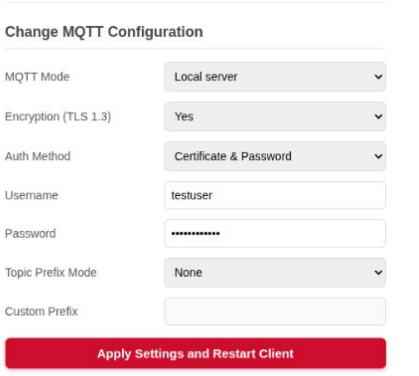


Abbildung 5: Change MQTT Configuration

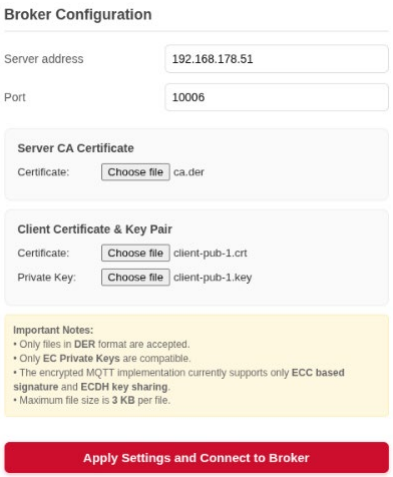


Abbildung 6: Broker Configuration

5 MQTT-Einstellungen

Feld	Einstellung	Bemerkung
MQTT Mode	Off	Deaktivierung der MQTT-Schnittstelle
	Local Server	Eine Verschlüsselung ist nicht zwingend notwendig, die IP-Adresse des Brokers muss im gleichen Subnetz wie das Gerät liegen
	External Server	Eine Verschlüsselung ist notwendig
Encryption (TLS 1.3)	No	Keine Verschlüsselung der Nachrichten
	Yes	Nachrichten werden verschlüsselt
Auth Method	None	Keine Authentifizierung am Broker
	Certificate	Client authentifiziert sich am Broker mit Client-Zertifikat
	Password	Client authentifiziert sich am Broker mit Nutzer und Passwort
	Certificate & Password	Client authentifiziert sich am Broker neben Nutzer und Passwort auch mit einem Clientzertifikat
Username / Password	Max. 31 Zeichen	Nur aktiv, wenn *Password* oder *Certificate & Password* als Authentifizierungsmethode ausgewählt wurde
Topic Prefix Mode	None	Kein benutzerdefiniertes Prefix am Beginn des Topics
	Custom	Benutzerdefiniertes Prefix am Beginn des Topics
Custom Prefix	Max. 12 Zeichen	Nur aktiv, wenn *Topic Prefix Mode* auf *Custom* gestellt wurde

Tabelle 1: MQTT-Client Einstellungen

Nachdem alle gewünschten Einstellungen eingegeben wurden, können mit dem Drücken auf den Button *Apply Settings and Restart Client* diese bestätigt und der Client neu gestartet werden.

6 MQTT-Broker-Einstellungen

Anschließend müssen noch die Daten des MQTT-Brokers eingestellt werden. Dafür wird die IP-Adresse und der Port des Brokers benötigt. Diese werden in den entsprechenden Feldern eingegeben. Ist eine Verschlüsselung aktiviert, so muss zusätzlich noch ein Zertifikat der CA (*certificate authority*) hinterlegt werden, mit dem das Serverzertifikat signiert wurde, damit das Gerät das Serverzertifikat prüfen kann, um eine TLS-Verbindung mit diesem aufbauen zu können.

Ist eine zertifikatsbasierte Authentifizierungsmethode ausgewählt worden, so muss ein Client-Zertifikat mit dazugehörigem *private key* hinterlegt werden, welches von derselben CA signiert wurde.

Für die Zertifikate gelten folgende Einschränkungen:

- Dateien müssen im DER-Format vorliegen
- Als private Schlüssel werden nur EC Private Keys akzeptiert
- Nur ECC-basierte Signaturen und ECDH-Schlüsselaustausch ist möglich
- Die maximale Dateigröße beträgt 3 kB
- Für Zertifikate werden die Endungen .der / .cert akzeptiert
- Für private Schlüssel werden die Endungen .der / .pem / .key akzeptiert

Sind alle Einstellungen getätigt, kann über die Schaltfläche *Apply Settings and Connect to Broker* eine Verbindung zum Broker aufgebaut werden. Bei fehlenden Eingaben werden entsprechende Fehlermeldungen angezeigt (Tabelle 2).

Meldung / Symptom	Bedeutung	Abhilfe
Successful (grün)	Aktion erfolgreich ausgeführt	Keine
Error: … (rot)	Ungültige Anfrage; der angehängte Text nennt die Ursache	Eingabe gemäß Meldung korrigieren
Error: … (orange)	Konflikt; z. B. Aktion aktuell nicht möglich	Kurz warten und erneut versuchen
Internal Device Error	Interner Fehler im Gerät	Client neu starten; ggf. Gerät neu starten
Error loading initial config	Die Startkonfiguration konnte nicht geladen werden	Seite neu laden; Netzwerkverbindung zum Gerät prüfen
Network Error during save	Netzwerkfehler beim Speichern	Verbindung zum Gerät prüfen und erneut versuchen
Not all needed files have been provided	Es fehlen erforderliche Zertifikatsdateien	Alle benötigten Dateien (CA bzw. Client-Zertifikat + Key) hochladen
… file is too large (> 3 kB)	Eine Zertifikats- / Schlüsseldatei überschreitet 3 kB	Kleinere Datei im korrekten Format verwenden
Valid port number between 0 and 65535	Ungültige Portnummer eingegeben	Gültige Portnummer im Bereich von 0 bis 65535 eingeben
Failed to get status	Statusabfrage fehlgeschlagen	Netzwerkverbindung überprüfen

Tabelle 2: Status- und Fehlermeldungen

–weishaupt–

Max Weishaupt SE · 88475 Schwendi

Weishaupt in Ihrer Nähe? Adressen, Telefonnummern usw. finden sie unter www.weishaupt.de

Änderungen aller Art vorbehalten. Nachdruck verboten.

Das ist Zuverlässigkeit. C'est la fiabilité. That's reliability. Questa è affidabilità. 信頼性とは、ころいろものです。Това е надеждност. Ez a megbízhatóság. Đó là sự đáng tin cậy. ست ان ان ون ال ت ب ق ن ا To je zanesljivost. Güvence budur. Αυτό σημαίνει αξιοπιστία. 그것은 바로 신뢰성입니다. To je spoľahlivosť. Dat is betrouwbaarheid. Tämä on luotettavuutta. ه ذه ه ي ال و ث و ق ي ة See on usaldusväärsus. Pouzdana tvrtka. To jest niezawodność. นั่นคือความเชื่อถือใค้ Це надійність. Isto é fiabilidade. To je spolehlivost. यही वशि्वसनीयता है. Det är pålitlighet. .זאת אמינות Esto es fiabilidad. Это надежность. Itulah kepercayaan. 值得信赖。 Is é sin iontaofacht. Iyan ang maaasahan. Aceasta este fiabilitatea. ه ے و ش و س ن ی ی ت ا. Tai - patikimumas. Det er pålitelighet. Tā ir uzticamība. Sa se fyab. To je pouzdanost. La fiabilité avant tout. Det er pålidelighed.