IoT Gateway Technical Training

Contents

Introduction

In this Quick Start Guide, the Festo CPX-IOT-O Gateway is regarded in a demonstration scenario to send data from a field device to an MQTT broker.

Chapter 1 provides an overview of the setup.
In Chapter 2 and 3 the installation and configuration of the gateway are described.
In Chapter 4 a field device is connected.
In Chapter 5 and 6 the MQTT broker is created and connected.
In Chapter 7 a sample application based on the data received via MQTT is developed.
Chapter 8 introduces two aspects of increasing the security of the MQTT connection.

1. Overview

CPX-IOT Gateway

- Connects shop floor devices to servers
- Enables on-boarding of predefined devices
- Provides edge computing via Node-RED *

North Side (Cloud Side)

- Connection to MQTT broker
- 3 load balanced MQTT addresses
- Local or cloud

South Side (Device Side)

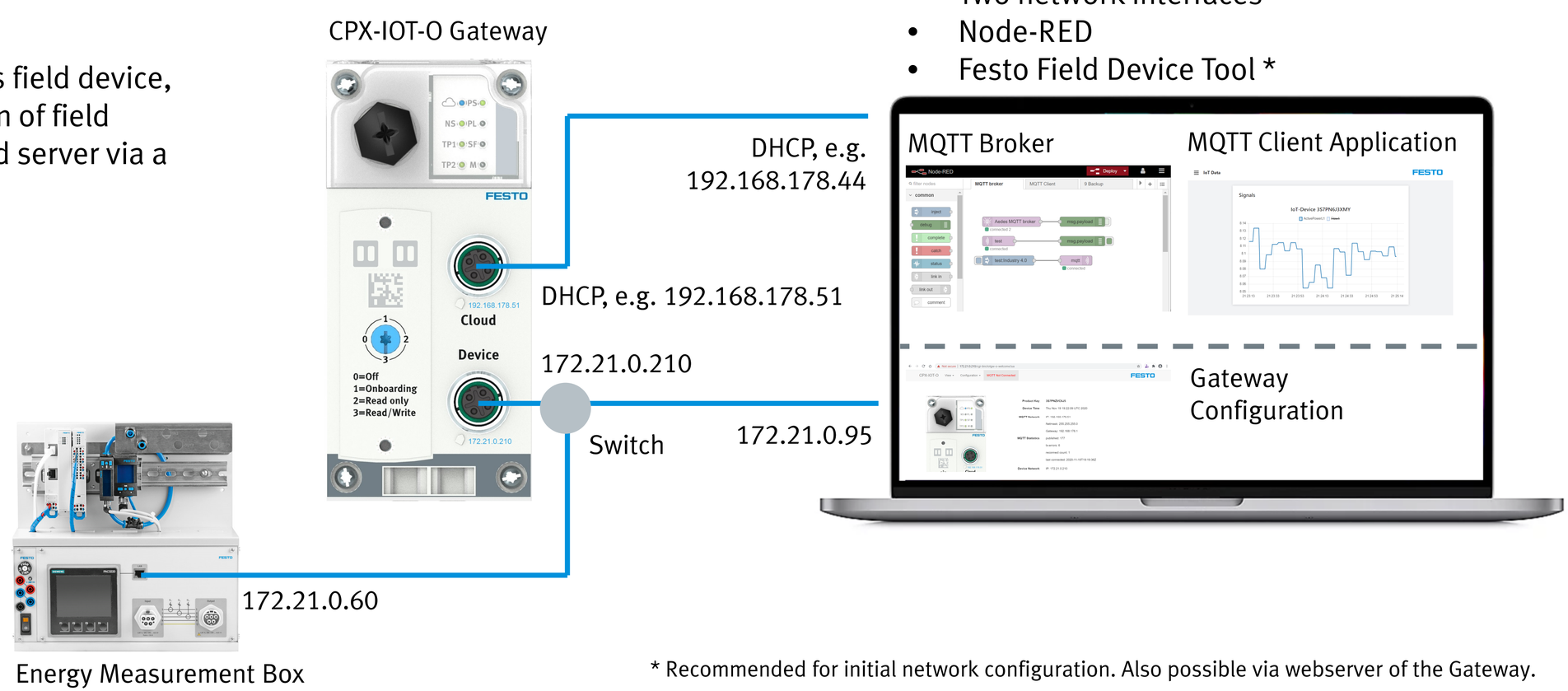
- OPC UA client connects to devices
- 10 devices with OPC UA server can be connected
- Automatic device detection
- Mapping to MQTT via signatures

* Feature will be added in 2021 via firmware update

1. Overview

The test setup considered in this Quick Start Guide consists of

- one CPX-IOT Gateway
- one Energy Measurement Box as field device,
- one PC both for the configuration of field devices and representing a cloud server via a second network interface.



* Recommended for initial network configuration. Also possible via webserver of the Gateway.

2. Gateway Installation

1. The Gateway can be mounted on an H-rail with the provided accessories.
   Ensure the cables can be connected easily later.

Mounting example CP Lab trolley

2. Gateway Installation

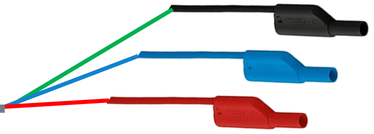
1. The Gateway can be mounted on an H-rail with the provided accessories.
   Ensure the cables can be connected easily later.
2. Connect the ethernet cable to the Device network.
3. Connect the ethernet cable to the Cloud network.
   Device and server networks must not be the same.
4. Connect the power cable to a 24 V DC power supply unit.

Ethernet cable M12 - RJ45
NEBC-D12G4-ES-5-S-R3G4-ET

Ethernet cable M12 - RJ45
NEBC-D12G4-ES-1-S-R3G4-ET

Power connector M18
18493 / 18527

Power cable with 4 mm plugs



Grounding

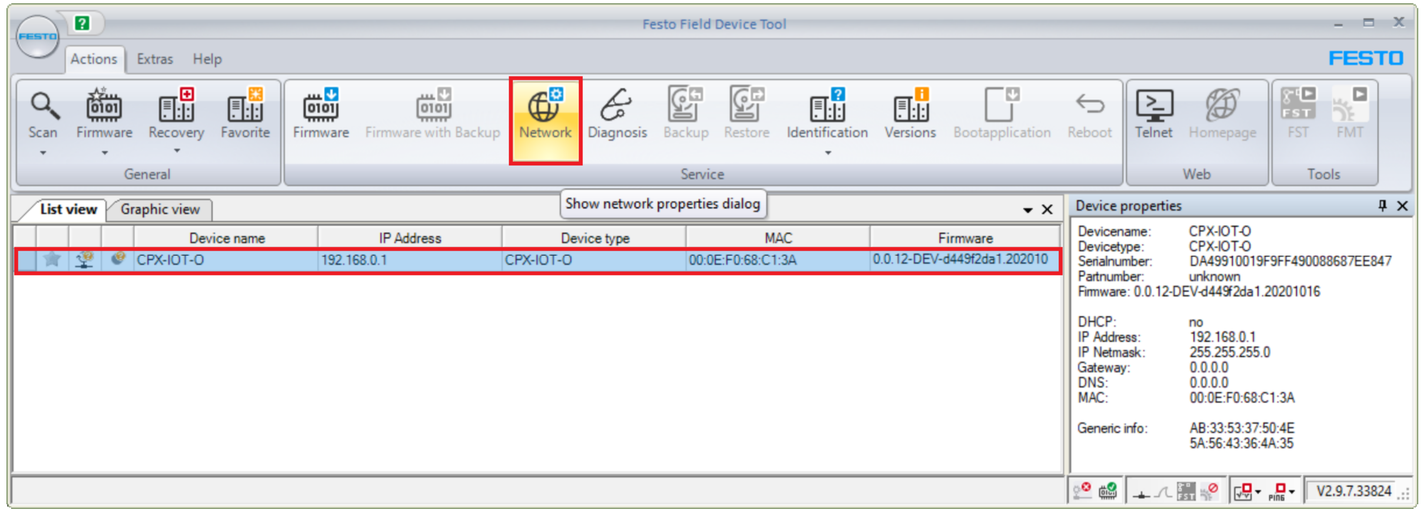
0 V DC

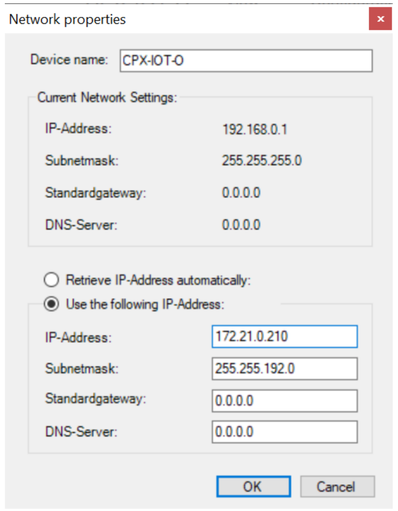
24 V DC

3. Gateway Configuration: Device Network Settings

The device network settings can be changed using the Festo Field Device Tool [1] via a PC in the Device network.

1. Open FFT, select CPX-IOT device and click on “Network”
2. Change IP address to 172.21.*{n}*.210, subnet 255.255.192.0 with *{n}* = resource ID
3. Restart device manually (power off, power on)



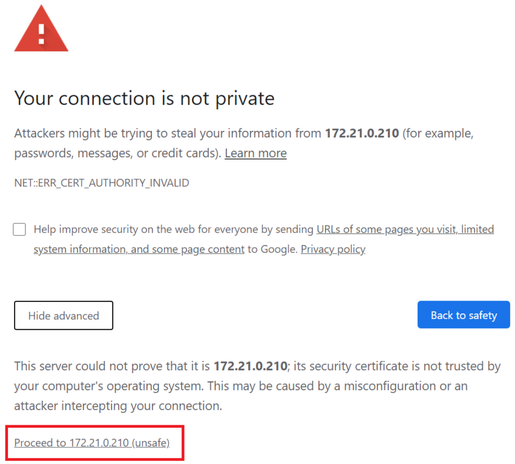


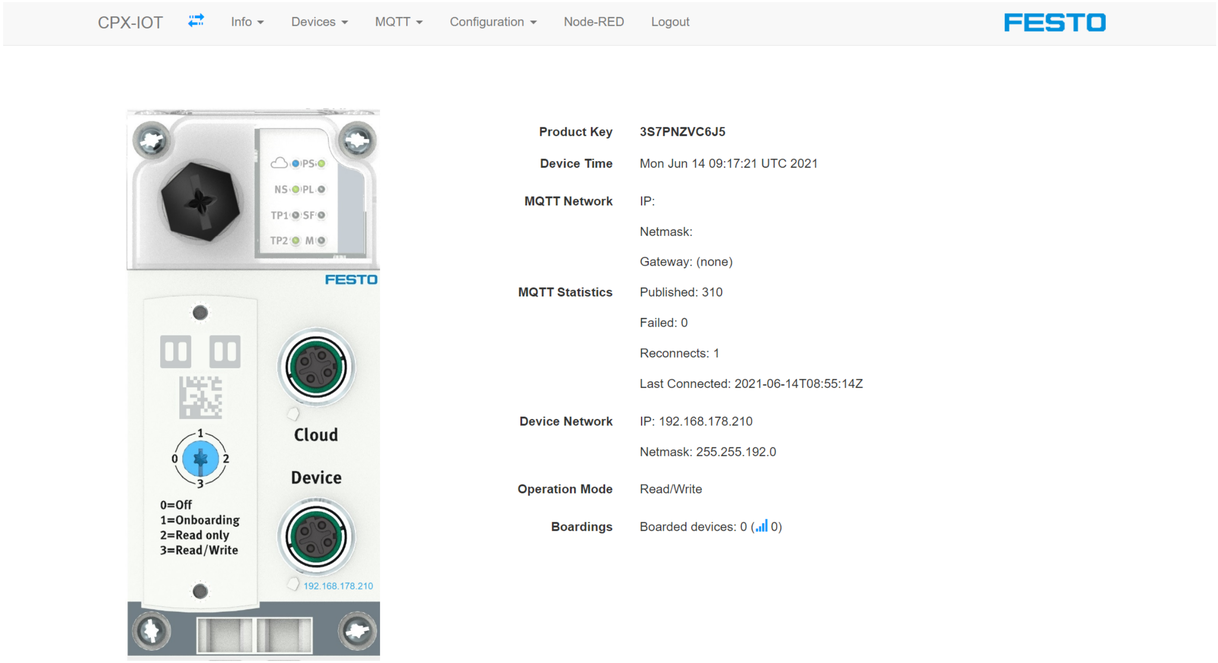
[1] https://www.festo.com/net/en-gb_gb/SupportPortal/default.aspx?q=Festo+Field+Device+Tool&documentId=281501&tab=4&s=t#result

3. Gateway Configuration: Cloud Network Settings

The Cloud network settings can be changed via the webserver.

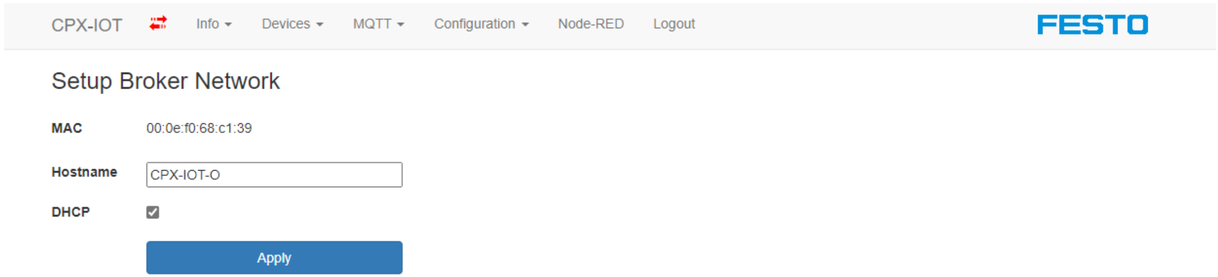
1. Open webserver via the device network
   http://172.21.0.210
   Acknowledge the security warning, depending on the browser





3. Gateway Configuration: Cloud Network Settings

2. Go to “Configuration”, “Setup Broker Network”
3. Change IPv4 settings to fit the server’s network
   Here: DHCP is activated
4. Apply changes

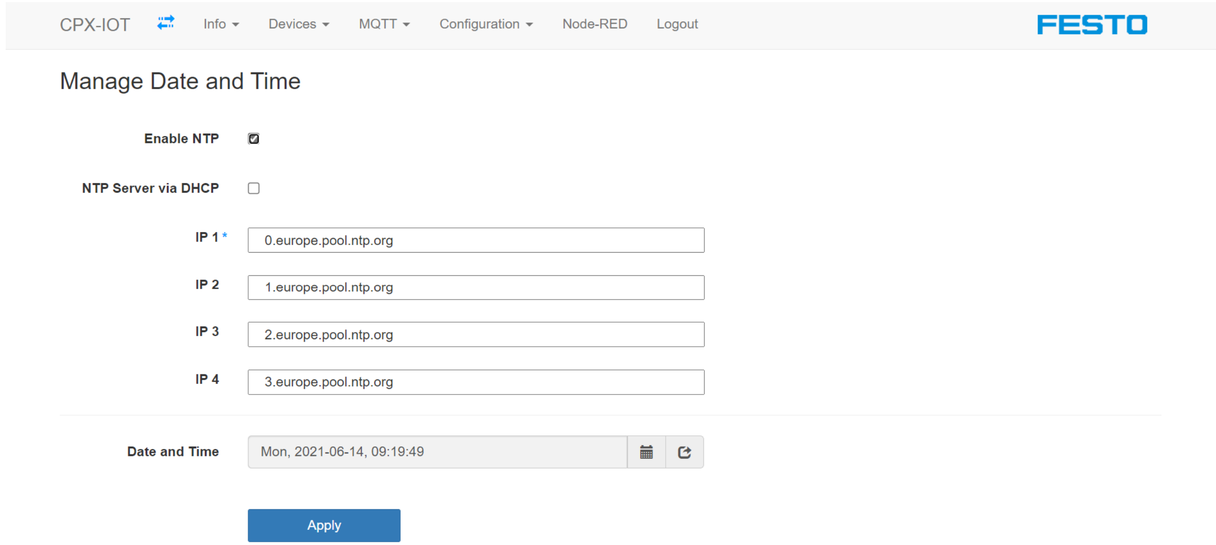


3. Gateway Configuration: Time Settings

1. Go to “Configuration”, “Manage Date and Time”
2. Enable NTP with predefined or custom servers or set the time manually

   Note: The MES PC (IP address default 172.21.0.90) has an activated time server

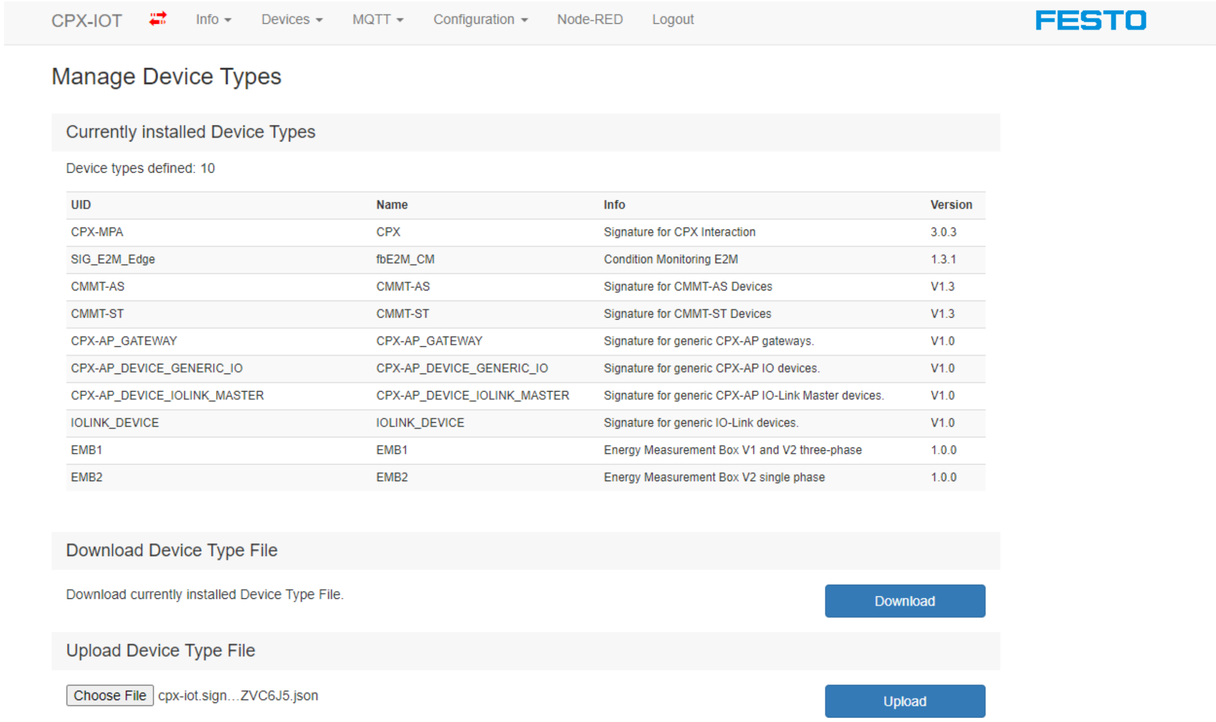
3. Apply the changes



3. Gateway Configuration: MQTT Signatures

Editing the signatures file:

1. Navigate to “Devices”, “Manage Device Types”
2. Click on “Download” to save your current signature file
3. Edit the file in a text editor to define new devices and save as new file, or use an existing signature file *
4. Click on “Choose File” to select the new signature file
5. Click on “Upload” to upload and install the new signature file



* The file “cpx-iot.signatures_EMB.json” is prepared for the Energy Measurement Boxes and is available in the Appendix.

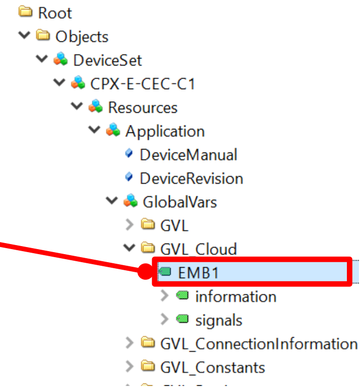
3. Gateway Configuration: MQTT Signatures

The MQTT signature maps OPC UA structures to MQTT messages.

Important elements of the MQTT signature file:

Element	Description
iname	OPC UA browse name of the root element • The iname root will be searched automatically • Only elements below this root will be available

signatures.json



OPC UA address space

3. Gateway Configuration: MQTT Signatures

Important elements of the MQTT signature file:

Element	Description
Nodes	Array of elements mapping OPC UA variables to MQTT topics
srcKey	OPC UA identifier **%nspath%** represents the namespace and path of the iname (root)
destKey	MQTT topic name
messageTypeIds	One or multiple of the defined messageTypes, e.g. **RT**: “Real Time” interval 1000 ms **CYCLE**: Triggered when a cycle counter changes
isDeviceID	=1 Unique identification of one node containing the ID of the device, usually the ProductKey Is used in the MQTT messages for identification
triggerValueType: “VALUE” **triggerMessageTypeIds: [“CYCLE”]**	Makes this node trigger messages of type CYCLE on value change

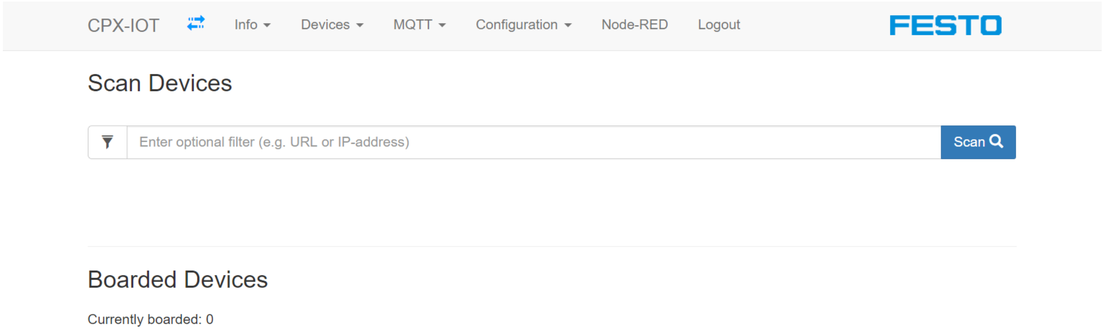

```
"Nodes": [
  {
    "srcKey": "%nspath%.information.sProductKey",
    "destKey": "ProductKey",
    "messageTypeIds": [
      "CYCLE",
      "KEEPALIVE"
    ],
    "isDeviceID": 1
  },
  {
    "srcKey": "%nspath%.information.sVersion",
    "destKey": "Version",
    "messageTypeIds": [
      "CYCLE"
    ]
  },
  {
    "srcKey": "%nspath%.signals.iCycleProcessCounter",
    "destKey": "CYCLPRCOUNT",
    "messageTypeIds": [
      "CYCLE"
    ],
    "triggerValueType": "VALUE",
    "triggerMessageTypeIds": [
      "CYCLE"
    ]
  },
  {
    "srcKey": "%nspath%.signals.ActivePowerL1.rAverageValue",
    "destKey": "ActivePowerL1",
    "messageTypeIds": [
      "RT"
    ]
  },
  {
    "srcKey": "%nspath%.signals.ActivePowerL1.sUnit",
    "destKey": "ActivePowerL1Unit",
    "messageTypeIds": [
      "CYCLE"
    ]
  }
```

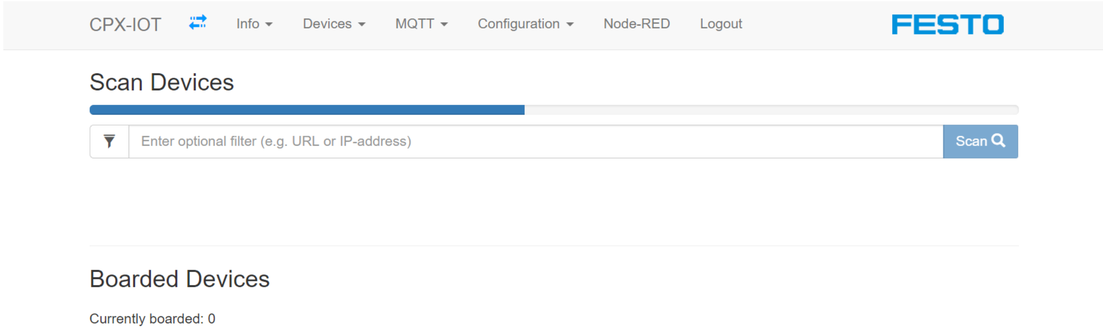

signatures.json

4. Onboarding of Devices

Devices containing one of the defined signatures can automatically be detected and onboarded (= connected to the gateway).

1. Navigate to “Devices”, “Manage Devices”
2. Click on “Scan”

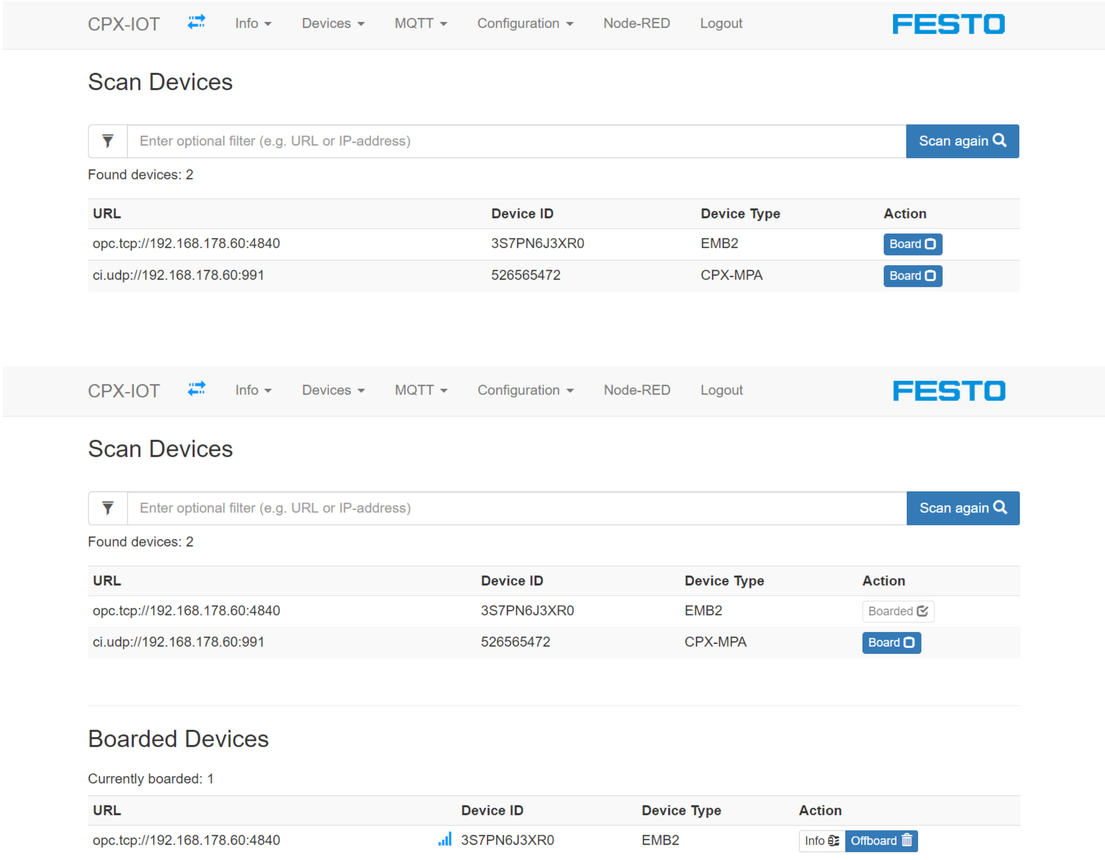




4. Onboarding of Devices

3. Select “Board” and “Board device”, here device with signature EMB1 or EMB2
4. Select “Board device”
5. The device is registered as “Boarded device” and indicates the connectivity with the blue symbol

Note: The rotary switch must be in position “3 Read/Write” to enable detection and onboarding of devices!

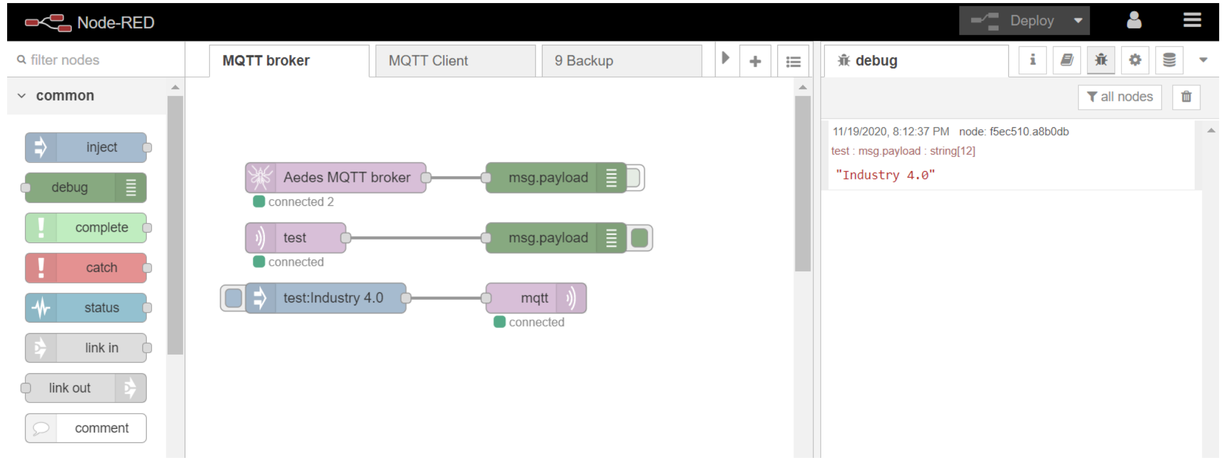


5. Set up an MQTT Broker

MQTT (Message Queuing Telemetry Transport) is an open publish-subscribe network protocol.
The IoT Gateway can connect to an MQTT broker to send data.

An MQTT broker can be implemented in Node-RED* on the PC (simulating the cloud) as follows:

1. Open the Node-RED editor
2. Install the palette “node-red-contrib-aedes”
3. Add the node “aedes broker”
4. Add “mqtt in” node, listening on topic “test” and debug node
5. Add “mqtt out” node and inject node with topic “test”
6. Deploy
7. Inject and observe the debug message

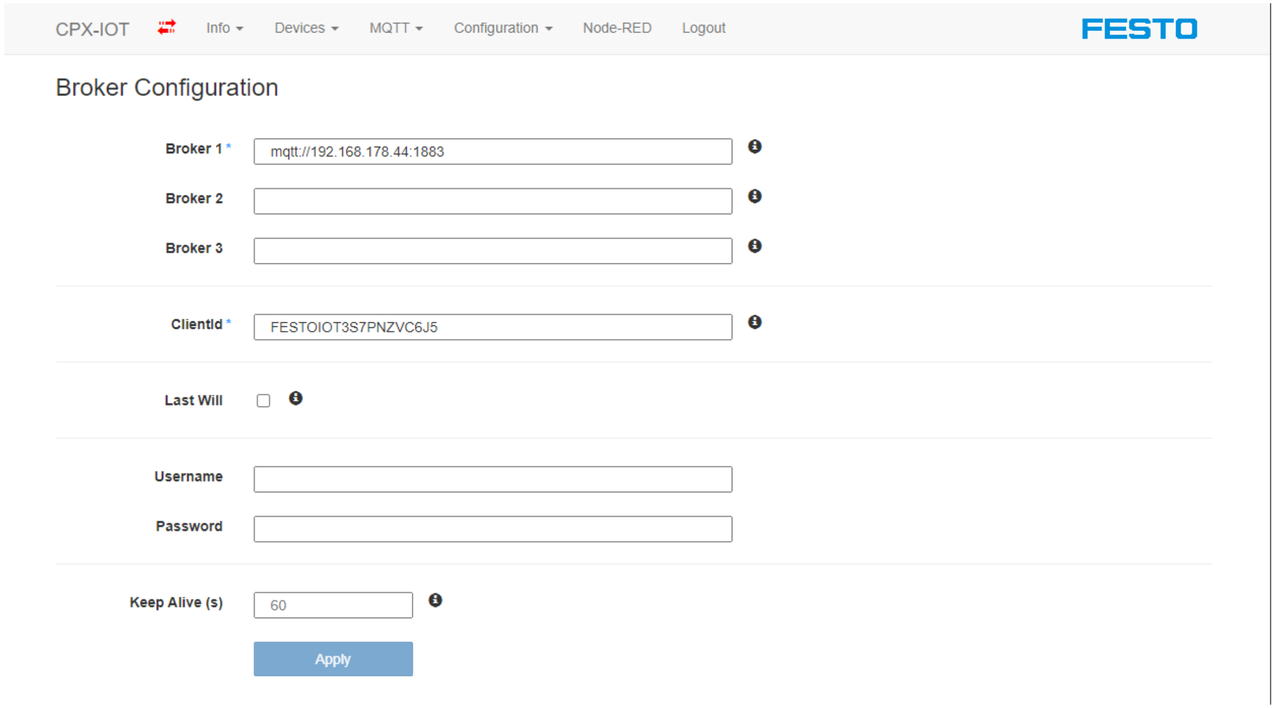


* https://nodered.org/

6. Set up the MQTT Connection

The MQTT broker information will now be configured on the gateway.

1. Navigate to “MQTT”, “Broker Configuration”
2. Insert in “Broker 1”:
   mqtt://*{server}*:1883
   where *{server}* is the server name or IP address of the MQTT broker in the Cloud network.
   Here: IP address of the Node-RED server (192.168.178.44) *
3. Submit

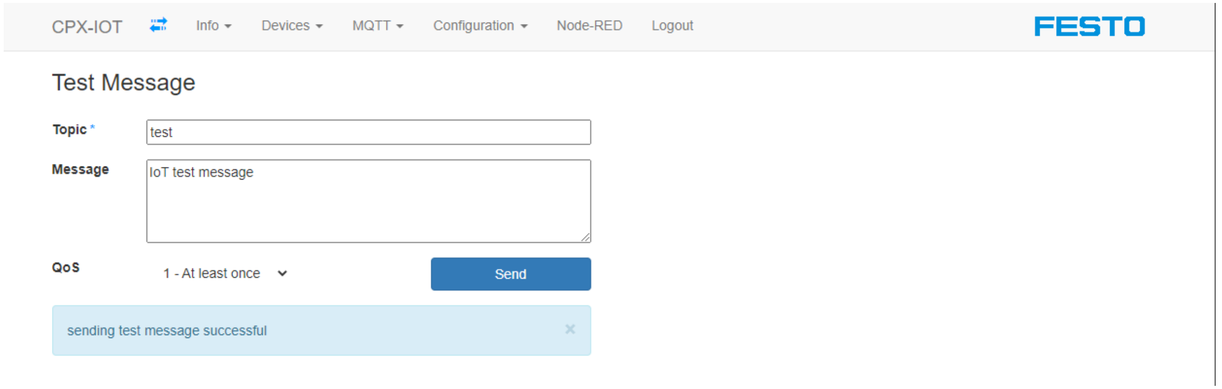


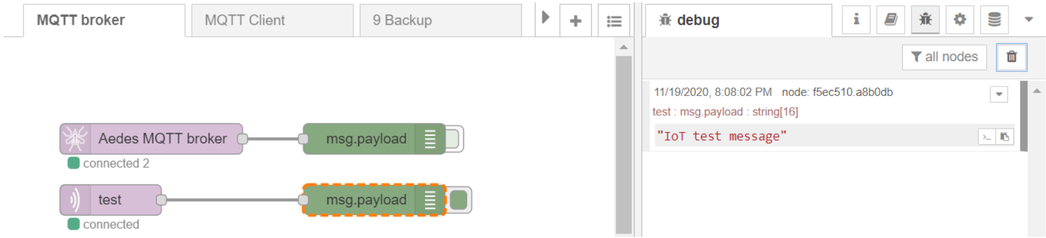
* In this setup, also the device side IP address of the PC (172.21.0.91) can be used. Requirement: **The cloud** side of the gateway is still connected to **any** DHCP server.

6. Set up the MQTT Connection

The MQTT connection between gateway and broker is now tested.

4. The status bar should indicate a blue connection symbol.
5. Navigate to “MQTT”, “Test Message”
6. Insert a message text
7. Insert the topic “test”
8. Send
9. “sending test message successful” appears
10. In Node-RED, the message text is shown in the debug sidebar

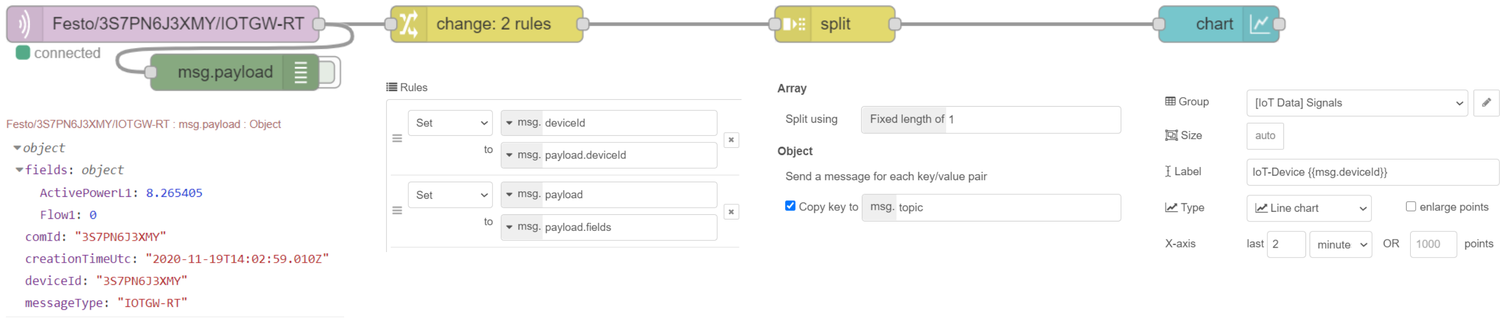


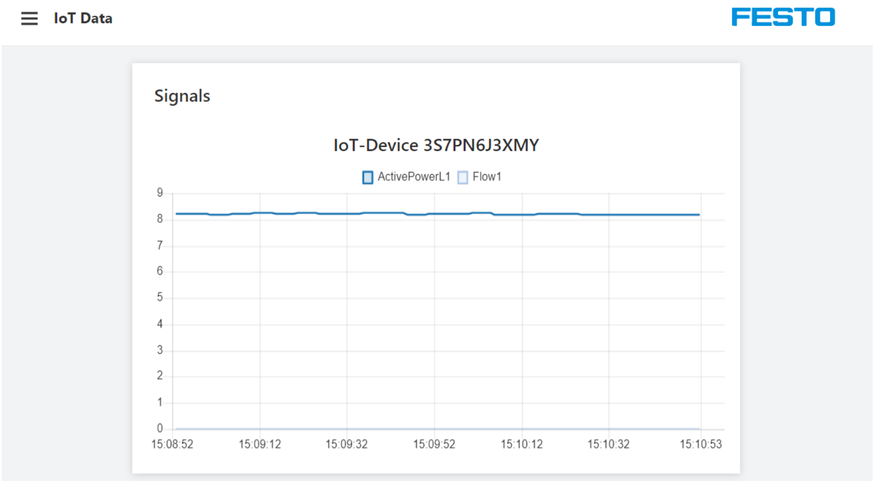


7. Set up an MQTT Client Application

An MQTT client can be implemented in Node-RED to receive the data.

1. Add an “mqtt in” node with topic “Festo/*{deviceId}*/IOTGW-RT”, where *{deviceId}* is the Device ID shown in the list of boarded devices. Output “a parsed JSON object”.
2. Add “change” and “split” nodes to extract the data
3. Add a “chart” node to visualise the data
4. Deploy and navigate to the dashboard. Data is updated in the chart every second. *

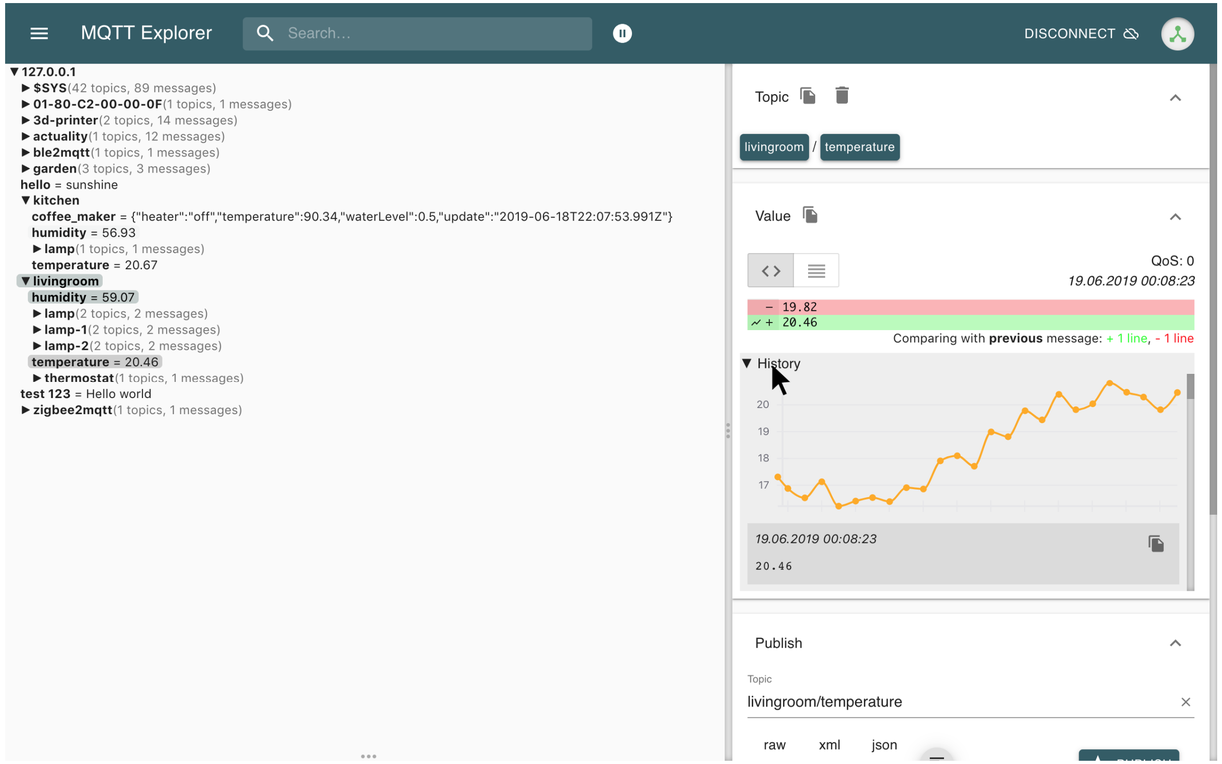




* The variables of the devices may be updated in another interval, depending on the devices and definitions in the signature file.

7. Set up an MQTT Client Application

To browse the data of the MQTT broker, third party tools can be applied, e.g., the “MQTT Explorer”. It provides a structured overview of the MQTT topics.



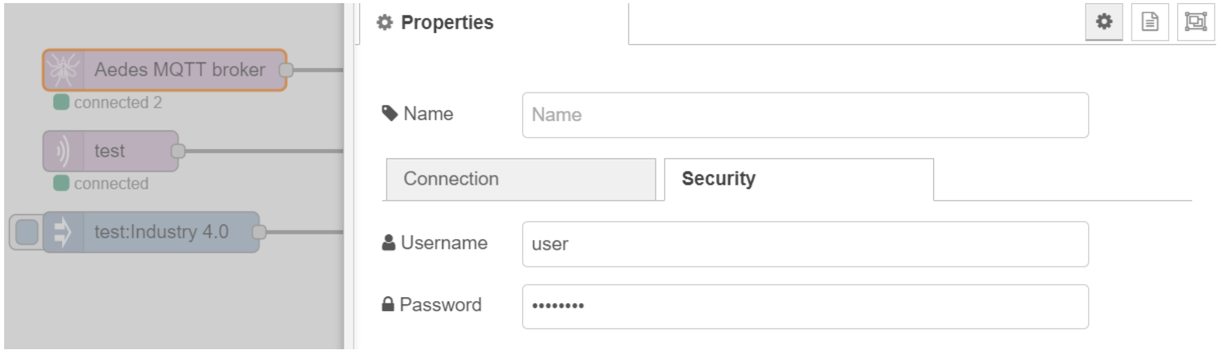
https://mqtt-explorer.com/

8. MQTT Security

To increase the security of the MQTT connection, password authentication and certificates can be used.

Password

1. MQTT broker in Node-RED:
   Go to tab “Security”
   Add username and password
   Deploy



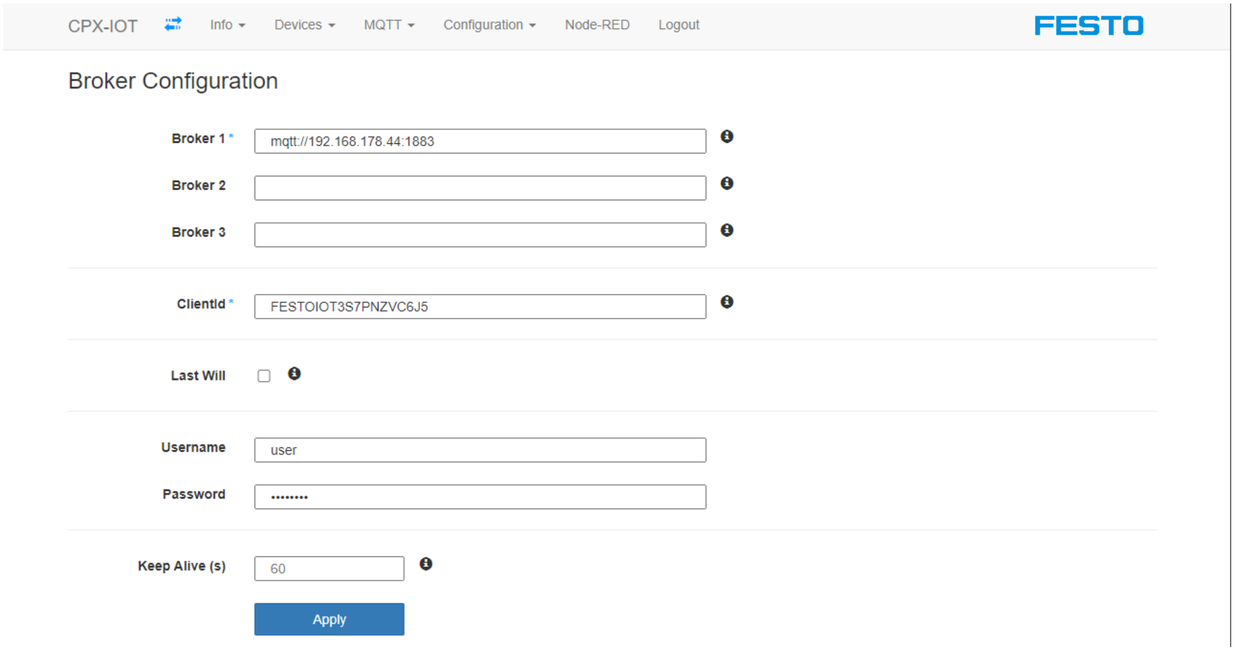
MQTT broker Properties

8. MQTT Security

To increase the security of the MQTT connection, password authentication and certificates can be used.

Password

2. MQTT gateway configuration:
   Navigate to “Configuration“, “Broker Configuration“
   Add username and password
   Apply



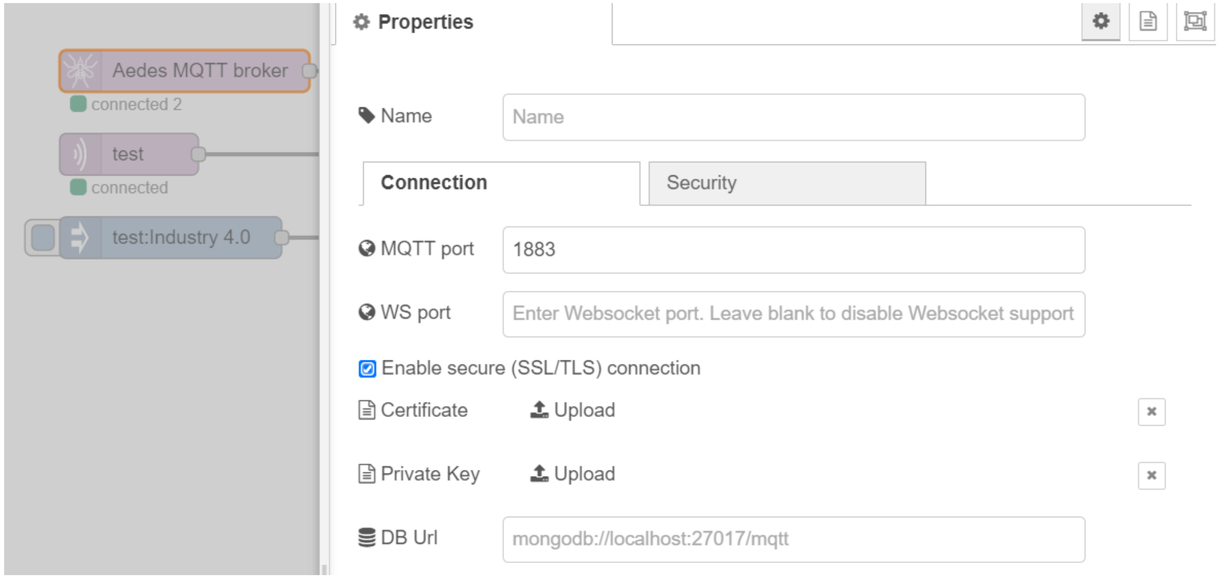
MQTT gateway configuration

8. MQTT Security

To increase the security of the MQTT connection, password authentication and certificates can be used.

Certificates

1. MQTT broker in Node-RED:
   Go to tab “Connection”
   Enable secure (SSL/TLS) connection
   Upload Certificate and Key files
   Deploy



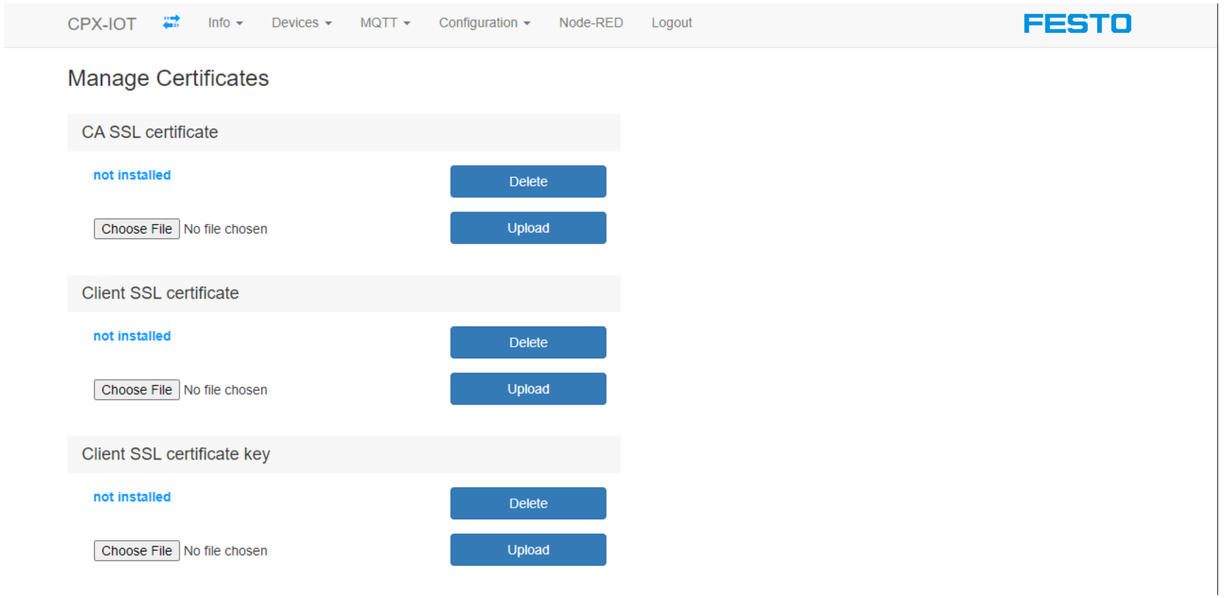
MQTT Broker certificate settings

8. MQTT Security

To increase the security of the MQTT connection, password authentication and certificates can be used.

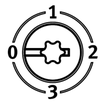
Certificates

2. MQTT gateway configuration:
   Navigate to “Configuration“, “Manage Certificates“
   Upload Certificate and Key files



Certificate configuration on the gateway

Appendix: Rotary switch operating mode

Switching position		Operating mode/ function
	0: Off	- Network connection “Cloud” deactivated (switch-off of interface) - No communication with the cloud
	1: Onboarding	- Network connection “Cloud” activated - Gateway sends process data of the configured field devices to the MQTT broker
	2: Read only	
	3: Read/Write	- Same as “Read only”, and additionally: - Onboarding and Offboarding of field devices enabled

Appendix: Signature files

Description	Signature file
Signature file on delivery	 cpx-iot.signatures_original.json
Signature file with added signatures for Energy Measurement Boxes	 cpx-iot.signatures_EMB.json
Your own signature file	

Tested with CPX-IOT firmware version 1.0.2