

IoT Gateway Technical Training



Contents

1. Introduction and sample scenario
 - Components and their functionality
 - Network overview of the sample scenario
 2. Installation of the gateway
 - Mounting
 - Power and network connection
 3. Configuration of the gateways
 - Configuring the device network
 - Configuring the cloud network
 - Time server
 - MQTT device signature
 4. Adding devices („Onboarding“)
 5. MQTT broker
 - Creating and configuring a sample MQTT broker
 6. MQTT connection to the gateway
 - Connection configuration
 - Connection testing
 7. MQTT client
 - Creating and configuring a client
 - Creating a sample application
 - Analyzing MQTT messages
 8. MQTT security
 - Access protection via password
 - Access protection via certificates
- Appendix
- Hardware configuration
 - Signature files

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

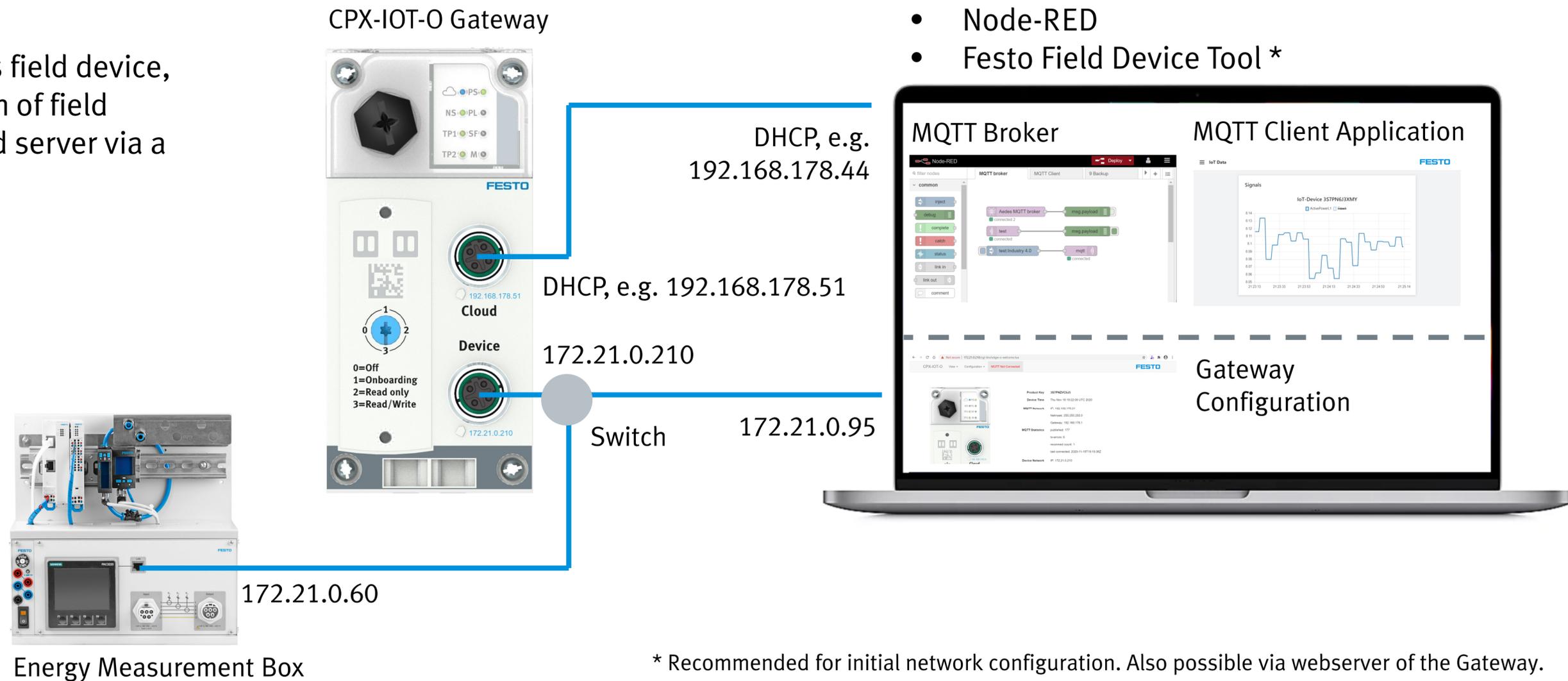


* Feature will be added in 2021 via firmware update

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.



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

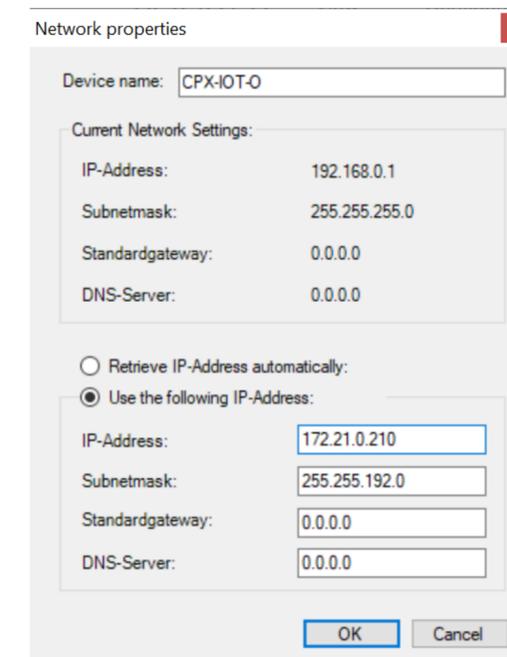
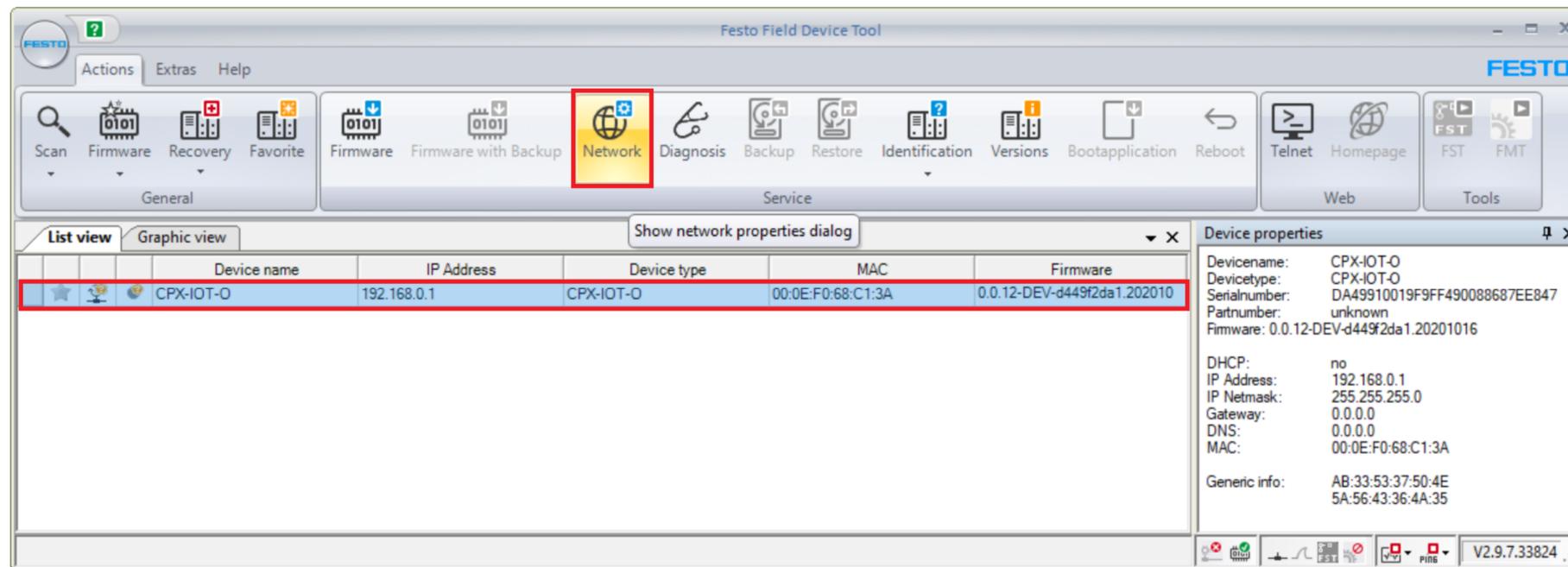
Power cable with 4 mm plugs



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

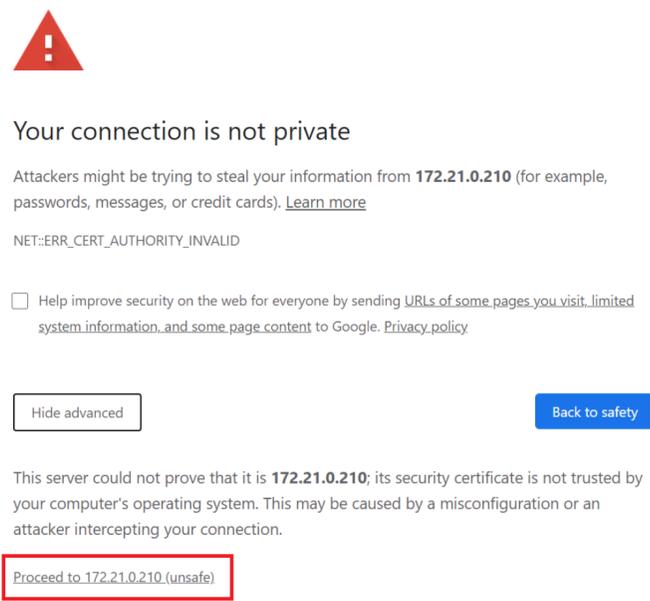
3. Gateway Configuration: Cloud Network Settings

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

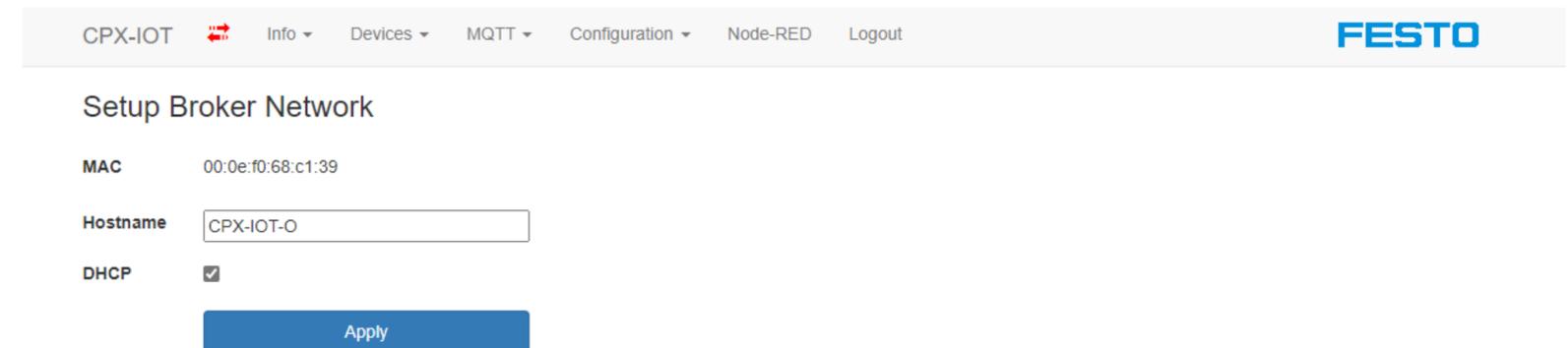


| | |
|------------------------|--|
| Product Key | 3S7PNZVC6J5 |
| Device Time | Mon Jun 14 09:17:21 UTC 2021 |
| MQTT Network | IP: Netmask: Gateway: (none) |
| MQTT Statistics | Published: 310 Failed: 0 Reconnects: 1 Last Connected: 2021-06-14T08:55:14Z |
| Device Network | IP: 192.168.178.210 Netmask: 255.255.192.0 |
| Operation Mode | Read/Write |
| Boardings | Boarded devices: 0 (0) |



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



The screenshot shows the 'Setup Broker Network' configuration page. The top navigation bar includes 'CPX-IOT', 'Info', 'Devices', 'MQTT', 'Configuration', 'Node-RED', and 'Logout'. The 'FESTO' logo is in the top right corner. The main content area displays the following settings:

- MAC:** 00:0e:f0:68:c1:39
- Hostname:** CPX-IOT-0
- DHCP:**

An 'Apply' button is located at the bottom of the configuration area.

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

The screenshot shows the 'Manage Date and Time' configuration page in the CPX-IOT gateway interface. The page has a navigation bar at the top with the following items: CPX-IOT, Info, Devices, MQTT, Configuration, Node-RED, Logout, and the FESTO logo. The main content area is titled 'Manage Date and Time' and contains the following settings:

- Enable NTP:** A checkbox that is checked.
- NTP Server via DHCP:** A checkbox that is unchecked.
- NTP Servers:** Four input fields labeled IP 1, IP 2, IP 3, and IP 4, each containing a predefined NTP server address:
 - IP 1: 0.europe.pool.ntp.org
 - IP 2: 1.europe.pool.ntp.org
 - IP 3: 2.europe.pool.ntp.org
 - IP 4: 3.europe.pool.ntp.org
- Date and Time:** A field showing the current date and time: Mon, 2021-06-14, 09:19:49. To the right of the field are icons for a calendar and a refresh/clock icon.
- Apply:** A blue button at the bottom of the form.

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

CPX-IOT Info Devices MQTT Configuration Node-RED Logout

Manage Device Types

Currently installed Device Types

Device types defined: 10

| UID | Name | Info | Version |
|-----------------------------|-----------------------------|--|---------|
| CPX-MPA | CPX | Signature for CPX Interaction | 3.0.3 |
| SIG_E2M_Edge | fbE2M_CM | Condition Monitoring E2M | 1.3.1 |
| CMMT-AS | CMMT-AS | Signature for CMMT-AS Devices | V1.3 |
| CMMT-ST | CMMT-ST | Signature for CMMT-ST Devices | V1.3 |
| CPX-AP_GATEWAY | CPX-AP_GATEWAY | Signature for generic CPX-AP gateways. | V1.0 |
| CPX-AP_DEVICE_GENERIC_IO | CPX-AP_DEVICE_GENERIC_IO | Signature for generic CPX-AP IO devices. | V1.0 |
| CPX-AP_DEVICE_IOLINK_MASTER | CPX-AP_DEVICE_IOLINK_MASTER | Signature for generic CPX-AP IO-Link Master devices. | V1.0 |
| IOLINK_DEVICE | IOLINK_DEVICE | Signature for generic IO-Link devices. | V1.0 |
| EMB1 | EMB1 | Energy Measurement Box V1 and V2 three-phase | 1.0.0 |
| EMB2 | EMB2 | Energy Measurement Box V2 single phase | 1.0.0 |

Download Device Type File

Download currently installed Device Type File. [Download](#)

Upload Device Type File

[Choose File](#) cpx-iot.sign...ZVC6J5.json [Upload](#)

* 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

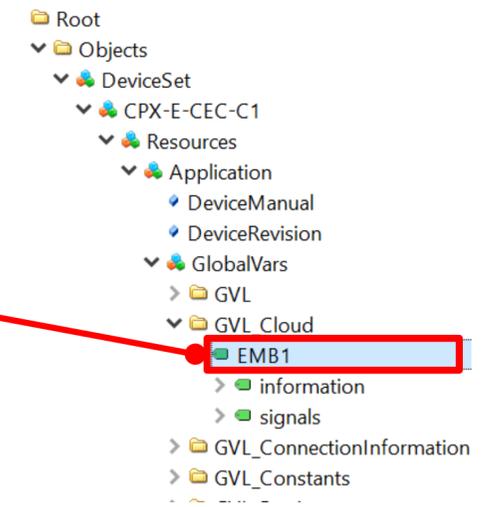
The MQTT signature maps OPC UA structures to MQTT messages.

Important elements of the MQTT signature file:

| Element | Description |
|--------------|--|
| iname | OPC UA browse name of the root element <ul style="list-style-type: none"> The iname root will be searched automatically Only elements <u>below</u> this root will be available |

```

{
  "Signatures": [
    {
      "uid": "EMB1",
      "iname": "EMB1",
      "info": "Energy Measurement Box",
      "version": "1.0.0",
      "Subscriptions": [
        {
          "id": "Default",
          "interval": 100
        }
      ],
      "messageTypes": [
      ],
      "Nodes": [
      ]
    }
  ]
}
    
```



OPC UA address space

signatures.json

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” triggerMessageTypes: [“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",
    "triggerMessageTypes": [
      "CYCLE"
    ]
  },
  {
    "srcKey": "%nspath%.signals.ActivePowerL1.rAverageValue",
    "destKey": "ActivePowerL1",
    "messageTypeIds": [
      "RT"
    ]
  },
  {
    "srcKey": "%nspath%.signals.ActivePowerL1.sUnit",
    "destKey": "ActivePowerL1Unit",
    "messageTypeIds": [
      "CYCLE"
    ]
  }
]

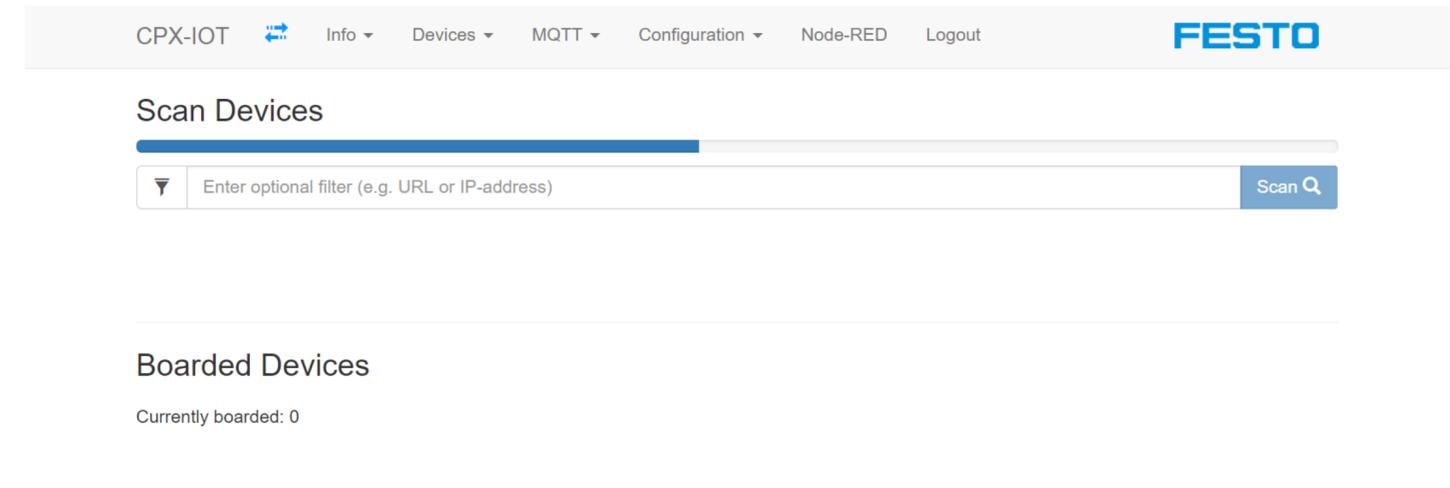
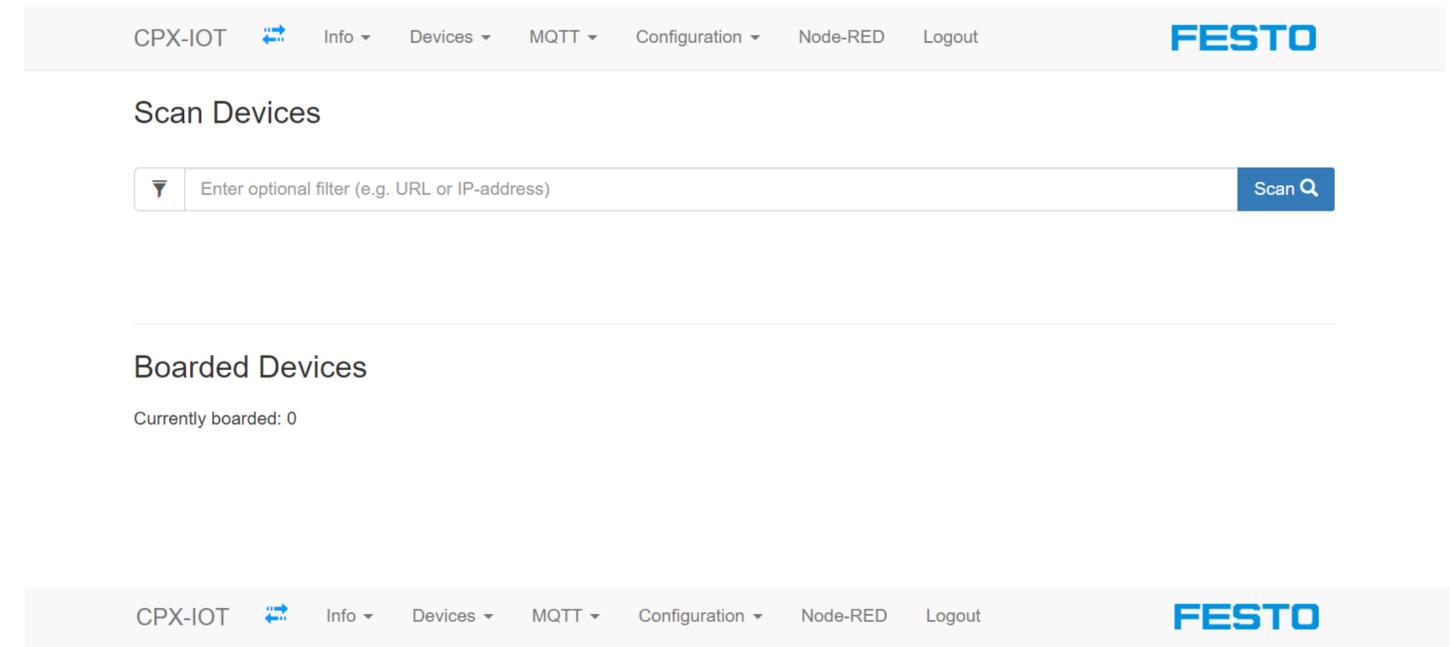
```

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!

CPX-IOT  Info ▾ Devices ▾ MQTT ▾ Configuration ▾ Node-RED Logout **FESTO**

Scan Devices

Enter optional filter (e.g. URL or IP-address) Scan again 

Found devices: 2

| URL | Device ID | Device Type | Action |
|-------------------------------|-------------|-------------|--------------------------------|
| opc.tcp://192.168.178.60:4840 | 3S7PN6J3XR0 | EMB2 | Board <input type="checkbox"/> |
| ci.udp://192.168.178.60:991 | 526565472 | CPX-MPA | Board <input type="checkbox"/> |

CPX-IOT  Info ▾ Devices ▾ MQTT ▾ Configuration ▾ Node-RED Logout **FESTO**

Scan Devices

Enter optional filter (e.g. URL or IP-address) Scan again 

Found devices: 2

| URL | Device ID | Device Type | Action |
|-------------------------------|-------------|-------------|---|
| opc.tcp://192.168.178.60:4840 | 3S7PN6J3XR0 | EMB2 | Boarded <input checked="" type="checkbox"/> |
| ci.udp://192.168.178.60:991 | 526565472 | CPX-MPA | Board <input type="checkbox"/> |

Boarded Devices

Currently boarded: 1

| URL | Device ID | Device Type | Action |
|-------------------------------|---|-------------|---|
| opc.tcp://192.168.178.60:4840 |  3S7PN6J3XR0 | EMB2 | Info  Offboard  |

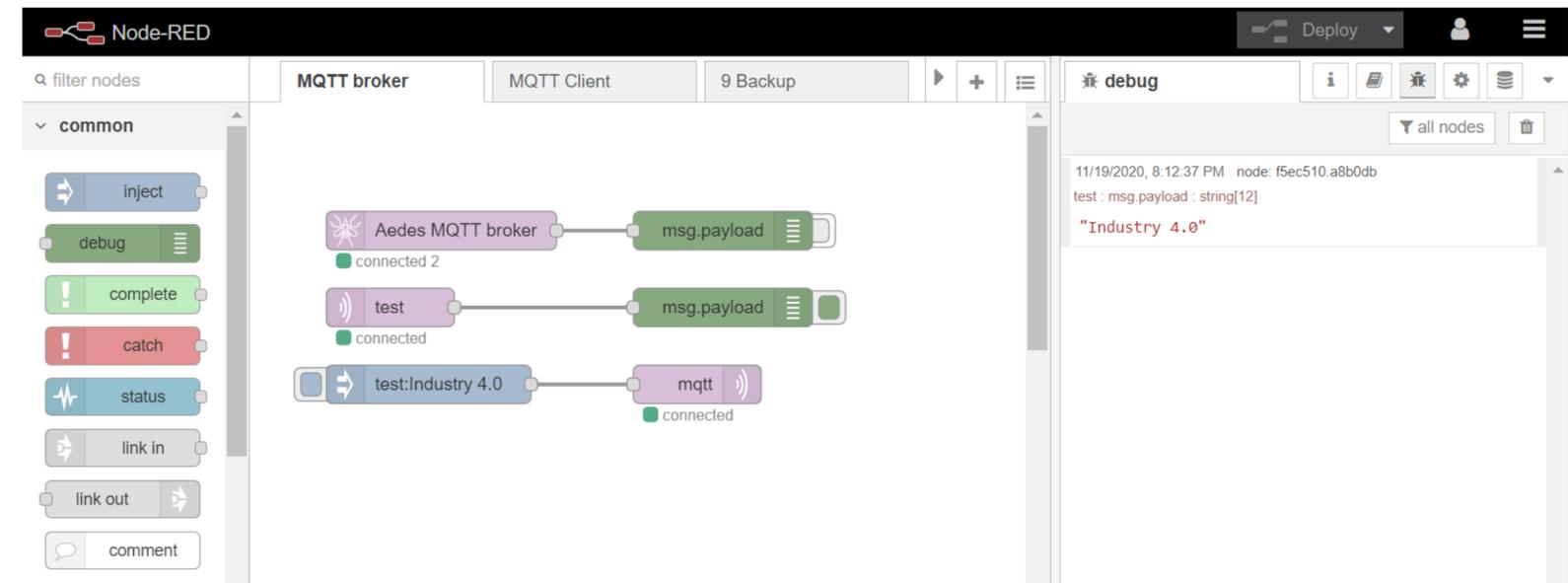
5. Set up an MQTT Broker

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

CPX-IOT Info Devices MQTT Configuration Node-RED Logout

Broker Configuration

Broker 1 * ⓘ

Broker 2 ⓘ

Broker 3 ⓘ

ClientId * ⓘ

Last Will ⓘ

Username

Password

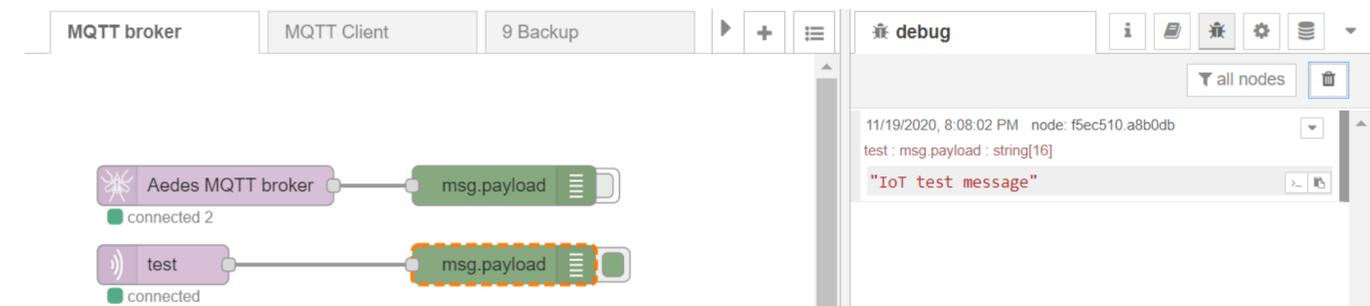
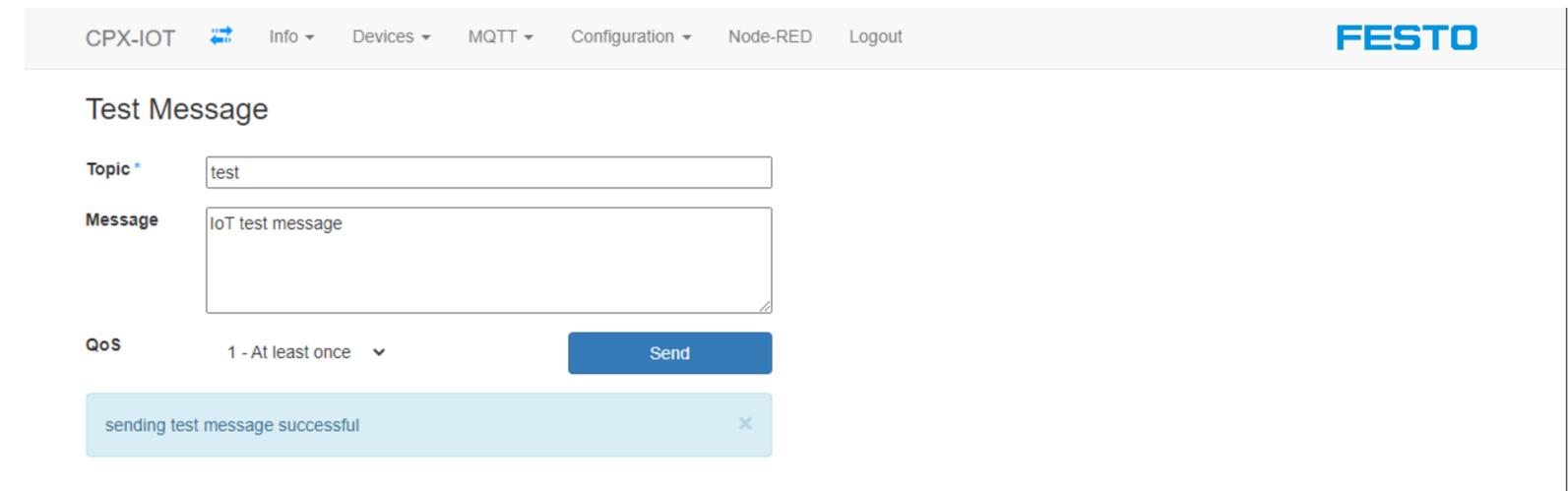
Keep Alive (s) ⓘ

* 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.

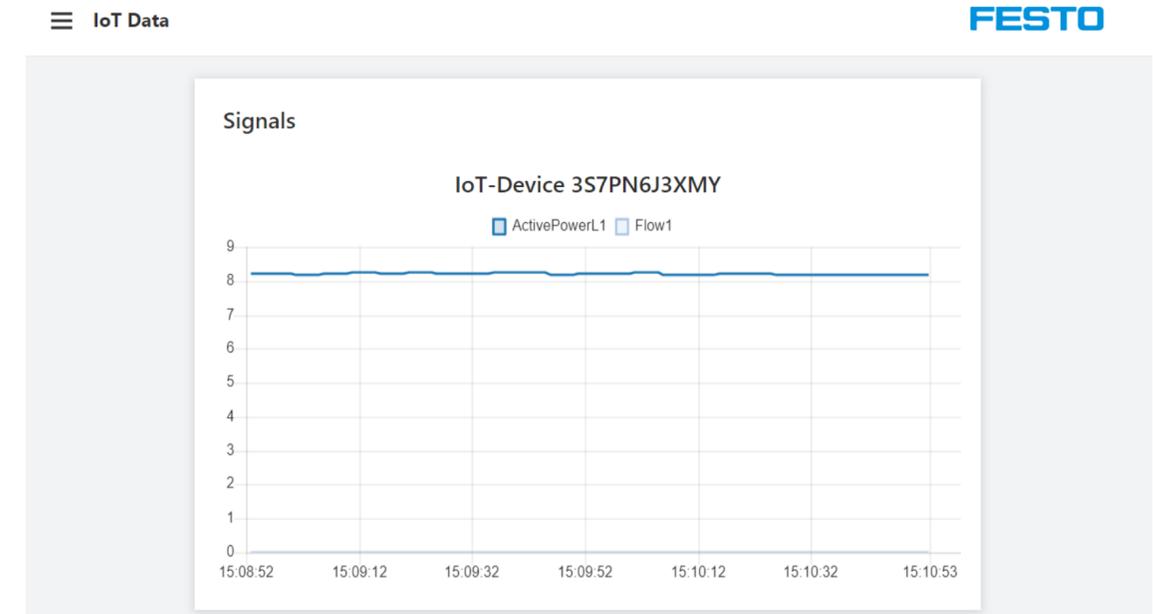
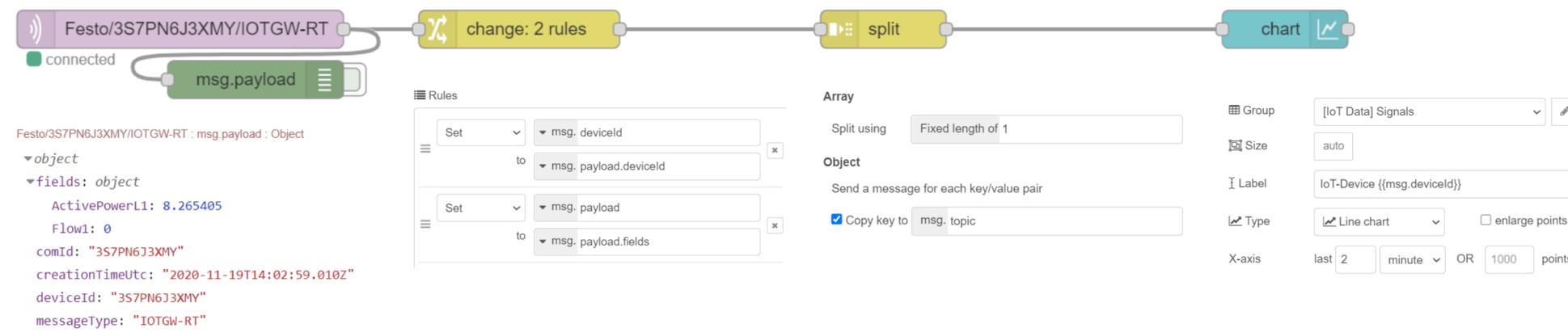
4. The status bar should indicate a blue connection symbol. 
5. Navigate to “MQTT”, “Test Message”
6. Insert a message text
7. Insert the topic “test”
8. Send
9. “sending test message successful” appears
10. In Node-RED, the message text is shown in the debug sidebar



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.

The screenshot displays the MQTT Explorer interface. On the left, a tree view shows the following structure:

- 127.0.0.1
 - ▶ \$SYS (42 topics, 89 messages)
 - ▶ 01-80-C2-00-00-0F (1 topics, 1 messages)
 - ▶ 3d-printer (2 topics, 14 messages)
 - ▶ actuality (1 topics, 12 messages)
 - ▶ ble2mqtt (1 topics, 1 messages)
 - ▶ garden (3 topics, 3 messages)
 - hello = sunshine
 - ▼ kitchen
 - coffee_maker = {"heater":"off","temperature":90.34,"waterLevel":0.5,"update":"2019-06-18T22:07:53.991Z"}
 - humidity = 56.93
 - ▶ lamp (1 topics, 1 messages)
 - temperature = 20.67
 - ▼ livingroom
 - humidity = 59.07
 - ▶ lamp (2 topics, 2 messages)
 - ▶ lamp-1 (2 topics, 2 messages)
 - ▶ lamp-2 (2 topics, 2 messages)
 - temperature = 20.46
 - ▶ thermostat (1 topics, 1 messages)
 - test 123 = Hello world
 - ▶ zigbee2mqtt (1 topics, 1 messages)

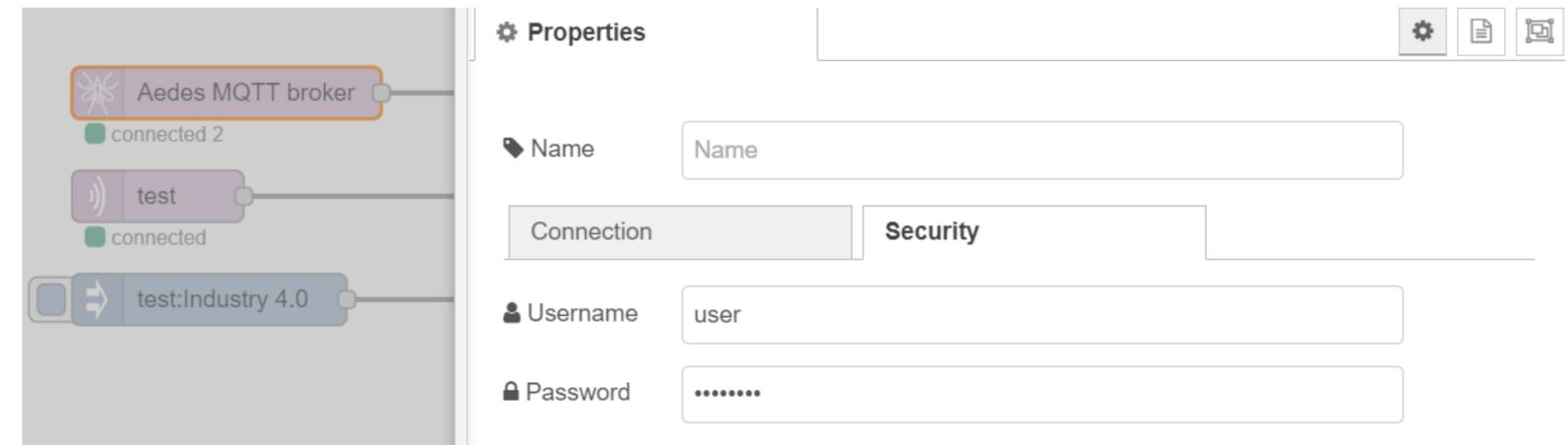
The right panel shows the selected topic `livingroom/temperature`. It displays the current value `20.46` in green, compared to the previous message `19.82` in red. A line graph history shows the temperature fluctuating between approximately 17 and 20. The interface also includes a 'Publish' section with a topic input field containing `livingroom/temperature` and format options for raw, xml, and json.

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

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

The screenshot shows the MQTT gateway configuration interface. The top navigation bar includes 'CPX-IOT', 'Info', 'Devices', 'MQTT', 'Configuration', 'Node-RED', and 'Logout'. The 'FESTO' logo is in the top right corner. The main content area is titled 'Broker Configuration' and contains the following fields:

- Broker 1 ***: Input field containing 'mqtt://192.168.178.44:1883' with an information icon.
- Broker 2**: Empty input field with an information icon.
- Broker 3**: Empty input field with an information icon.
- Clientid ***: Input field containing 'FESTOIOT3S7PNZVC6J5' with an information icon.
- Last Will**: A checkbox that is unchecked, with an information icon.
- Username**: Input field containing 'user'.
- Password**: Input field containing '.....'.
- Keep Alive (s)**: Input field containing '60' with an information icon.

An 'Apply' button is located at the bottom of the configuration area.

MQTT gateway configuration

8. MQTT Security

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

Certificates

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

The screenshot shows the Node-RED MQTT broker configuration interface. On the left, a flow contains three nodes: 'Aedes MQTT broker' (highlighted with an orange box), 'test', and 'test:Industry 4.0'. The 'Aedes MQTT broker' node is connected to the 'test' node, and the 'test' node is connected to the 'test:Industry 4.0' node. On the right, the 'Properties' panel is open, showing the 'Security' tab. The 'MQTT port' is set to 1883, and the 'WS port' is set to 'Enter Websocket port. Leave blank to disable Websocket support'. The 'Enable secure (SSL/TLS) connection' checkbox is checked. There are 'Certificate' and 'Private Key' upload buttons, each with a close button (x). The 'DB Url' is set to 'mongodb://localhost:27017/mqtt'.

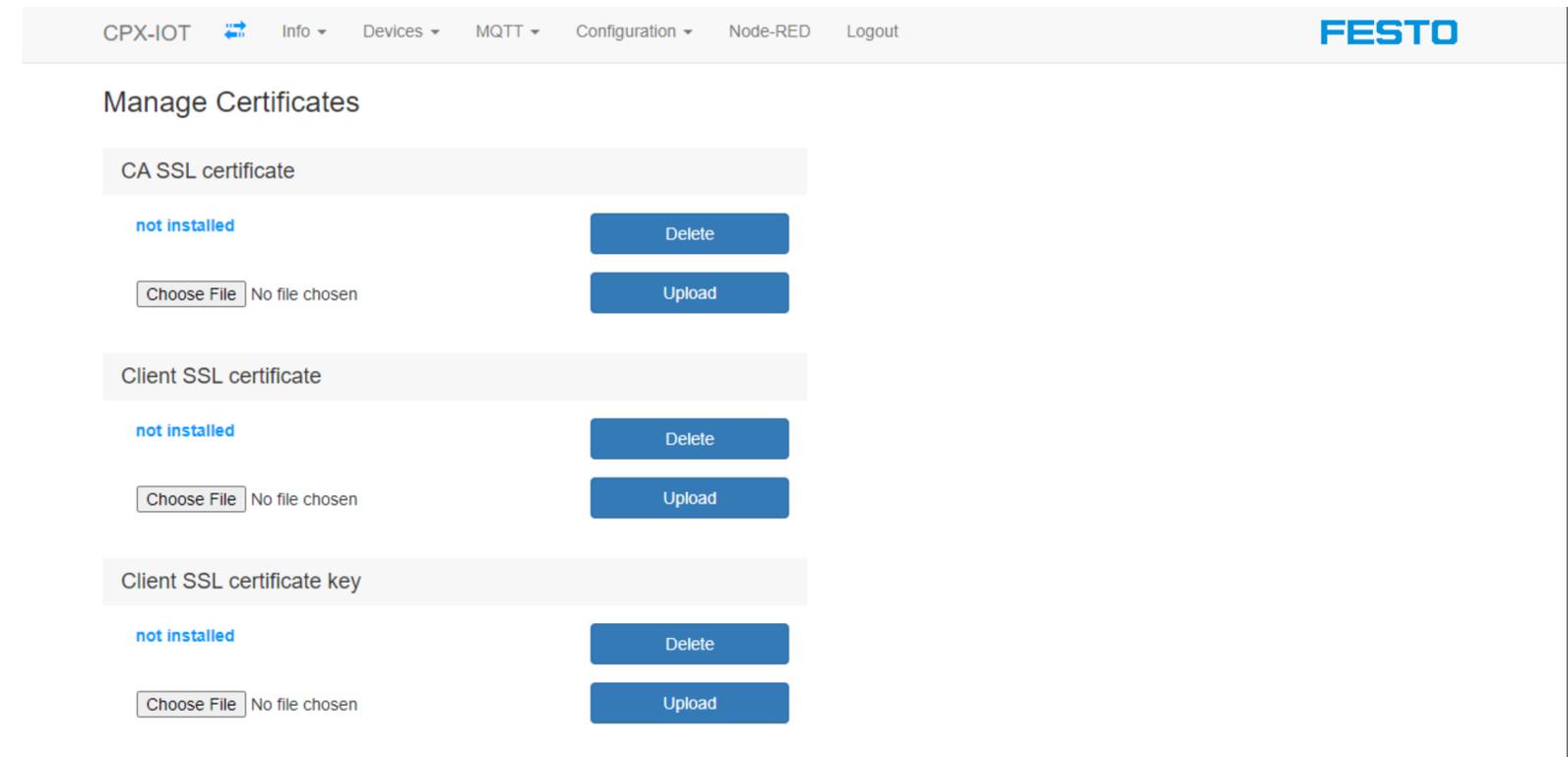
MQTT Broker certificate settings

8. MQTT Security

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

Certificates

- 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 | <ul style="list-style-type: none"> - Network connection “Cloud” deactivated (switch-off of interface) - No communication with the cloud |
| | 1: Onboarding | <ul style="list-style-type: none"> - Network connection “Cloud” activated - Gateway sends process data of the configured field devices to the MQTT broker |
| | 2: Read only | |
| | 3: Read/Write | <ul style="list-style-type: none"> - 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 | |