SD02663D/06/EN/02.23-00
71632709
2023-10-31

Valid as of version
01.01.zz (Device firmware)

Special Documentation
Proline Promag 800
OPC UA

Electromagnetic flowmeter
Cellular radio

Endress+Hauser
People for Process Automation

Table of contents

1 About this document 4
1.1 Document function 4
1.2 Target group 4
1.3 Using this document 4
1.4 Symbols 5

2 Basic safety instructions 7
2.1 Requirements for personnel 7
2.2 Intended use 7
2.3 Workplace safety 7
2.4 Operational safety 7
2.5 Product safety 7
2.6 IT security 8
2.7 Device-specific IT security 8

3 Product features 11
3.1 Product features 11

4 Commissioning 11
4.1 Commissioning overview 11
4.2 Connection of Promag 800 to the OPC UA client via an MQTT broker 12

5 OPC UA parameters 22
5.1 "Connectivity" submenu 22

6 Diagnostics and troubleshooting 36
6.1 General troubleshooting 36
6.2 Diagnostic information on local display 38
6.3 Diagnostic information via communication interface 38
6.4 Adapting the diagnostic information ... 39
6.5 Overview of diagnostic information ... 39
6.6 Pending diagnostic events 39
6.7 Diagnostics list 40
6.8 Event logbook 40
6.9 Resetting the measuring device 43
6.10 Device information 44
6.11 Firmware history 44

1 About this document

1.1 Document function

It serves as a reference for setting up an OPC UA client, which calls up the device data via an MQTT broker and the Endress+Hauser OPC UA Connectivity Server.

1.2 Target group

The document is aimed at specialists who work with the device over the entire life cycle and perform specific configurations for IIoT and SCADA applications.

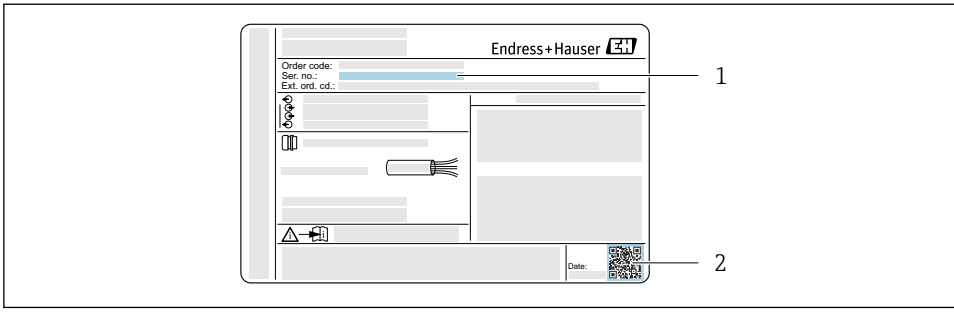
1.3 Using this document

1.3.1 Information on the document structure

This Special Documentation contains a range of information, including:
- Device-specific IT security
- Product features and availability
- Device operating options for accessing the OPC UA parameters
- Integration of the device into a plant network
- OPC UA information model

1.3.2 Device documentation

The relevant Operating Instructions, the description of the device parameters and all other technical documentation for the device are available via:
- Internet: *Device Viewer* (www.endress.com/deviceviewer):
  Enter the device serial number indicated on the transmitter nameplate.
- Smartphone/tablet: *Endress+Hauser Operations App* (App Store or Google Play):
  Enter the device serial number indicated on the transmitter nameplate or scan the 2-D matrix code (QR code) on the nameplate.



A0034947

1 *Example of a transmitter nameplate*

1 *Serial number (Ser. no.)*
2 *2-D matrix code (QR code)*

Technical documentation can also be downloaded from the Download Area of the Endress+Hauser website: www.endress.com → Download.

However this technical documentation applies to a particular instrument family and is not assigned to a specific measuring device.

1.4 Symbols

1.4.1 Safety symbols

DANGER
This symbol alerts you to a dangerous situation. Failure to avoid this situation will result in serious or fatal injury.

WARNING
This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in serious or fatal injury.

CAUTION
This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in minor or medium injury.

NOTICE
This symbol contains information on procedures and other facts which do not result in personal injury.

1.4.2 Symbols for certain types of Information

Symbol	Meaning
✓	**Permitted** Indicates procedures, processes or actions that are permitted.
✗	**Forbidden** Indicates procedures, processes or actions that are forbidden.

Symbol	Meaning
	**Tip** Indicates additional information.
	Reference to documentation
	Reference to page
	Reference to graphic
	Notice or individual step to be observed
1., 2., 3...	Series of steps
	Result of a step

1.4.3 Symbols in graphics

Symbol	Meaning
1, 2, 3,...	Item numbers
1., 2., 3...	Series of steps

1.4.4 Electrical symbols

Symbol	Meaning
	**Ground connection** A grounded terminal which, as far as the operator is concerned, is grounded via a grounding system.
	**Protective earth (PE)** Ground terminals that must be connected to ground prior to establishing any other connections. The ground terminals are located on the interior and exterior of the device: ▪ Inner ground terminal: protective ground is connected to the power supply network. ▪ Outer ground terminal: the device is connected to the grounding system of the facility.

1.4.5 Communication-specific symbols

Symbol	Meaning
	**Bluetooth** Wireless data transmission between devices over a short distance via radio technology.

2 Basic safety instructions

2.1 Requirements for personnel

Personnel involved in installation, commissioning, diagnostics and maintenance must meet the following requirements:
- Trained, qualified specialists must have a relevant qualification for this specific function and task
- Are authorized by the plant owner/operator
- Are familiar with federal/national regulations
- Before starting work, read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application)
- Follow instructions and comply with basic conditions

Operating personnel must meet the following requirements:
- Be instructed and authorized by the plant operator with regard to the requirements of the task
- Follow the instructions in this manual

2.2 Intended use

The designated use of the measuring device is described in the Operating Instructions pertaining to the device.

2.3 Workplace safety

For work on and with the device:
- Wear the required personal protective equipment according to federal/national regulations.

If working on and with the device with wet hands:
- It is recommended to wear gloves on account of the higher risk of electric shock.

2.4 Operational safety

Risk of injury!
- Operate the device in proper technical condition and fail-safe condition only.
- The operator is responsible for interference-free operation of the device.

Modifications to the device

Unauthorized modifications to the device are not permitted and can lead to unforeseeable dangers.
- If, despite this, modifications are required, consult with Endress+Hauser.

2.5 Product safety

This device is designed in accordance with good engineering practice to meet state-of-the-art safety requirements, has been tested, and left the factory in a condition in which it is safe to operate.

It meets general safety standards and legal requirements. It also complies with the EC directives listed in the device-specific EC Declaration of Conformity. Endress+Hauser confirms this by affixing the CE mark to the device.

2.6 IT security

Our warranty is valid only if the product is installed and used as described in the Operating Instructions. The product is equipped with security mechanisms to protect it against any inadvertent changes to the settings.

IT security measures, which provide additional protection for the product and associated data transfer, must be implemented by the operators themselves in line with their security standards.

2.7 Device-specific IT security

The device offers a range of specific functions to support protective measures on the operator's side. These functions can be configured by the user and guarantee greater in-operation safety if used correctly. The following list provides an overview of the most important functions:

2.7.1 Access via the SmartBlue app

Two access levels (user roles) are defined for the device: the Operator user role and the Maintenance user role. The Maintenance user role is the default setting.

If a user-specific access code is not defined (in the Enter access code parameter), the default setting **0000** continues to apply and the Maintenance user role is automatically enabled. The device's configuration data are not write-protected and can be edited at all times.

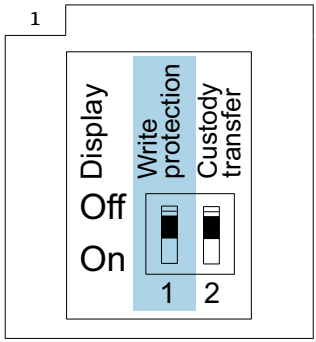
If a user-specific access code has been defined (in the Enter access code parameter), all the parameters are write-protected and the device is accessed with the Operator user role. The previously defined access code must first be entered again before the Maintenance user role is enabled and all the parameters can be write-accessed.

2.7.2 Protecting access via hardware write protection

Write access to the device parameters via the operating tool can be disabled by means of a write protection switch (DIP switch on the back of the local display). When hardware write protection is enabled, only read access to the parameters is possible.

Hardware write protection is disabled when the device is delivered.

Write protection via write protection switch



A0047361

- Information regarding the write protection switch is provided on the connection nameplate in the connection compartment cover.

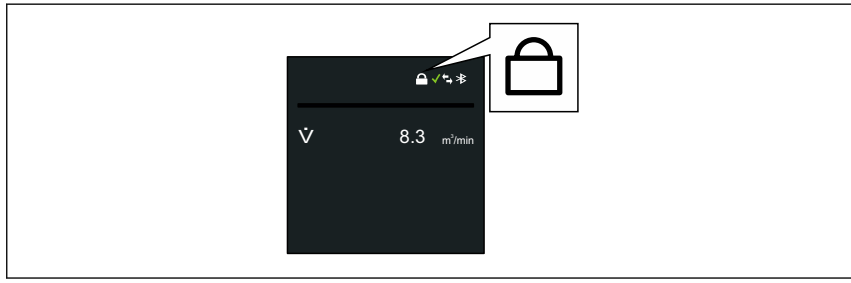
Unlike parameter write protection via a user-specific access code, this allows write access to the entire operating menu to be locked.

The parameter values are now read only and cannot be edited any more.

The following parameters can always be modified even if parameter write protection is activated:

- Enter access code
- Contrast display
- Clientt ID

1. Set the write protection (WP) switch on the display module to the **ON** position.
   ↳ Hardware write protection is enabled.
   In the **Locking status** parameter, the **Hardware locked** option is displayed.
   On the local display, the symbol appears in the header.



A0044218

2.

2.7.3 Access via Bluetooth® wireless technology

Secure signal transmission via Bluetooth® wireless technology uses an encryption method tested by the Fraunhofer Institute.

- The device is not visible via *Bluetooth*® wireless technology without the SmartBlue App.
- Only one point-to-point connection is established between the device and a smartphone or tablet.
- It is possible to configure the *Bluetooth*® wireless technology interface in such a way that *Bluetooth*® is only active (the device is only then visible) if the display is activated onsite via Wake on Touch.

3 Product features

3.1 Product features

With the OPC UA, the device can communicate with an OPC UA client and be integrated into Industrial Internet of Things (IIoT) and Supervisory Control And Data Acquisition (SCADA) applications. Integration is via the MQTT broker.

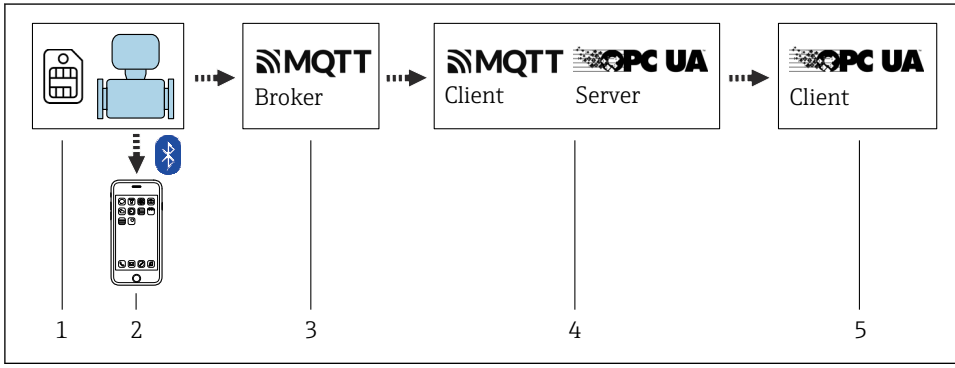
In addition to the measured values, device status information is also displayed, allowing users to monitor the status of the device.

The corresponding data can be taken either from the local display or via the SmartBlue App.

4 Commissioning

The MQTT broker and APN settings of the device must be configured before the device is integrated into an IIoT or SCADA application of a plant network. In addition, an MQTT broker must be set up and the OPC UA Connectivity Server must be configured. Only then can a connection be established between an OPC UA client and the device via the OPC UA Connectivity Server and the MQTT broker. → 12.

4.1 Commissioning overview



A0044632

1 *SIM card, provided by the customer*
2 *SmartBlue App via Bluetooth, provided by Endress+Hauser*
3 *MQTT broker, provided by the customer*
4 *OPC UA Connectivity Server, provided by Endress+Hauser*
5 *OPC UA client, provided by the customer*

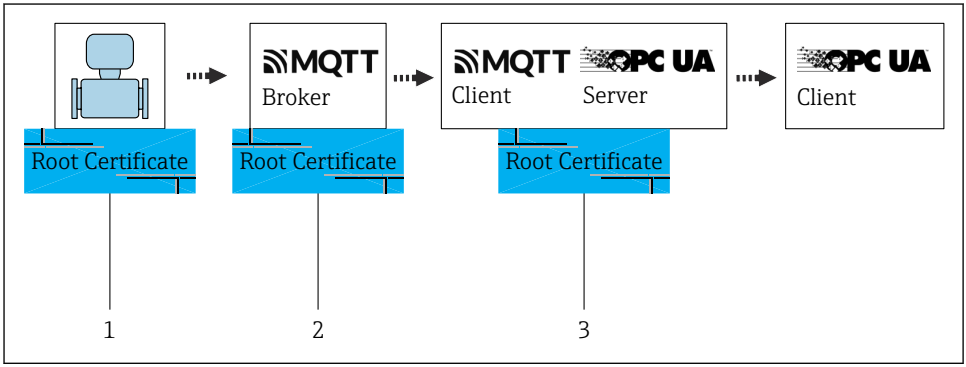
For custody transfer, once the device has been put into circulation or sealed, its operation is restricted. The device is only suitable for custody transfer measurement in conjunction with the display.

4.2 Connection of Promag 800 to the OPC UA client via an MQTT broker

Several steps must be performed to be able to access the measured values of the Promag 800. These steps are described below. The Promag 800 measured data reach the OPC UA client as follows: The Promag 800 sends the data to an MQTT broker via the MQTT network protocol. The Endress+Hauser OPC UA Connectivity Server is set up in such a way that it connects to the MQTT broker and makes these data available in a structured manner via OPC UA. An OPC UA client is then used to access the measured data via the OPC UA Connectivity Server.

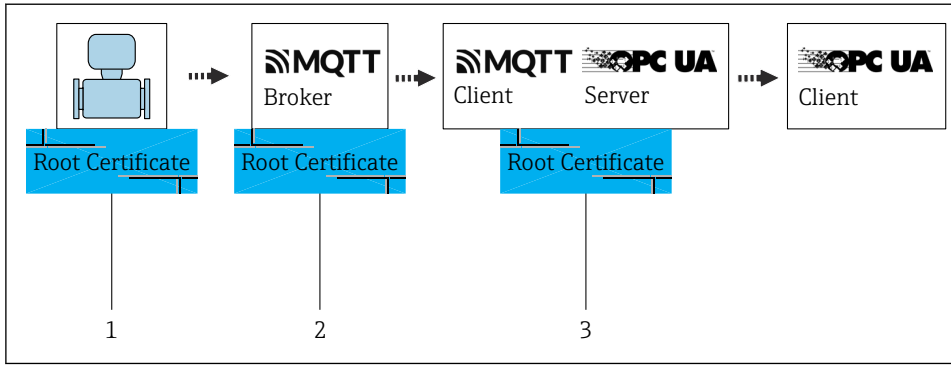
4.2.1 MQTT broker setup

Before setting up an MQTT broker, pay attention to the connection options listed below. The TLS encryption protocol must be used for wireless communication between the Promag 800 and the MQTT broker. Otherwise it is not possible to connect to the Promag 800. Four connection options can be derived from this:



2 *Server authentication without MQTT broker user name+password (root CA certificate required)*

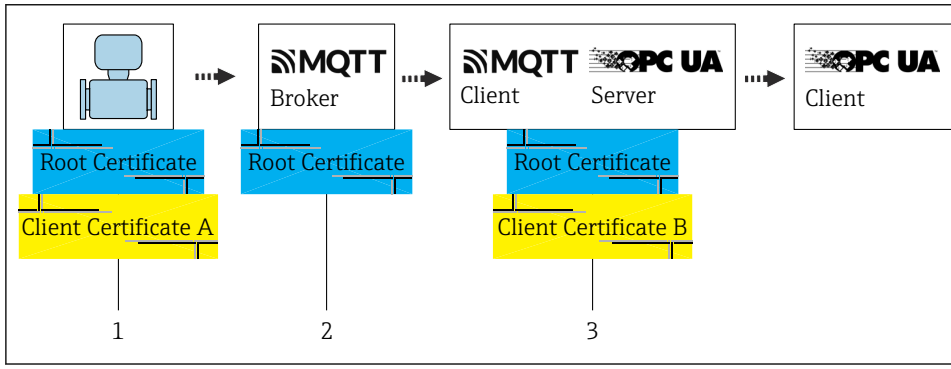
1 Root certificate
2 Root certificate
3 Root certificate



3 *Server authentication with MQTT broker user name+password (root CA certificate required)*

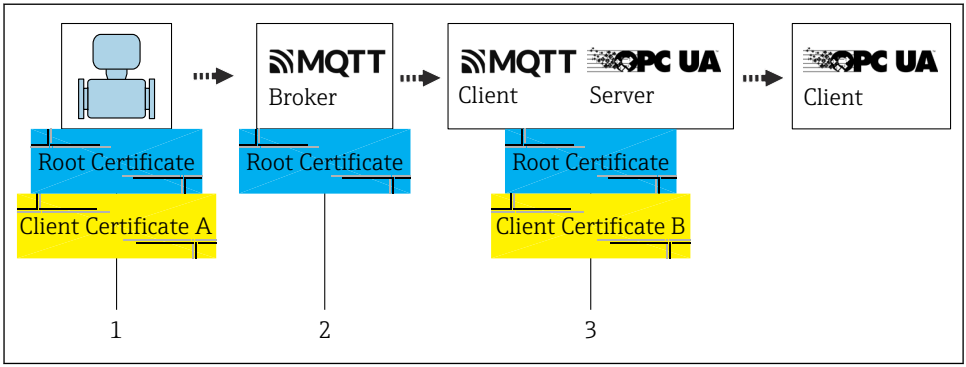
1 *Root certificate+user name+password*
2 *Root certificate+user name+password*
3 *Root certificate+user name+password*

The user name+password are defined in the MQTT broker.



4 *Server authentication and client authentication without MQTT broker user name+password (root CA certificate and client certificate required)*

1 *Root certificate+client certificate A*
2 *Root certificate*
3 *Root certificate+client certificate B*



5 Server authentication and client authentication with MQTT broker user name+password (root CA certificate and client certificate required)

1 Root certificate+client certificate A+user name+password
2 Root certificate+user name+password
3 Root certificate+client certificate A+user name+password

The user name+password are defined in the MQTT broker.

When establishing a connection between the Promag 800 (client) and the MQTT broker (server), the MQTT broker must be authenticated to the Promag 800 with a certificate (server authentication). It is also possible for the Promag 800 to be authenticated to the MQTT broker with its own client certificate (client authentication).

The MQTT broker setup is described in the documentation of the MQTT broker of your choice. Once the MQTT broker has been set up, at least one MQTT broker URL and one MQTT broker port should be available (e.g.: URL: mqtt.mycompany.com, port: 8883). The root CA certificate is also required. This allows the Promag 800 to authenticate the MQTT broker.

A variety of certificates can be created with "open SSL" (freeware).

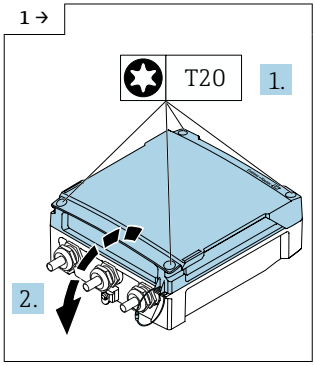
4.2.2 Inserting the SIM card

The device is equipped with an Endress+Hauser eSIM. The device automatically recognizes an additional SIM card that has been inserted.

The additionally inserted SIM card may not be protected by a PIN.

Only 1.8 V SIM cards are recognized.

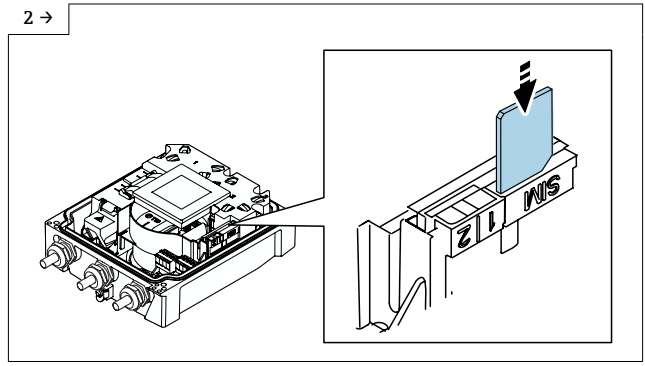
1 →



A0042838

- Open the connection compartment cover.

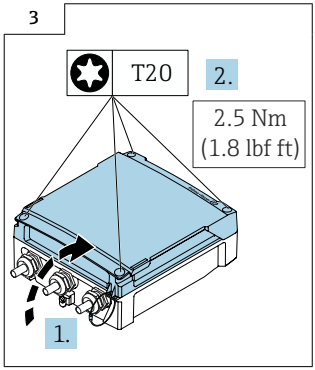
2 →



A0044342

- Remove the plastic cover of the SIM card slot.
- Insert the SIM card.
- Put the plastic cover of the SIM card slot back on.

3



A0042855

- Close the connection compartment cover.

4.2.3 Device setup using the E+H SmartBlue App

Access to the operating menu via the SmartBlue app

The device can be operated and configured via the SmartBlue app. In this case, the connection is established via the Bluetooth® wireless technology interface.

Supported functions
- Device selection in Live List and access to the device (login)
- Configuration of the device
- Access to measured values, device status and diagnostic information
- Data logger readout
- Certificate management
- Device software update
- Heartbeat report
- Parameter report

The SmartBlue app is available to download free of charge for Android devices (Google Playstore) and iOS devices (iTunes Apple Store): *Endress+Hauser SmartBlue*

Directly to the app with the QR code:

A0033202

- For energy-saving reasons, if the device is not powered by a power unit, it is only visible in the live list for 10 seconds every minute.
- The device appears immediately in the live list if the local display is touched for 5 seconds.
- The device with the highest signal strength appears at the very top of the live list.

Forgotten your password: contact Endress+Hauser Service.

Setting up Promag 800 with the SmartBlue App

1. Open the SmartBlue App.
2. Enter the user name.
   ↳ admin
3. Enter the password.
   ↳ Serial number of the device (case sensitive).

Login is successful.

Setting up the APN in the SmartBlue App:

1. Open the **System** menu.
2. Open the **Connectivity** submenu.
3. Open the **Cellular radio network** submenu.
4. Open the **Access data** submenu.

5. Edit the **APN name** parameter.
   ↳ As per the cellular communications provider.
6. Optional: enter the **APN user name** parameter.
7. Optional: enter the **APN password** parameter.

APN is set up.

Setting up the DNS server IP and the NTP server:

1. Open the **System** menu.
2. Open the **Connectivity** submenu.
3. Open the **Cellular radio network** submenu.
4. Open the **DNS configuration** submenu.
5. Enter the **DNS server IP** parameter.
   ↳ This is only necessary if the URL of the MQTT broker is not publicly accessible.

The DNS server IP and NTP server are set up.

Setting up the MQTT broker configuration in the SmartBlue App:

1. Open the **System** menu.
2. Open the **Connectivity** submenu.
3. Open the **Cloud** submenu.
4. Open the **MQTT configuration** submenu.
5. Edit the **MQTT broker port** parameter.
6. Enter the URL with the data of the configured MQTT broker.
7. Optional: enter the **MQTT user name** parameter.
8. Optional: enter the **MQTT password** parameter.

Make sure that the SmartBlue app and device firmware are up-to-date.

Renew the certificates:

1. Open the **Guidance** menu.
2. Open the **Update certificates** wizard.
3. Follow the instructions in the **SmartBlue app**.
   ↳ The certificates are renewed.

Install the root CA certificate of the MQTT broker on the Promag 800:

This step is needed to verify the MQTT broker to the Promag 800.

For this, save the root CA certificate on the smartphone under the following path.

- Android: *internal storage/SmartBlue/Documents/*
- iOS: */files/my Iphone/SmartBlue/*

1. Open the **SmartBlue App**.
2. Open the **Guidance** menu.
3. Open the **Update certificates** wizard.
   ↳ Follow the instructions in the **SmartBlue app**.
4. Under **Select step**, select **Write TCC to device**.

The root CA certificate is installed.

Install a client certificate on the Promag 800:

This step must only be performed if client authentication is required.

a) Create a CSR (certificate signing request):

A new **Public+Private Key pair** must first be generated, and a **CSR** must then be generated from this.

1. Open the **SmartBlue App**.
2. Open the **Guidance** menu.
3. Open the **Update certificates** wizard.
   ↳ Follow the instructions in the **SmartBlue app**.
4. Under **Select step**, select **Get CSR**.
   ↳ It can take up to 30 seconds for the CSR configuration to be completed.
   When the wizard is finished, the **CSR_from_device.csr.** file can be found at the following path:

- Android: internal storage/SmartBlue/Documents/
- iOS: /files/my Iphone/SmartBlue

b) Create a client certificate:

1. Use the CSR file to get it signed by a certificate authority (CA).
   ↳ The client certificate has been created.
2. Save the client certificate on the smartphone under the following path:

- Android: internal storage/SmartBlue/Documents/
- iOS: /files/my Iphone/SmartBlue/

c) Write the client certificate to Promag 800:

This step must only be performed if client authentication is required.

1. Open the **Guidance** menu.
2. Open the **Update certificates** wizard.
   ↳ Follow the instructions in the SmartBlue app.
3. Under **Select step**, select **Write SPK to device**.
4. Select client certificate.

When the wizard is finished, the client certificate is written to the device.

Renew the certificates:

1. Open the **Guidance** menu.
2. Open the **Update certificates** wizard.
3. Follow the instructions in the **SmartBlue app**.
   ↳ The certificates are renewed.

To check whether the Promag 800 was able to connect to the network provider, open the following path in the SmartBlue App: **Settings/System/Connectivity/Cellular network/Information**. If a network provider is entered here, it was possible to establish the connection.

To check whether the Promag 800 was able to establish a connection to the MQTT broker, open the following path in the SmartBlue App: **Settings/System/Connectivity/Cloud/MQTT/Information**. If the **MQTT broker status** is set to **Connection OK** and the status of **MQTT TLS certificate valid** is set to **Yes**, the connection has been established successfully.

A client certificate is preinstalled on the Promag 800. This is signed by an Endress+Hauser CA. This certificate will expire 5 years after device production. To be able to use client authentication, an individual client certificate that has been signed by a CA must be made available. If operating without client certificates, after 5 years the device will display a warning that the preinstalled client certificate has expired: in this case the message can be simply ignored.

4.2.4 OPC UA Connectivity Server Setup (OPC UA Server)

1. Download the **Promag W 800 OPC UA Server**
   ↳ https://www.endress.com
2. Click Downloads.
3. Click Software.
4. Product root: Enter 5W8C.
5. Text search: Enter OPC UA.
6. Click "Proline Promag W 800 OPC/UA Connectivity Server".
7. Click Download.
8. Double-click the **OPC UA Connectivity Server.exe** to run the installation package.
9. Follow the instructions that are given during the installation and start the Configurator via the OPC UA Connectivity Server icon on the desktop.
10. Activate the free software in the Endress+Hauser software portalhttps://www.software-products.endress.com.
11. Click **Add new data source**.
12. Enter the **Broker name** and **Port**.
    ↳ Enter as defined in the MQTT broker.

13. Activate **TLS encryption**.
14. Enter the **user name** and **password**.
    ↳ Enter as defined when setting up the MQTT broker.
15. Install the CA certificate for the verification of the MQTT broker.
    ↳ The broker CA certificate must be installed on the OPC UA Connectivity Server host system under « Trusted Root Certification Authorities».
16. Double-click the CA file to start the Windows certificate import wizard.
    ↳ If client authentication is used on the MQTT broker, a client certificate must be added as a PFX file. The PFX file contains the client certificate and the client key. A PFX file can be created from the client certificate and client key using common **SSL tools**.
17. In the Configurator, enter the path to the PFX file and the PFX password.
    ↳ The Configurator setting is adopted when the PC or the **OPC UA Connectivity Server** service is restarted. The latter is located under **Computer Management/ Services and Applications**. Administrator rights are required in Windows for this. Under Windows, the service can be found under the name **EHOpcUaServer**.

The OPC UA Connectivity Server is designed for connection to an MQTT broker. The Promag 800 MQTT data cannot be used directly. Instead, the OPC UA Connectivity Server is needed to put the data into a structured format.

For detailed information on the "Connectivity Server", see the Special Documentation → 4

4.2.5 OPC UA client setup

1. Install and start an OPC UA client.
2. Enter the endpoint URL: **opc.tcp://<Host>:<Port>/Server**.
   ↳ If the OPC UA client application is installed on the same computer as the OPC UA Connectivity Server, this appears as follows: **opc.tcp://localhost:62541/Server**.
   Host: DNS name or IP address of the host system. Here, **localhost** stands for an OPC UA client installed locally (on the same computer as the OPC UA Connectivity Server).
   Port: Port of the OPC UA Connectivity Server; the default port is **62541**. The firewall must allow access to this port.
3. Connect the client to the server.
4. Search through the server address tree and select the measuring instrument (device serial number, pay attention to upper/lower case).
5. Check the measured values (Serial Number/ValueDataLogger/Volume Flow).

OPC UA client setup is finished.

The OPC UA Connectivity Server normally generates a machine-specific, self-signed certificate for authentication when it is started for the first time. The OPC UA Client must trust the certificate of the server to establish communication. The self-signed certificate can be replaced by the server administrator.

4.2.6 Switching to the Endress+Hauser Netilion solution

If, during installation, another solution is found to be preferable, it is always possible to switch to the Endress+Hauser Netilion solution. With Netilion, it is possible to directly access device data via a cloud solution without having to integrate an MQTT broker or reconfigure the device.

For this purpose, reset the device to the factory settings and renew the certificates.

Reset the device to the factory settings:

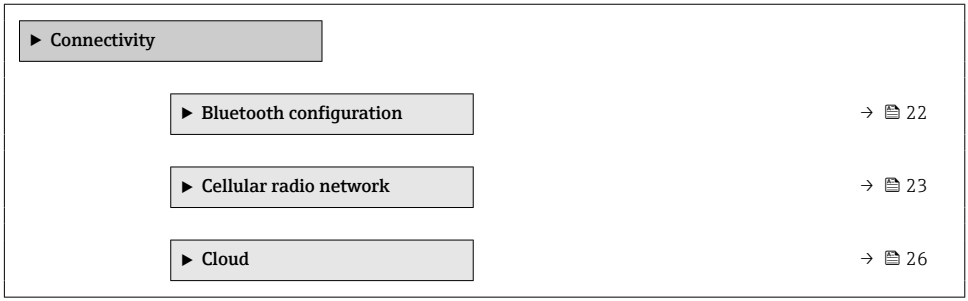
1. Open the **System** menu.
2. Open the **Device management** submenu.
3. Open the **Device reset** parameter.
4. Select the **To delivery settings** option.
5. Follow the instructions in the **SmartBlue app**.
   ↳ The device is reset to the factory settings.

Detailed information regarding "onboarding":

5 OPC UA parameters

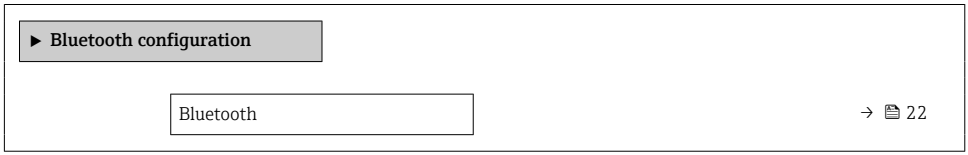
5.1 "Connectivity" submenu

Navigation
"System" menu → Connectivity



5.1.1 "Bluetooth configuration" submenu

Navigation
"System" menu → Connectivity → Bluetooth configuration



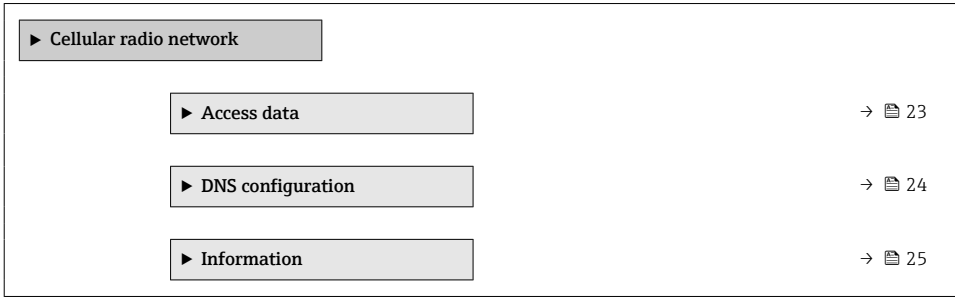
Parameter overview with brief description

Parameter	Description	Selection
Bluetooth	Enable or disable Bluetooth function.	▪ Enable ▪ On touch ▪ Not available *

* Visibility depends on order options or device settings

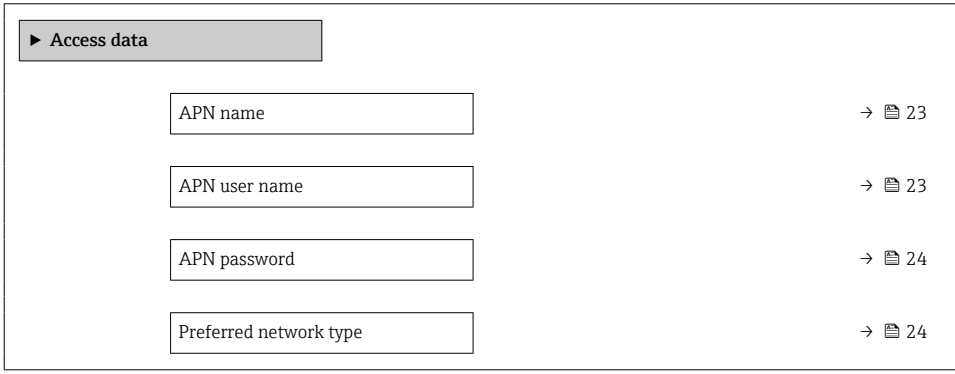
5.1.2 "Cellular radio network" submenu

Navigation
"System" menu → Connectivity → Cellular radio network



"Access data" submenu

Navigation
"System" menu → Connectivity → Cellular radio network → Access data



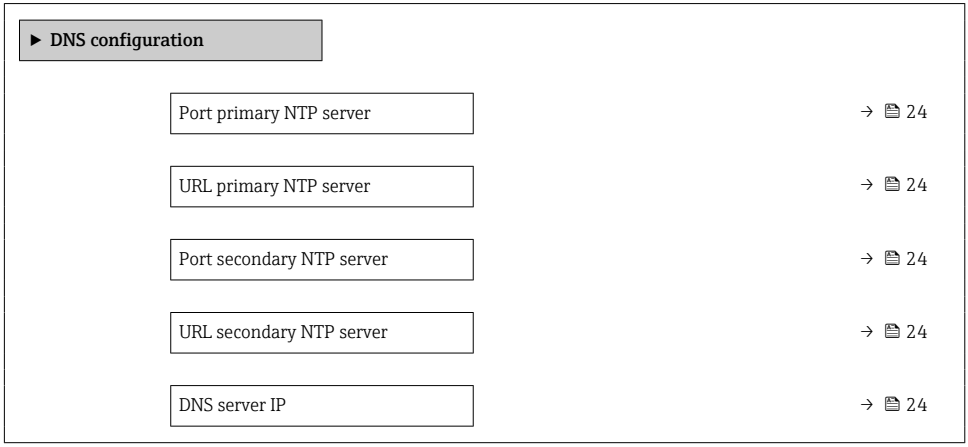
Parameter overview with brief description

Parameter	Description	User entry / Selection
APN name	Shows or enter the access point name (APN) used by the cellular service provider for your SIM card.	Character string comprising numbers, letters and special characters (32)
APN user name	Shows or enter the APN user name used by the cellular service provider for your SIM card.	Character string comprising numbers, letters and special characters (32)

Parameter	Description	User entry / Selection
APN password	Enter the APN password according to the information provided by your cellular network provider.	Character string comprising numbers, letters and special characters (32)
Preferred network type	Select the preferred network type to use to connect to a cellular network.	▪ GSM ▪ LTEM1 ▪ LTE-NB-IoT ▪ Automatic

"DNS configuration" submenu

Navigation
"System" menu → Connectivity → Cellular radio network → DNS configuration

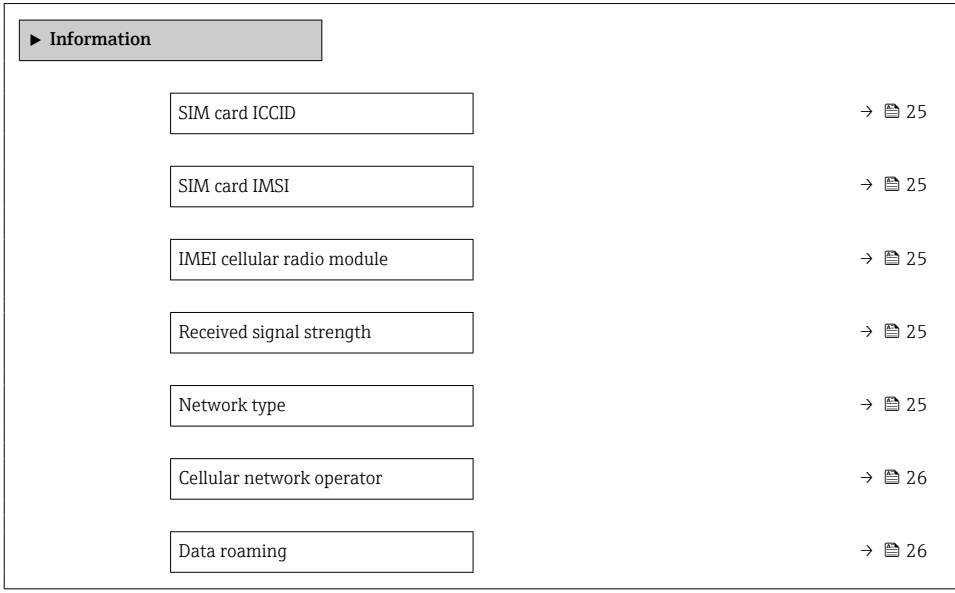


Parameter overview with brief description

Parameter	Description	User entry
Port primary NTP server	Enter the port of the primary NTP server.	0 to 65 535
URL primary NTP server	Enter the URL of the primary NTP server.	Character string comprising numbers, letters and special characters (100)
Port secondary NTP server	Enter the port of the secondary NTP server.	0 to 65 535
URL secondary NTP server	Enter the URL of the secondary NTP server.	Character string comprising numbers, letters and special characters (100)
DNS server IP	Enter the IP address of the DNS server.	Character string comprising numbers, letters and special characters (100)

"Information" submenu

Navigation
"System" menu → Connectivity → Cellular radio network → Information



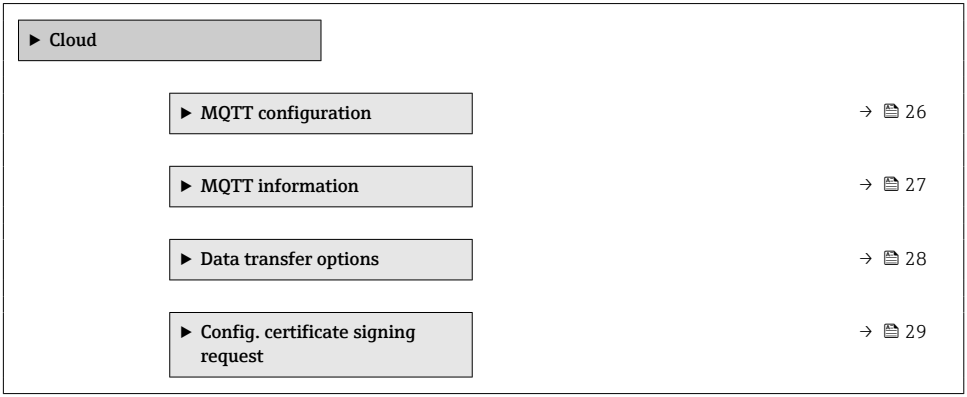
Parameter overview with brief description

Parameter	Description	User interface
SIM card ICCID	Shows ICCID of the SIM card.	Character string comprising numbers, letters and special characters
SIM card IMSI	Shows IMSI of the SIM card.	Character string comprising numbers, letters and special characters
IMEI cellular radio module	Shows IMEI of the cellular radio module.	Character string comprising numbers, letters and special characters
Received signal strength	Shows the received signal strength.	0 to 255 %
Network type	Shows network type used for the cellular radio connection.	▪ GSM ▪ LTEM1 ▪ LTE-NB-IoT ▪ None

Parameter	Description	User interface
Cellular network operator	Shows the cellular network operator currently used.	Character string comprising numbers, letters and special characters
Data roaming	Shows whether the device is in data roaming mode. Additional charges may apply in data roaming mode.	▪ Not active ▪ Active

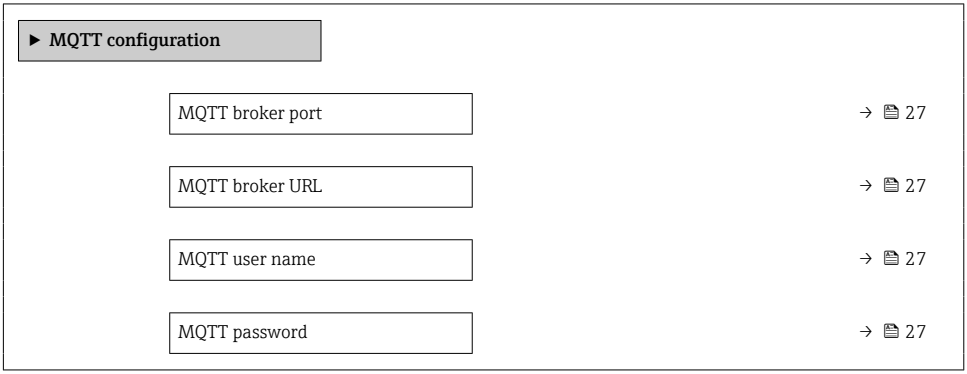
5.1.3 "Cloud" submenu

Navigation
"System" menu → Connectivity → Cloud



"MQTT configuration" submenu

Navigation
"System" menu → Connectivity → Cloud → MQTT configuration

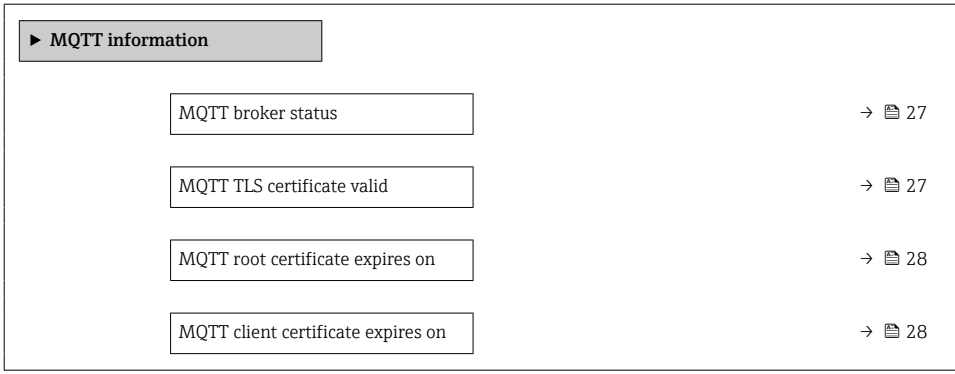


Parameter overview with brief description

Parameter	Description	User entry
MQTT broker port	Enter port of the MQTT broker.	0 to 65 535
MQTT broker URL	Enter URL of the MQTT broker.	Character string comprising numbers, letters and special characters (100)
MQTT user name	Enter user name for connection to the MQTT broker.	Character string comprising numbers, letters and special characters (32)
MQTT password	Enter password for connection to the MQTT broker.	Character string comprising numbers, letters and special characters (32)

"MQTT information" submenu

Navigation
"System" menu → Connectivity → Cloud → MQTT information



Parameter overview with brief description

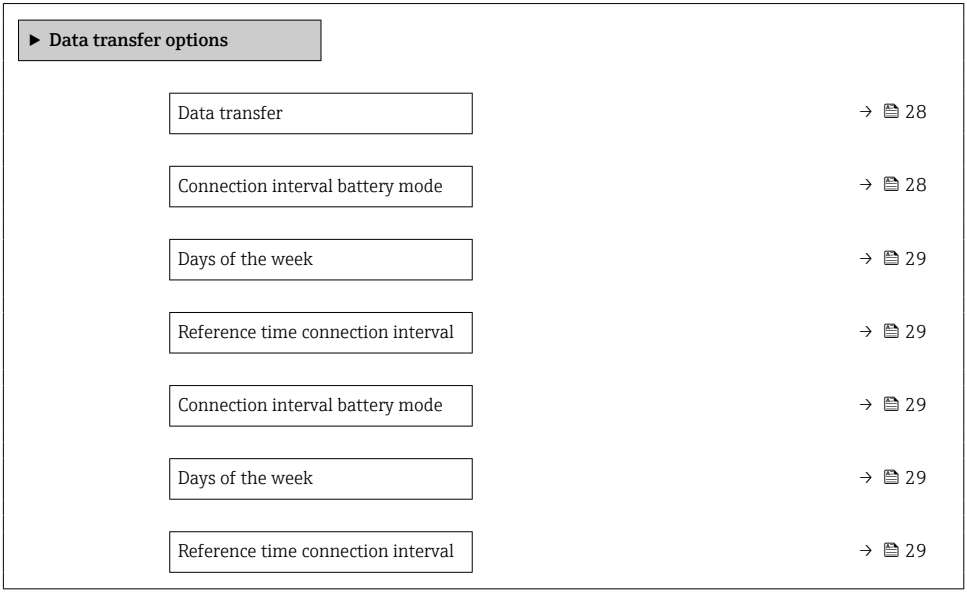
Parameter	Description	User interface
MQTT broker status	Shows status of the last connection to the MQTT broker.	▪ Connection OK ▪ Connecting ▪ No connection ▪ Not used
MQTT TLS certificate valid	Shows whether a valid TLS certificate is available to establish a connection to the MQTT broker.	▪ No ▪ Yes

Parameter	Description	User interface
MQTT root certificate expires on	Shows until which date the root certificate of the MQTT broker is valid.	Date
MQTT client certificate expires on	Shows until which date the measuring device certificate is valid.	Date

"Data transfer options" submenu

Navigation

"System" menu → Connectivity → Cloud → Data transfer options



Parameter overview with brief description

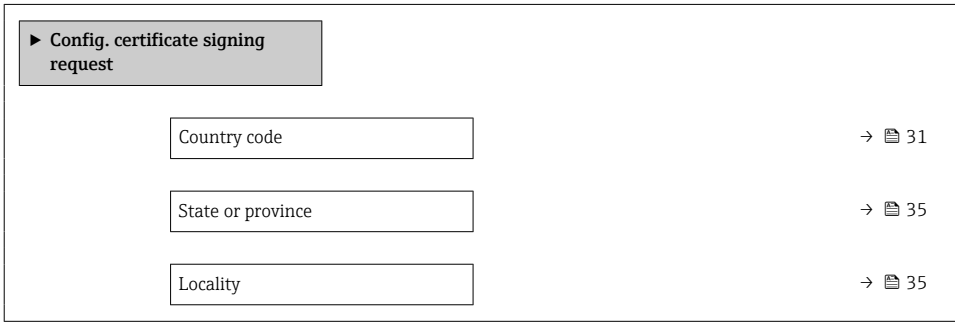
Parameter	Description	Selection / User entry
Data transfer	Enable or disable data transfer to the cloud.	▪ Disable ▪ Enable
Connection interval battery mode	Select the interval at which the measuring device connects to the MQTT broker in battery mode.	▪ 15 minutes ▪ 30 minutes ▪ 1 hour ▪ 2 hours ▪ 4 hours ▪ 6 hours ▪ 12 hours ▪ 24 hours

Parameter	Description	Selection / User entry
Days of the week	Select one or more days of the week on which the measuring device connects to the MQTT broker in battery mode.	▪ Sunday ▪ Monday ▪ Tuesday ▪ Wednesday ▪ Thursday ▪ Friday ▪ Saturday
Reference time connection interval	Enter time to which the interval of the connection to the MQTT broker refers. At this time a connection is guaranteed.	Time
Connection interval battery mode	Select the interval at which the measuring device connects to the MQTT broker in battery mode.	▪ 15 minutes ▪ 30 minutes ▪ 1 hour ▪ 2 hours ▪ 4 hours ▪ 6 hours ▪ 12 hours ▪ 24 hours
Days of the week	Select one or more days of the week on which the measuring device connects to the MQTT broker in battery mode.	▪ Sunday ▪ Monday ▪ Tuesday ▪ Wednesday ▪ Thursday ▪ Friday ▪ Saturday
Reference time connection interval	Enter time to which the interval of the connection to the MQTT broker refers. At this time a connection is guaranteed.	Time

"Config. certificate signing request" submenu

Navigation

"System" menu → Connectivity → Cloud → Config. certificate signing request



Organization	→ 36
Organization unit	→ 36

Parameter overview with brief description

Parameter	Description	Selection / User entry
Country code	Select the two-digit country code of the country in which the organization operates.	▪ -- ▪ AD : Andorra ▪ AE : United Arab Emirates ▪ AF : Afghanistan ▪ AG : Antigua and Barbuda ▪ AI : Anguilla ▪ AL : Albania ▪ AM : Armenia ▪ AO : Angola ▪ AQ : Antarctica ▪ AR : Argentina ▪ AS : American Samoa ▪ AT : Austria ▪ AU : Australia ▪ AW : Aruba ▪ AX : Åland Islands ▪ AZ : Azerbaijan ▪ BA : Bosnia and Herzegovina ▪ BB : Barbados ▪ BD : Bangladesh ▪ BE : Belgium ▪ BF : Burkina Faso ▪ BG : Bulgaria ▪ BH : Bahrain ▪ BI : Burundi ▪ BJ : Benin ▪ BL : Saint Barthélemy ▪ BM : Bermuda ▪ BN : Brunei Darussalam ▪ BO : Bolivia, Plurinational State of ▪ BQ : Bonaire, Sint Eustatius and Saba ▪ BR : Brazil ▪ BS : Bahamas ▪ BT : Bhutan ▪ BV : Bouvet Island ▪ BW : Botswana ▪ BY : Belarus ▪ BZ : Belize ▪ CA : Canada ▪ CC : Cocos (Keeling) Islands ▪ CD : Congo, the Democratic Republic of the ▪ CF : Central African Republic ▪ CG : Congo ▪ CH : Switzerland ▪ CI : Côte d'Ivoire ▪ CK : Cook Islands ▪ CL : Chile ▪ CM : Cameroon ▪ CN : China ▪ CO : Colombia

Parameter	Description	Selection / User entry
		▪ CR : Costa Rica ▪ CU : Cuba ▪ CV : Cabo Verde ▪ CW : Curaçao ▪ CX : Christmas Island ▪ CY : Cyprus ▪ CZ : Czechia ▪ DE : Germany ▪ DJ : Djibouti ▪ DK : Denmark ▪ DM : Dominica ▪ DO : Dominican Republic ▪ DZ : Algeria ▪ EC : Ecuador ▪ EE : Estonia ▪ EG : Egypt ▪ EH : Western Sahara ▪ ER : Eritrea ▪ ES : Spain ▪ ET : Ethiopia ▪ FI : Finland ▪ FJ : Fiji ▪ FK : Falkland Islands ▪ FM : Micronesia ▪ FO : Faroe Islands ▪ FR : France ▪ GR : Greece ▪ GB : United Kingdom of Great Britain and Northern Ireland ▪ GA : Gabon ▪ GP : Guadeloupe ▪ GE : Georgia ▪ GF : French Guiana ▪ GN : Guinea ▪ GM : Gambia ▪ GD : Grenada ▪ GG : Guernsey ▪ GH : Ghana ▪ GI : GI ▪ GL : Greenland ▪ GQ : Equatorial Guinea ▪ GS : South Georgia and the South Sandwich Islands ▪ GT : Guatemala ▪ GU : Guam ▪ GW : Guinea-Bissau ▪ GY : Guyana ▪ HK : Hong Kong ▪ HM : Heard Island and McDonald Islands ▪ HN : Honduras ▪ HR : Croatia ▪ HT : Haiti ▪ HU : Hungary ▪ IL : Israel

Parameter	Description	Selection / User entry
		▪ IE : Ireland ▪ ID : Indonesia ▪ IM : Isle of Man ▪ IN : India ▪ IO : British Indian Ocean Territory ▪ IQ : Iraq ▪ IR : Iran ▪ IS : Iceland ▪ IT : Italy ▪ JE : Jersey ▪ JM : Jamaica ▪ JO : Jordan ▪ JP : Japan ▪ KH : Cambodia ▪ KG : Kyrgyzstan ▪ KE : Kenya ▪ KI : Kiribati ▪ KM : Comoros ▪ KN : Saint Kitts and Nevis ▪ KP : Korea ▪ KR : Korea ▪ KW : Kuwait ▪ KY : Cayman Islands ▪ KZ : Kazakhstan ▪ LU : Luxembourg ▪ LI : Liechtenstein ▪ LC : Saint Lucia ▪ LB : Lebanon ▪ LA : Lao People's Democratic Republic ▪ LK : Sri Lanka ▪ LR : Liberia ▪ LS : Lesotho ▪ LT : Lithuania ▪ LV : Latvia ▪ LY : Libya ▪ MH : Marshall Islands ▪ ME : Montenegro ▪ MD : Moldova ▪ MC : Monaco ▪ MA : Morocco ▪ MF : Saint Martin ▪ MG : Madagascar ▪ MK : North Macedonia ▪ ML : Mali ▪ MM : Myanmar ▪ MN : Mongolia ▪ MO : Macao ▪ MP : Northern Mariana Islands ▪ MQ : Martinique ▪ MR : Mauritania ▪ MS : Montserrat ▪ MT : Malta

Parameter	Description	Selection / User entry
		▪ MU : Mauritius ▪ MV : Maldives ▪ MW : Malawi ▪ MX : Mexico ▪ MY : Malaysia ▪ MZ : Mozambique ▪ NE : Niger ▪ NF : Norfolk Island ▪ NG : Nigeria ▪ NC : New Caledonia ▪ NA : Namibia ▪ NI : Nicaragua ▪ NL : Netherlands ▪ NO : Norway ▪ NP : Nepal ▪ NR : Nauru ▪ NU : Niue ▪ NZ : New Zealand ▪ OM : Oman ▪ PA : Panama ▪ PE : Peru ▪ PF : French Polynesia ▪ PG : Papua New Guinea ▪ PH : Philippines ▪ PK : Pakistan ▪ PL : Poland ▪ PM : Saint Pierre and Miquelon ▪ PN : Pitcairn ▪ PR : Puerto Rico ▪ PS : Palestine ▪ PT : Portugal ▪ PW : Palau ▪ PY : Paraguay ▪ QA : Qatar ▪ RE : Réunion ▪ RO : Romania ▪ RS : Serbia ▪ RU : Russian Federation ▪ RW : Rwanda ▪ SA : Saudi Arabia ▪ SB : Solomon Islands ▪ SC : Seychelles ▪ SD : Sudan ▪ SE : Sweden ▪ SG : Singapore ▪ SH : Saint Helena, Ascension and Tristan da Cunha ▪ SI : Slovenia ▪ SJ : Svalbard and Jan Mayen ▪ SK : Slovakia ▪ SL : Sierra Leone ▪ SM : San Marino ▪ SN : Senegal ▪ SO : Somalia

Parameter	Description	Selection / User entry
		▪ SR : Suriname ▪ SS : South Sudan ▪ ST : Sao Tome and Principe ▪ SV : El Salvador ▪ SX : Sint Maarten ▪ SY : Syrian Arab Republic ▪ SZ : Eswatini ▪ TC : Turks and Caicos Islands ▪ TD : Chad ▪ TJ : Tajikistan ▪ TK : Tokelau ▪ TL : Timor-Leste ▪ TM : Turkmenistan ▪ TN : Tunisia ▪ TR : Turkey ▪ TT : Trinidad and Tobago ▪ TF : French Southern Territories ▪ TG : Togo ▪ TH : Thailand ▪ TO : Tonga ▪ TV : Tuvalu ▪ TW : Taiwan ▪ TZ : Tanzania ▪ UA : Ukraine ▪ UG : Uganda ▪ UM : United States Minor Outlying Islands ▪ US : United States of America ▪ UY : Uruguay ▪ UZ : Uzbekistan ▪ VA : Holy See ▪ VC : Saint Vincent and the Grenadines ▪ VE : Venezuela ▪ VG : Virgin Islands ▪ VI : Virgin Islands ▪ VN : Viet Nam ▪ VU : Vanuatu ▪ WF : Wallis and Futuna ▪ WS : Samoa ▪ YE : Yemen ▪ YT : Mayotte ▪ ZA : South Africa ▪ ZM : Zambia ▪ ZW : Zimbabwe
State or province	Enter the state or region in which the organization operates.	Character string comprising numbers, letters and special characters (32)
Locality	Enter the city or locality in which the organization is located.	Character string comprising numbers, letters and special characters (32)

Parameter	Description	Selection / User entry
Organization	Enter the organization to which the certificate applies.	Character string comprising numbers, letters and special characters (32)
Organization unit	Enter the organization unit to which the certificate applies.	Character string comprising numbers, letters and special characters (32)

6 Diagnostics and troubleshooting

6.1 General troubleshooting

For local display

Error	Possible causes	Remedial action
Local display remains dark for longer than 5 seconds when touched	Supply voltage does not match the voltage specified on the nameplate.	Apply the correct supply voltage .
	Supply voltage has incorrect polarity.	Reverse polarity of supply voltage.
	The connecting cables are not connected correctly.	Check the cable connection and correct if necessary.
	No battery pack inserted or connected. No buffer capacitor inserted or connected.	Insert or connect battery pack. Insert or connect buffer capacitor.
	Device is not powered from the mains.	Touch the display for 5 seconds .

For output signals

Error	Possible causes	Remedial action
Signal output outside the valid range	Main electronics module is defective.	Order spare part .
Device shows correct value on local display, but signal output is incorrect, though in the valid range.	Parameter configuration error	Check and adjust parameter configuration.
Device measures incorrectly.	Configuration error or device is operated outside the application.	1. Check and correct parameter configuration. 2. Observe limit values specified in the "Technical Data".
Measuring device not in smartphone or tablet live list	Bluetooth communication set to "on touch"	1. Check whether the Bluetooth logo is visible on the local display or not. 2. Touch the display for 5 seconds so that a measured value is displayed.

Error	Possible causes	Remedial action
Device not responding via SmartBlue app	No Bluetooth connection	Enable Bluetooth function on smartphone or tablet. The device is already connected to another smartphone/tablet.
Login via SmartBlue app not possible	Device is being put into operation for the first time	Enter initial password (device serial number) and change.
Device cannot be operated via SmartBlue app	Incorrect password entered	Enter correct password.
	Password forgotten	Contact Endress+Hauser Service.
No write access to parameters	Hardware write protection enabled	▪ Check user role ▪ Enter the correct customer-specific access code ▪ Hardware write protection via DIP switch

For access

Fault	Possible causes	Remedial action

SmartBlue operation with Bluetooth®

Error	Possible causes	Remedial action
Device is not visible in the live list	No Bluetooth connection	Enable Bluetooth in the device
	Bluetooth signal outside range	Reduce distance between device and smartphone/tablet
	Geopositioning is not enabled on Android devices or is not permitted for the SmartBlue app	Enable/permit the geopositioning service on Android device for the SmartBlue app
Device appears in the live list but a connection cannot be established	The device is already connected with another smartphone/tablet via Bluetooth. Only one point-to-point connection is permitted	Disconnect the smartphone/tablet from the device
	Incorrect user name and password	The standard user name is "admin" and the password is the device serial number indicated on the device nameplate (only if the password was not changed by the user beforehand) If the password has been forgotten, contact Endress+Hauser Service (www.addresses.endress.com)
Connection via SmartBlue not possible	Incorrect password entered	Enter the correct password, paying attention to lower/upper case
	Password forgotten	contact Endress+Hauser Service (www.addresses.endress.com)

Error	Possible causes	Remedial action
No communication with device via SmartBlue	No Bluetooth connection	Enable the Bluetooth function on the smartphone, tablet and device
	The device is already connected to another smartphone/tablet.	Disconnect the device from the other smartphone/tablet
	Ambient conditions (e.g. walls/tanks) disturbing the Bluetooth connection	Establish direct line-of-sight connection
Device cannot be operated via SmartBlue	**Operator** option has no authorization	Switch to the **Maintenance** option

6.2 Diagnostic information on local display

6.2.1 Diagnostic message

If two or more diagnostic events are pending simultaneously, only the message of the diagnostic event with the highest priority is shown.

6.3 Diagnostic information via communication interface

6.3.1 Reading out diagnostic information

Diagnostic information can be read out via Modbus RS485 register addresses.

- Via register address **6801** (data type = string): diagnosis code, e.g. F270
- Via register address **6821** (data type = string): diagnosis code, e.g. F270

For an overview of diagnostic events with diagnosis number and diagnosis code

6.3.2 Configuring error response mode

The error response mode for Modbus RS485 communication can be configured in the **Communication** submenu using 2 parameters.

Navigation path
Application → Communication

Parameter overview with brief description

Parameters	Description	Selection	Factory setting
Failure mode	Select measured value output behavior when a diagnostic message occurs via Modbus communication. The effect of this parameter depends on the option selected in the **Assign diagnostic behavior** parameter.	▪ NaN value ▪ Last valid value NaN ≡ not a number	NaN value

6.4 Adapting the diagnostic information

6.4.1 Adapting the diagnostic behavior

Each item of diagnostic information is assigned a specific diagnostic behavior at the factory. The user can change this assignment for specific diagnostic information in the **Diagnostic settings** submenu.

Diagnostics → Diagnostic settings

Options	Description
Alarm	The device stops measurement. The measured value output and totalizer assume the defined alarm condition. A diagnostic message is generated and the event with the highest priority is shown in alternation with the primary variable on the local display.
Warning	The device continues to measure. The measured value output and the totalizer are not affected. A diagnostic message is generated.
Logbook entry only	The device continues to measure. The diagnostic message is displayed only in the **Event logbook** submenu and is not displayed in alternation with the operational display.
Off	The diagnostic event is ignored, and no diagnostic message is generated or entered.

6.5 Overview of diagnostic information

The amount of diagnostic information and the number of measured variables affected increase if the measuring device has one or more application packages.

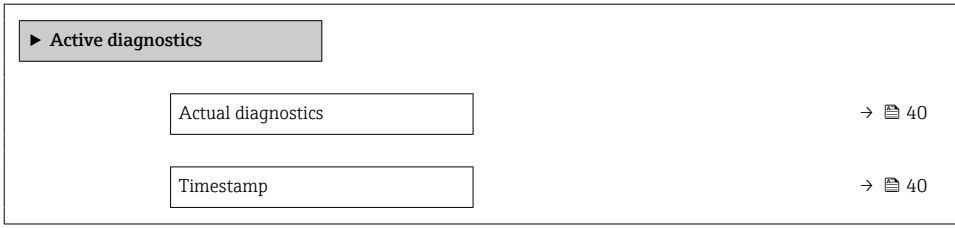
6.6 Pending diagnostic events

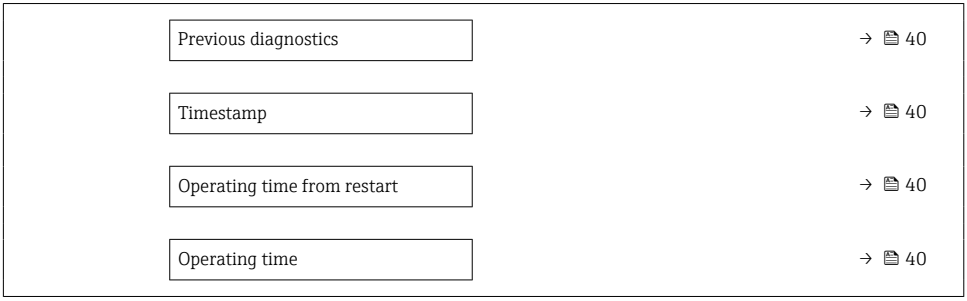
The **Diagnostics** menu allows the user to view the current diagnostic event and the previous diagnostic event separately.

To call up the measures to rectify a diagnostic event:
Via SmartBlue App

Other pending diagnostic events can be displayed in the **Diagnostic list** submenu
→ 📄 40

Navigation
"Diagnostics" menu → Active diagnostics





Parameter overview with brief description

Parameter	Description	User interface
Actual diagnostics	Shows the current occured diagnostic event along with its diagnostic information.	Positive integer
Timestamp	Displays the timestamp for the currently active diagnostic message.	Days (d), hours (h), minutes (m), seconds (s)
Previous diagnostics	Shows the diagnostic event that occurred prior to the current diagnostic event along with its diagnostic information.	Positive integer
Timestamp	Shows the timestamp of the previous diagnostic message.	Days (d), hours (h), minutes (m), seconds (s)
Operating time from restart	Shows the time the device has been in operation since the last device restart.	Days (d), hours (h), minutes (m), seconds (s)
Operating time	Indicates how long the device has been in operation.	Days (d), hours (h), minutes (m), seconds (s)

6.7 Diagnostics list

Up to 5 currently pending diagnostic events can be displayed in the **Diagnostic list** submenu along with the associated diagnostic information. If more than 5 diagnostic events are pending, the events with the highest priority are shown on the display.

Navigation path
Diagnostics → Diagnostic list

To call up the measures to rectify a diagnostic event:
Via SmartBlue App

6.8 Event logbook

6.8.1 Reading out the event logbook

A chronological overview of the event messages that have occurred is provided in the **Events list** submenu.

Navigation path
Diagnostics menu → **Event logbook** submenu → Events list

100 event messages can be displayed in chronological order.

The event history includes entries for:
- Diagnostic events → 📄 39
- Information events → 📄 41

In addition to the operating time when the event occurred, each event is also assigned a symbol that indicates whether the event has occurred or is finished:
- Diagnostics event
  - ⊕: Occurrence of the event
  - ⊖: End of the event
- Information event
  ⊕: Occurrence of the event

To call up the measures to rectify a diagnostic event:
Via SmartBlue App

For filtering the displayed event messages → 📄 41

6.8.2 Filtering the event logbook

Using the **Filter options** parameter you can define which category of event message is displayed in the **Events list** submenu.

Navigation path
Diagnostics → Event logbook → Filter options

Filter categories
- All
- Failure (F)
- Function check (C)
- Out of specification (S)
- Maintenance required (M)
- Information (I)

6.8.3 Overview of information events

Unlike a diagnostic event, an information event is displayed in the event logbook only and not in the diagnostic list.

Info number	Info name
I1000	--------(Device ok)
I1079	Sensor changed
I1089	Power on
I1090	Configuration reset
I1091	Configuration changed
I1092	HistoROM backup deleted

Info number	Info name
I1137	Electronic changed
I1151	History reset
I1155	Reset electronic temperature
I1156	Memory error trend
I1157	Memory error event list
I1256	Display: access status changed
I1264	Safety sequence aborted
I1278	I/O module restarted
I1335	Firmware changed
I1351	Empty pipe detection adjustment failure
I1353	Empty pipe detection adjustment ok
I1361	Web server: login failed
I1397	Fieldbus: access status changed
I1398	CDI: access status changed
I1443	Coating thickness not determined
I1444	Device verification passed
I1445	Device verification failed
I1457	Measurement error verification failed
I1459	I/O module verification failed
I1461	Sensor verification failed
I1462	Sensor electronic module verific. failed
I1512	Download started
I1513	Download finished
I1514	Upload started
I1515	Upload finished
I1517	Custody transfer active
I1518	Custody transfer inactive
I1554	Safety sequence started
I1555	Safety sequence confirmed
I1556	Safety mode off
I1618	I/O module 2 replaced
I1619	I/O module 3 replaced
I1621	I/O module 4 replaced

Info number	Info name
I1622	Calibration changed
I1624	Reset all totalizers
I1625	Write protection activated
I1626	Write protection deactivated
I1627	Web server: login successful
I1628	Display: login successful
I1629	CDI: login successful
I1631	Web server access changed
I1632	Display: login failed
I1633	CDI: login failed
I1634	Reset to factory settings
I1635	Reset to delivery settings
I1639	Max. switch cycles number reached
I1643	Custody transfer logbook cleared
I1649	Hardware write protection activated
I1650	Hardware write protection deactivated
I1651	Custody transfer parameter changed
I1712	New flash file received
I1725	Sensor electronic module (ISEM) changed
I1726	Configuration backup failed

6.9 Resetting the measuring device

The entire device configuration or some of the configuration can be reset to a defined state with the **Device reset** parameter (→ 43).

Navigation

"System" menu → Device management → Device reset

Parameter overview with brief description

Parameter	Description	Selection
Device reset	Reset the device configuration - either entirely or in part - to a defined state.	▪ Cancel ▪ To delivery settings ▪ Restart device ▪ Restore S-DAT backup *

* Visibility depends on order options or device settings

6.10 Device information

The **Device information** submenu contains all parameters that display different information for device identification.

Navigation

"System" menu → Information → Device

Parameter overview with brief description

Parameter	Description	User interface
Serial number	Shows the serial number of the measuring device.	Character string comprising numbers, letters and special characters
Order code	Shows the device order code.	Character string comprising numbers, letters and special characters
Firmware version	Shows the device firmware version installed.	Character string comprising numbers, letters and special characters
Extended order code 1	Shows the 1st part of the extended order code.	Character string comprising numbers, letters and special characters
Extended order code 2	Shows the 2nd part of the extended order code.	Character string comprising numbers, letters and special characters
Extended order code 3	Shows the 3rd part of the extended order code.	Character string comprising numbers, letters and special characters
Device name	Shows the name of the transmitter.	Character string comprising numbers, letters and special characters
ENP version	Shows the version of the electronic nameplate (ENP).	Character string comprising numbers, letters and special characters
Manufacturer		Character string comprising numbers, letters and special characters

6.11 Firmware history

Release date	Firmware version	Firmware changes	Documentation type	Documentation
03.2021	01.00.zz	Original firmware	Operating Instructions	BA02043D/06/EN/01.21

www.addresses.endress.com

Endress+Hauser

People for Process Automation