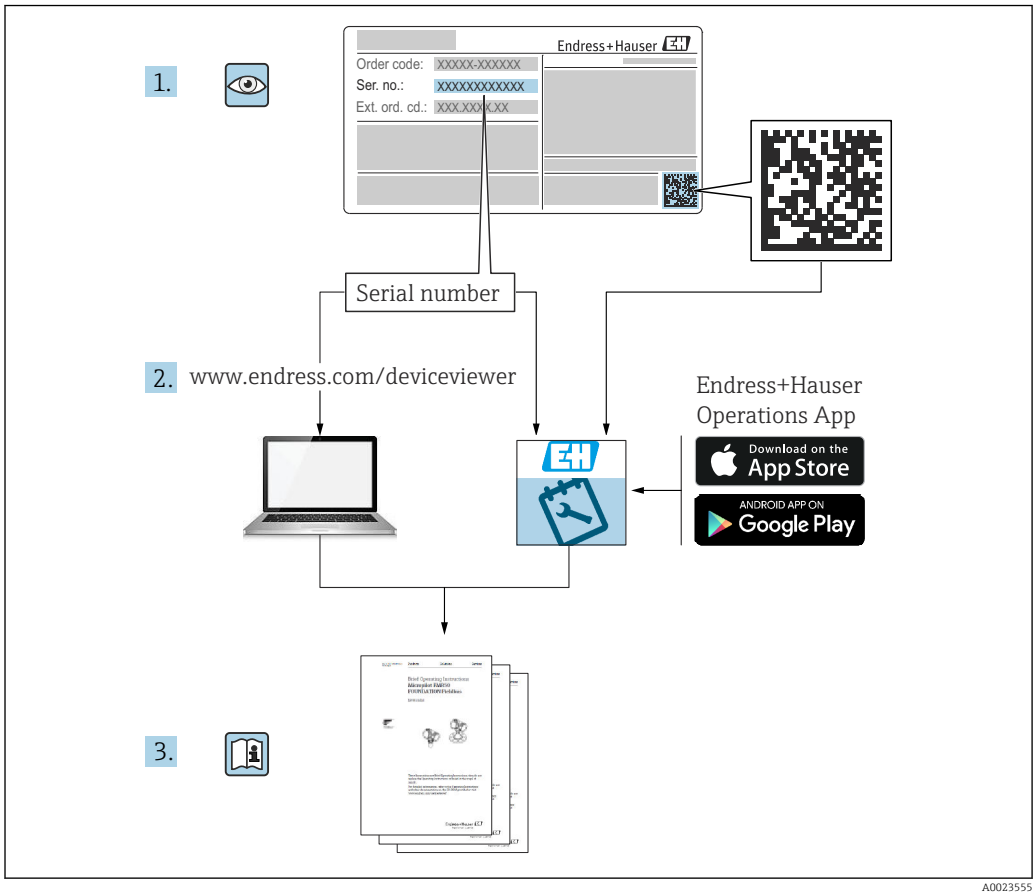
BA01778S/00/EN/05.26-00
71755806
2026-01-13

Operating Instructions
Fieldgate FXA42

System Products
Gateway for data transmission via Ethernet, WLAN or cellular radio

Endress+Hauser
People for Process Automation



- Make sure the document is stored in a safe place such that it is always available when working on or with the device.
- To avoid danger to individuals or the facility, read the **Basic safety instructions** section carefully, as well as all other safety instructions in the document that are specific to working procedures.
- The manufacturer reserves the right to modify technical data without prior notice. Your Endress+Hauser distributor will supply you with current information and updates to this manual.

Table of contents

1 About this document 4
1.1 Symbols 4
1.2 Registered trademarks 5

2 Basic safety instructions 6
2.1 Requirements for the personnel 6
2.2 Intended use 6
2.3 Workplace safety 6
2.4 Operational safety 6
2.5 Product safety 7

3 Product description 8
3.1 Product design 8

4 Incoming acceptance and product identification 10
4.1 Product identification 10
4.2 Scope of delivery 10
4.3 Manufacturer address 10

5 Installation 11
5.1 Installation conditions 11
5.2 Dimensions 11
5.3 Mounting procedure 12
5.4 Antenna 12
5.5 Post-installation check 13

6 Electrical connection 14
6.1 Supply voltage 14
6.2 RS485 serial interface (Modbus) 14
6.3 Terminal assignment 14

7 Commissioning 17
7.1 Display elements (device status indicator / LED) 17
7.2 Preparatory steps 18
7.3 Establishing the data connection 18
7.4 Installing the latest firmware 21
7.5 Configuration examples 22

8 Operation 40
8.1 Home page 40
8.2 Grid View 40
8.3 Fieldgate FXA42 editor 42
8.4 Settings 59
8.5 Event log messages at system start-up 104
8.6 Dojo Toolkit 107

9 Diagnostics and troubleshooting . . 108
9.1 Faults indicated by the LEDs 108
9.2 Restoring factory settings 108

10 Maintenance 108
10.1 Exterior cleaning 108

11 Repair 110
11.1 General information 110
11.2 Return 110
11.3 Disposal 110

12 Accessories 111
12.1 Device-specific accessories 111
12.2 Communication-specific accessories 111

13 Technical data 112
13.1 Input 112
13.2 Output 114
13.3 Environment 115
13.4 Certificates and approvals 116
13.5 Telecommunications approval 117

Index 119

1 About this document

1.1 Symbols

1.1.1 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.

1.1.2 Electrical symbols

Ground connection
Grounded clamp, which is grounded via a grounding system.

Signal ground connection
A terminal that can be used as a ground contact for the digital input.

1.1.3 Communication-specific symbols

Wireless Local Area Network (WLAN)
Communication via a wireless, local area network

LED is off

LED is on

LED is flashing

1.1.4 Symbols for certain types of Information

Tip
Indicates additional information

Reference to documentation

Reference to another section

1., 2., 3. Series of steps

1.1.5 Symbols in graphics

1, 2, 3 ... Item numbers

Hazardous area

Safe area (non-hazardous area)

1.2 Registered trademarks

Modbus®
Registered trademark of SCHNEIDER AUTOMATION, INC.

Microsoft®
Registered trademark of the Microsoft Corporation, Redmond, Washington, USA

2 Basic safety instructions

2.1 Requirements for the personnel

The personnel must fulfill the following requirements to carry out the necessary tasks, e. g., commissioning and maintenance:
- Trained, qualified specialists must have a relevant qualification for the specific function and task
- Are authorized by the plant owner/operator
- Are familiar with federal/national regulations
- Must have read and understood the instructions in the manual and supplementary documentation
- Follow instructions and comply with conditions

2.2 Intended use

2.2.1 Application

Fieldgates make it possible to remotely interrogate connected 4 to 20 mAModbus RS485 and Modbus TCP devices, either via Ethernet TCP/IP, WLAN or mobile telecommunications (UMTS, LTE-M and Cat NB1). The measured data are processed accordingly and forwarded to SupplyCare. In SupplyCare, the data are visualized, compiled into reports and used for other inventory management tasks. However, it is also possible to access the data transmitted by Fieldgate FXA42 without any additional software using the Web browser. Comprehensive configuration and automation capabilities are available for the Fieldgate FXA42 thanks to the integrated Web-PLC.

2.2.2 Incorrect use

The manufacturer is not liable for harm caused by improper or unintended use.

Clarification for borderline cases:
- With regard to special fluids and media used for cleaning, Endress+Hauser will be happy to assist in clarifying the corrosion-resistant properties of wetted materials but gives no guarantee or warranty as to the suitability of the materials.

2.2.3 Residual risks

When in operation, the housing may reach a temperature close to the process temperature.

Danger of burns from contact with surfaces!
- For elevated process temperatures, ensure protection against contact to prevent burns.

2.3 Workplace safety

When working on and with the device:
- Wear the required personal protective equipment as per national regulations.
- Switch off the supply voltage before connecting the device.

2.4 Operational safety

Risk of injury!
- Operate the device only if it is in proper technical condition, free from errors and faults.
- The operator is responsible for the 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 modifications are nevertheless required, consult with Endress+Hauser.

Hazardous area

To eliminate any danger to individuals or the facility when the device is used in the hazardous area (e.g. explosion protection, pressure vessel safety):

- Check the nameplate to verify if the device ordered can be put to its intended use in the hazardous area.
- Observe the instructions in the separate supplementary documentation. The separate supplementary documentation is an integral part of these Operating Instructions and can be in the form of an XA or SD document, for example.

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

The device also meets the legal requirements of the applicable UK regulations (Statutory Instruments). These are listed in the corresponding UKCA declaration of conformity along with the designated standards.

With selection of the order option for UKCA marking, Endress+Hauser confirms that the device has been successfully tested and evaluated in compliance with regulations by affixing the UKCA mark.

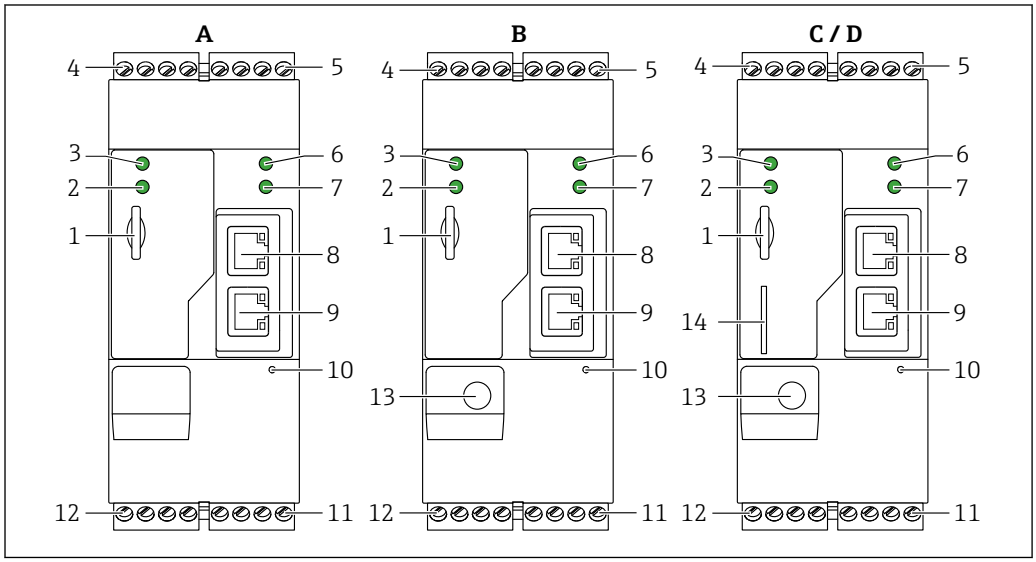
Contact address Endress+Hauser UK:
Endress+Hauser Ltd.
Floats Road
Manchester M23 9NF
United Kingdom
www.uk.endress.com

3 Product description

Information about accessories is provided in the **Accessories** section.

3.1 Product design

Four versions of the Fieldgate FXA42 are available. These versions differ in terms of the device features and data transmission technology.



1 *Fieldgate FXA42 versions and design*

A FXA42-A Ethernet
B FXA42-B Ethernet and WLAN
C FXA42-C Ethernet and 2G/3G
D FXA42-D Ethernet and LTE Cat M1 and Cat NB1 (2G/4G)
1 Slot for memory card, card type: microSD
2 Status LED for modem / WLAN / Ethernet
3 Status LED for supply voltage
4, 5 Input modules with analog input, digital input, current source and reference potential → 14
6 Status LED for network
7 Status LED for Web PLC
8, 9 Ethernet connections
10 Reset button
11 Power supply for Fieldgate FXA42, power supply for digital outputs, digital outputs → 14
12 RS-485 serial interface → 14
13 Connection for antenna (only WLAN and mobile telecommunications versions)
14 Slot for SIM card (only mobile telecommunications versions)

3.1.1 Supported frequency bands for mobile telecommunications

FXA42-C: supported frequency bands UMTS (2G/3G)

2G
Band 2 (1900 MHz), Band 3 (1800 MHz), Band 5 (850 MHz), Band 8 (900 MHz)

3G
Band 1 (2100 MHz), Band 2 (1900 MHz), Band 4 (1700 MHz), Band 5 (850 MHz), Band 6 (800 MHz), Band 8 (900 MHz)

FXA42-D: supported frequency bands LTE Cat M1 and Cat NB1 (2G/4G)

2G
Band 2 (1900 MHz), Band 3 (1800 MHz), Band 5 (850 MHz), Band 8 (900 MHz)

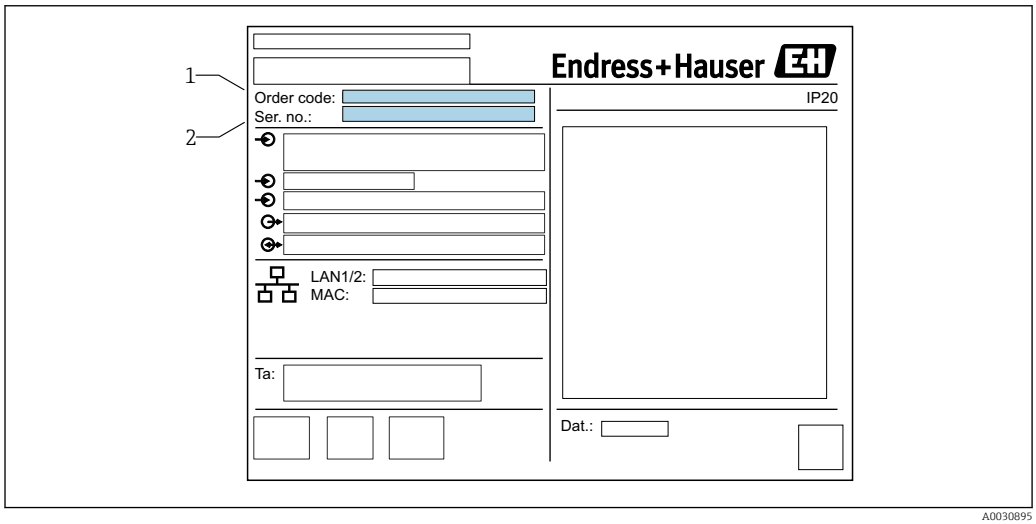
4G
Band 1 (2100 MHz), Band 2 (1900 MHz), Band 3 (1800 MHz), Band 4 (AWS 1700 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 12 (700 MHz), Band 13 (700 MHz), Band 18 (800 MHz), Band 19 (800 MHz), Band 20 (800 MHz), Band 26 (850 MHz), Band 28 (700 MHz)

4 Incoming acceptance and product identification

4.1 Product identification

The following options are available for identifying the gateway:
- Nameplate specifications
- Order code with breakdown of the device features on the delivery note
- Enter the serial number from the nameplate in *W@M Device Viewer* (www.endress.com/deviceviewer): all the information about the gateway is displayed.
- Enter the serial number on the nameplate into the *Endress+Hauser Operations App* or scan the 2-D matrix code (QR code) on the nameplate with the *Endress+Hauser Operations App*: all the information about the gateway is displayed.

4.1.1 Nameplate



1 Order code
2 Serial number

4.2 Scope of delivery

- Fieldgate FXA42 for DIN rail mounting
- SD card (card type: microSD), 1 GB
- Hard copy of Brief Operating Instructions

Information about accessories is provided in the **Accessories** section.

4.3 Manufacturer address

Endress+Hauser SE+Co. KG
Hauptstraße 1
79689 Maulburg, Germany

Place of manufacture: See nameplate.

5 Installation

5.1 Installation conditions

5.1.1 Temperature and humidity

Normal operation (EN 60068-2-14; Nb; 0.5 K/min): –20 to 60 °C (–4 to 140 °F)

Side by side installation: –20 to 50 °C (–4 to 122 °F)

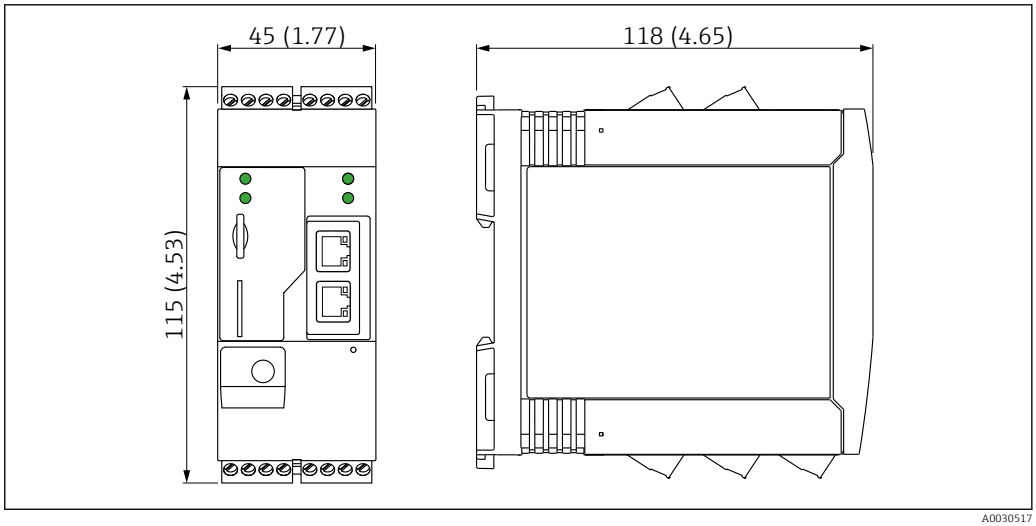
Avoid condensation.

Humidity (EN 60068-2-30; Db; 0.5 K/min): 5 to 85%; non-condensing

5.1.2 Orientation

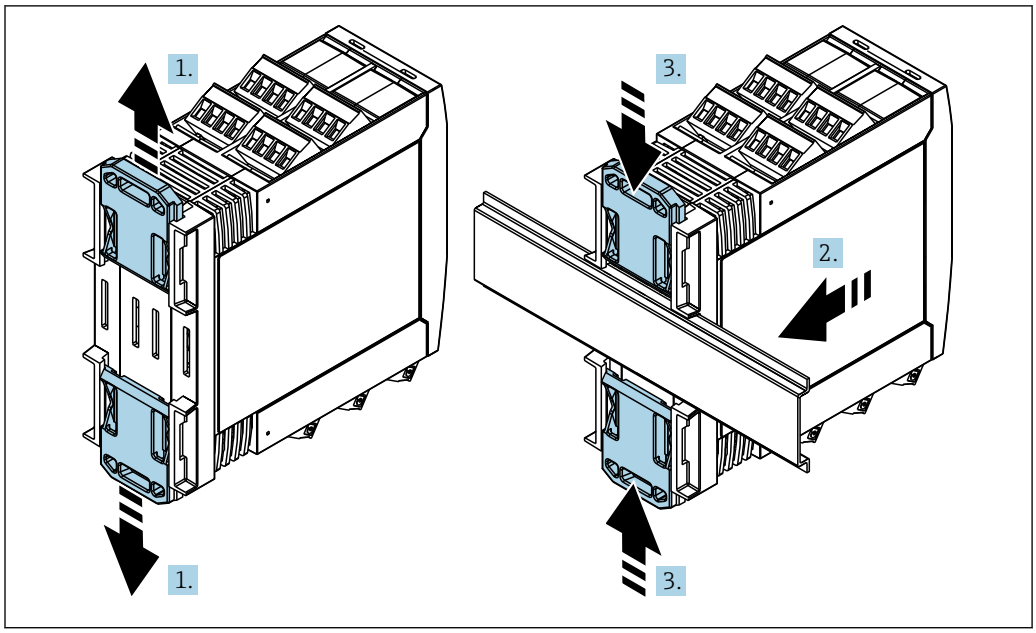
Vertical or horizontal on DIN rail (HT 35 as per EN 60715).

5.2 Dimensions



2 *Dimensions in mm (in)*

5.3 Mounting procedure



A0011766

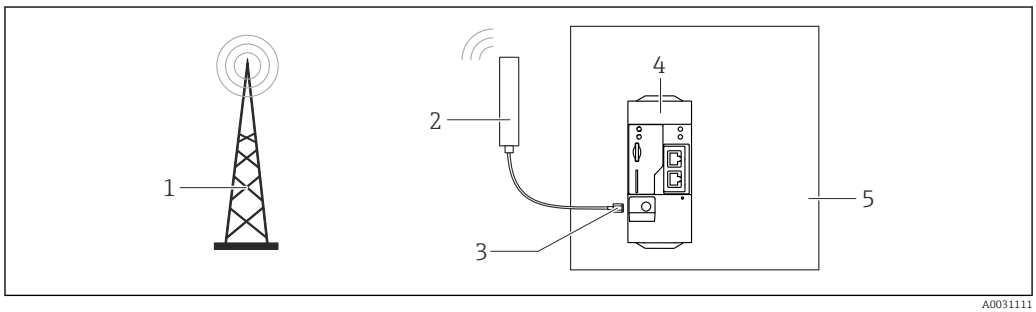
1. Slide the upper DIN rail clip upwards and the lower clip downwards until they click into place.
2. Fit the device on the DIN rail from the front.
3. Slide the two DIN rail clips back together until they click into place.

To disassemble the device, push the DIN rail clips up or down (see 1.) and remove the device from the rail. It also suffices to open just one of the DIN rail clips and then tilt the device to remove it from the rail.

5.4 Antenna

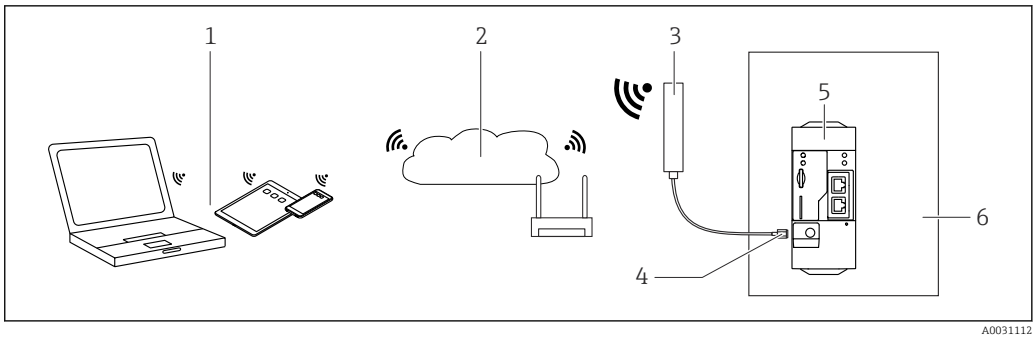
The devices require an external antenna for wireless communication via UMTS (2G/3G), LTE Cat M1 and Cat NB1 (2G/4G) and WLAN. The antenna can be purchased as an accessory from Endress+Hauser. The antenna cable is screwed onto the connection on the front of the device. The antenna must be mounted outside the cabinet or field housing. In areas with weak reception, it is advisable to first check the communication before securing the antenna permanently.

Connection: SMA connection.



A0031111

1 *Mobile communications networks*
2 *Antenna for Fieldgate FXA42*
3 *SMA connection*
4 *Fieldgate FXA42 Ethernet and 2G/3G/4G*
5 *Control cabinet*



1 WLAN receivers
2 Uplink to Internet or LAN via router
3 Antenna for Fieldgate FXA42
4 SMA connection
5 Fieldgate FXA42 Ethernet and WLAN
6 Control cabinet

5.5 Post-installation check

- Is the DIN rail clip clicked into place?
- Is the device securely seated on the DIN rail?
- Are all plug-in terminals securely engaged?
- Are the temperature limits observed at the mounting location?

6 Electrical connection

⚠ WARNING

Danger! Electric voltage!

Risk of electric shock and injury from startle response.

- De-energize all power sources before connecting.
- Before commissioning the device, measure the supply voltage and compare it with the voltage specifications on the nameplate. Only connect the device if the supply voltage measured matches the specifications.

6.1 Supply voltage

The supply voltage is 24 V_{DC} (±20 %). You may only use power units that ensure safe electrical isolation according to DIN VDE 0570-2-6 and EN61558-2-6 (SELV / PELV or NEC Class 2) and that are designed as limited-energy circuits.

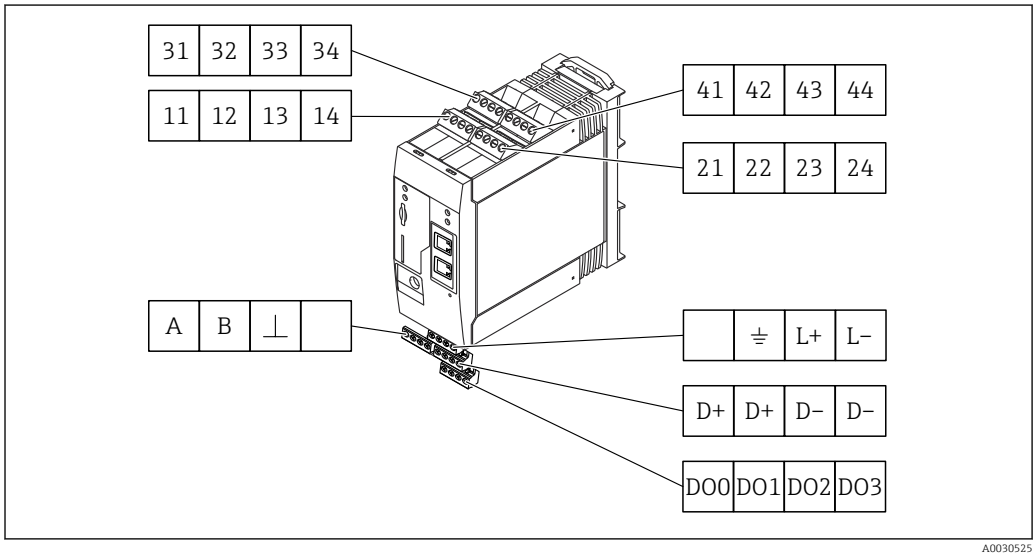
6.2 RS485 serial interface (Modbus)

Internal resistance: 96 kΩ

Protocol: Modbus RTU

External termination required (120 Ω)

6.3 Terminal assignment



A0030525

Terminal assignment of input modules				Properties	Function
11	21	31	41		GND
12	22	32	42	Input voltage L: < 5 V Input voltage H: > 11 V Input current: < 5 mA Maximum input voltage: 35 V	Digital input

Terminal assignment of input modules				Properties	Function
13	23	33	43	Maximum input voltage: 35 V Maximum input current: 22 mA Internal resistance: 250 Ω (suitable for HART communication)	Analog input4 to 20 mA
14	24	34	44	Output voltage: 28 V_{DC} (no-load) 26 V_{DC} @ 3 mA 20 V_{DC} @ 30 mA Output current: max. 160 mA The auxiliary voltage is short-circuit proof, galvanically isolated and non-stabilized.	Auxiliary voltage output The auxiliary voltage output can be used for loop power supply or to control the digital inputs.

Terminal assignment		Properties
DO0 DO1 DO2 DO3 Digital outputs	DO0	High-side driver, sourcing, DC-PNP. Output current: 500 mA
	DO1	
	DO2	
	DO3	
A B ⊥ RS485 serial interface (Modbus)	A	Signal
	B	Signal
	⊥	Ground / optional shield connection
		Not assigned

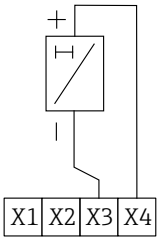
Terminal assignment		Properties
D+ D+ D− D− Power supply for digital outputs, 1)	D+	12 to 24 V_{DC}
	D+	12 to 24 V_{DC}
	D-	GND
	D-	GND
⏚ L+ L− Power supply for Fieldgate FXA42 1)		Not assigned
	⏚	Ground connection
	L+	24 V_{DC}
	L-	GND

1) You may only use power units that ensure safe electrical isolation according to DIN VDE 0570-2-6 and EN61558-2-6 (SELV / PELV or NEC Class 2) and that are designed as limited-energy circuits.

Analog input connection

2-wire

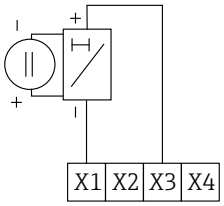
2W:



A0031282

4-wire

4W:

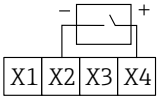


A0031283

Digital input connection

2-wire

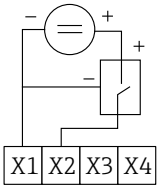
2W:



A0031284

3-wire

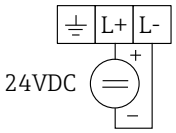
3W:



A0031285

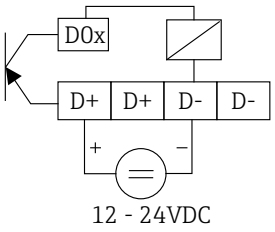
Power supply connection and digital output connection

Power supply



A0031288

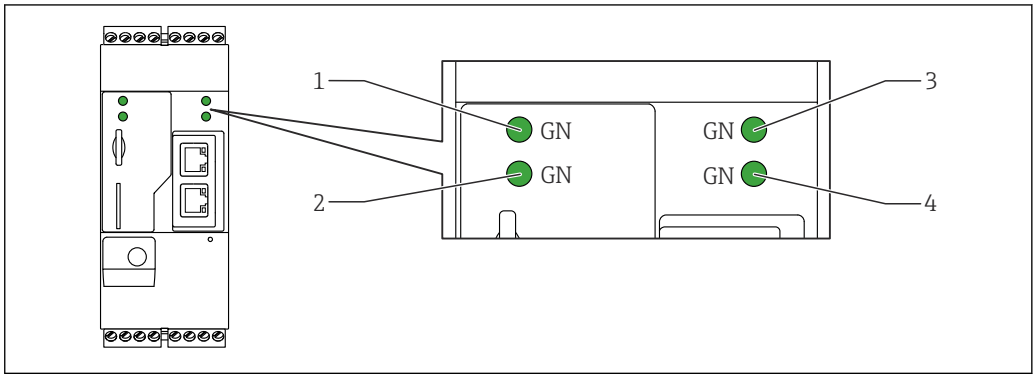
Digital output



A0031286

7 Commissioning

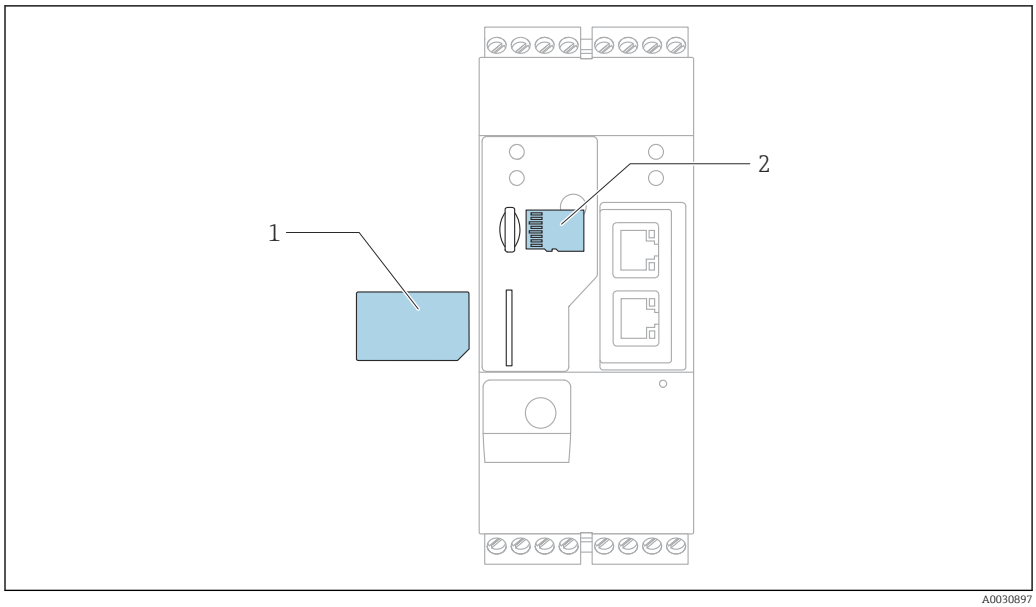
7.1 Display elements (device status indicator / LED)



1 Power
2 Modem (mobile communications versions) / WLAN / Ethernet
3 Network
4 Web-PLC

Description	State	Color	Meaning	Note
Power		Green (GN)	Power supply on	
Modem		Green (GN)	Power supply for modem on	Only mobile communications versions
WLAN		Green (GN)	Power supply for WLAN module on	Only WLAN version
Ethernet		Green (GN)	Power supply for Ethernet interface on	Only Ethernet version
Network		Green (GN)	Data connection established	Ethernet version: valid fixed IP address configured or DHCP completed successfully
Network			Data connection interrupted	Ethernet version: no valid fixed IP address configured or DHCP not completed successfully
Web-PLC		Green (GN)	Editor program for Web-PLC is enabled	
	2 x	Green (GN)	Manual firmware update completed successfully	
	2 x	Green (GN)	Reset to factory settings (factory reset) confirmed	

7.2 Preparatory steps



1 SIM card
2 SD card (microSD)

The SD card is already installed and formatted on delivery.

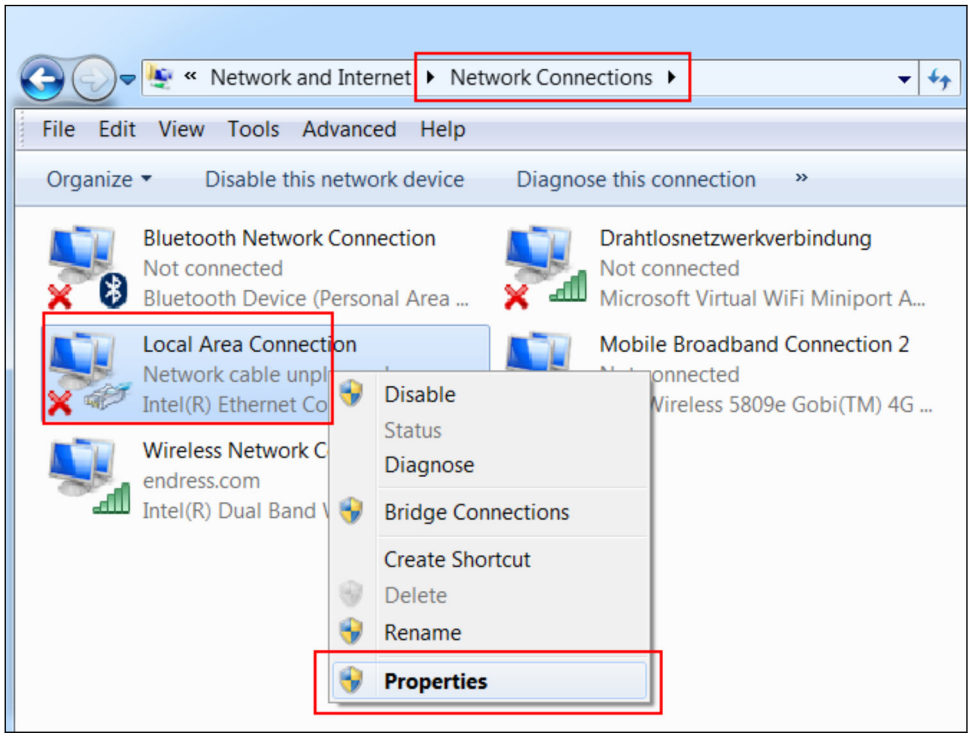
1. Check that the gateway is securely seated on the DIN rail and that the cable connections are correctly secured at the terminals and the antenna.
2. Mobile communications versions: insert the SIM card.
3. Switch on supply voltage.

7.3 Establishing the data connection

Default settings for the data connection:
- IP address: **https://192.168.252.1**
- User name for administrator: **super**
- Password for administrator: **super**
- Users who do not wish to configure the Fieldgate FXA42 or who do not have the necessary authorization can log on with the following default login data. User name: **eh**; Password: **eh**

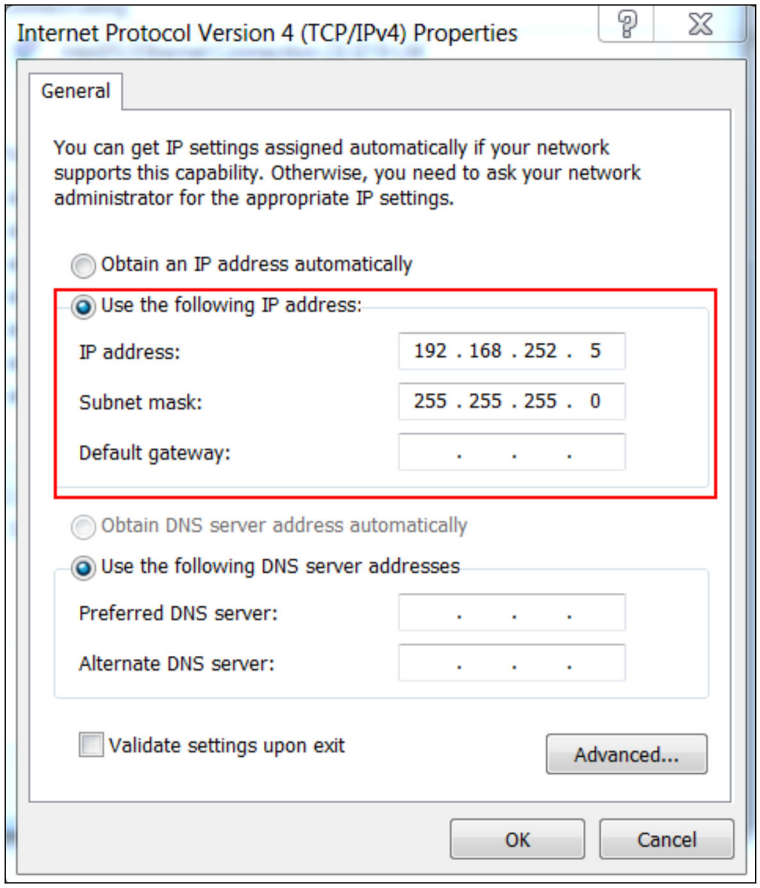
1. Connect the device directly to a PC or laptop using an Ethernet cable.
2. Assign the computer an IP address that is in the same subnet as the device itself. Therefore, select the IP address so that it is similar to, but not identical to, the preconfigured IP address of the device. The IP address of the computer and that of the device may not be identical.
3. Microsoft Windows: Open the**Start** menu and select the**Control Panel** menu item.
4. Select the**Network Connections** menu item and then select the Ethernet connection to which the device is connected.

5.



Right-click with the mouse button to open the context menu. Select the**Properties** menu item.

6.



Select the**Use the following IP address** and option and enter an IP address. Example of an IP address: 192.168.252.2

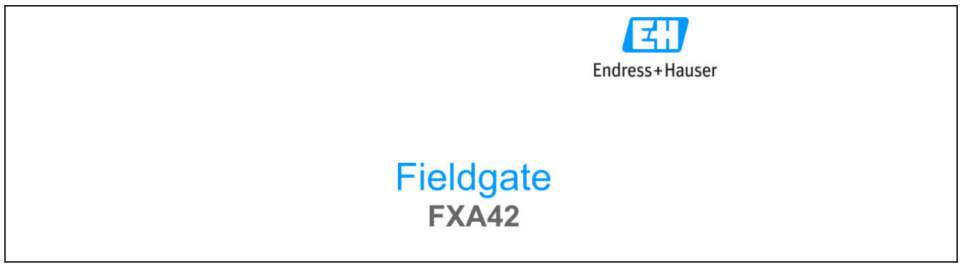
7. Enter**Subnet mask** 255.255.255.0 and click**OK** to confirm the entries.

8. Open an Internet browser and enter the preconfigured IP address https://192.168.252.1 in the address line of the browser.

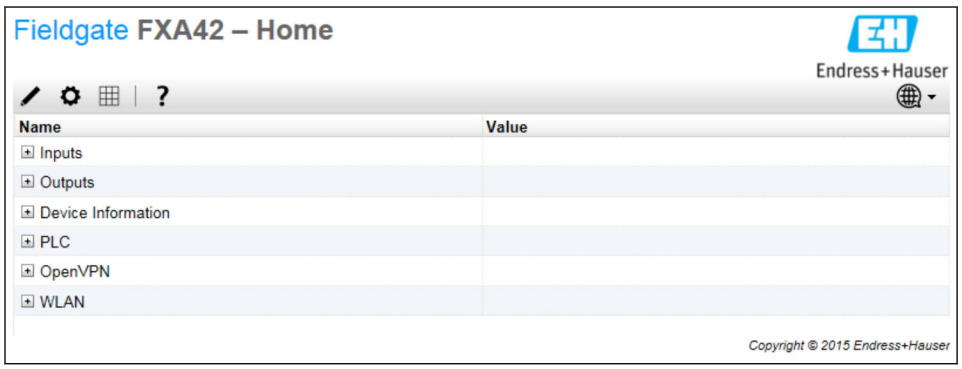
9.

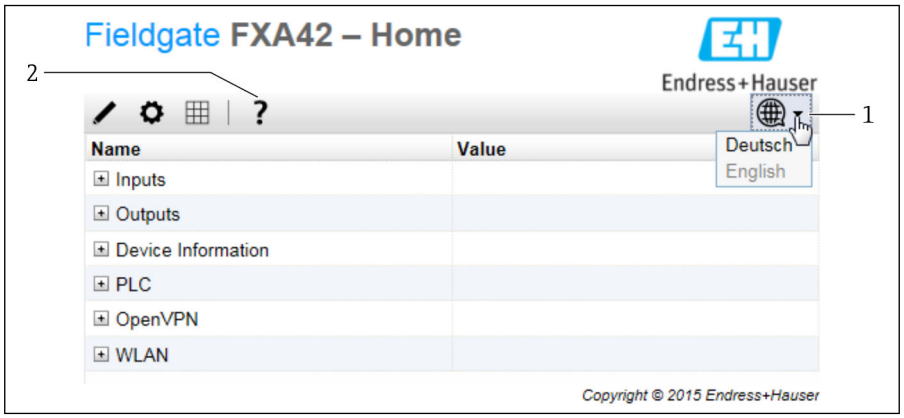
Enter the user name and password. Click**OK** to confirm the entries.

↳ The connection is now established and the Fieldgate FXA42 welcome screen is displayed.



The display changes automatically after a few seconds and the home screen to access the configuration menus appears.





1 Select the Language menu
2 Help

To change the language of the user interface, open the menu (1) in the top right-hand corner of the startup screen and select a language.

To open the Help function, click the question mark icon (2). The home page and the icons in the tool bar are explained in the Help function.

The home page gives a logged-in administrator access to the functions and settings of the device, the device's inputs and outputs and its properties.

7.4 Installing the latest firmware

Due to storage and transportation times, the latest firmware version might not be installed on your device. It is therefore advisable to update the firmware when commissioning the device.

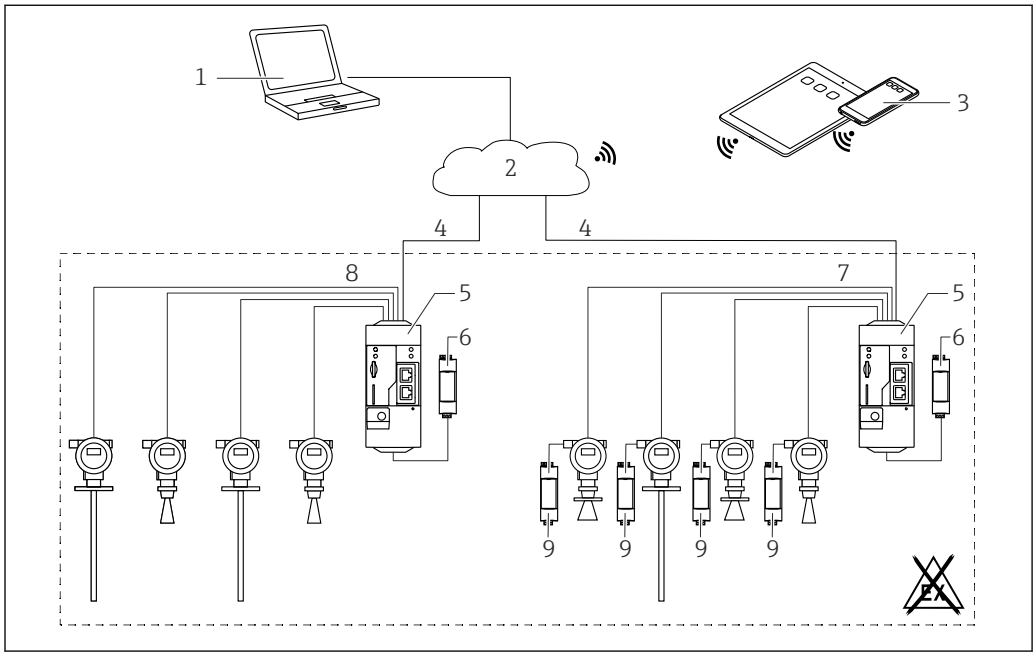
Click the following link to download the latest firmware:

https://weupcmasafgfirmware.blob.core.windows.net/fxa42/fxa42_current.cup

For detailed information on updating, see the **Operation** > **Settings** > **Update** section.

7.5 Configuration examples

7.5.1 Configuration with 4 to 20 mA analog input (2-wire/4-wire)



3 System architecture of a Fieldgate FXA42 with 4 to 20 mA analog input

1 SupplyCare Enterprise / SupplyCare Hosting (via Web browser)
2 Internet / LAN
3 SupplyCare Enterprise / SupplyCare Hosting on mobile devices (via Web browser)
4 Ethernet / WLAN / UMTS / LTE-M / LTE Cat NB1
5 Fieldgate FXA42
6 Power supply 24 V_{DC}
7 4 x 4 to 20 mA analog input (passive), 4-wire
8 4 x 4 to 20 mA analog input (active), 2-wire (loop-powered)
9 Measuring device power supply

Once a device has been connected to the Fieldgate FXA42, the measured values are displayed in the **Grid View** ▦.

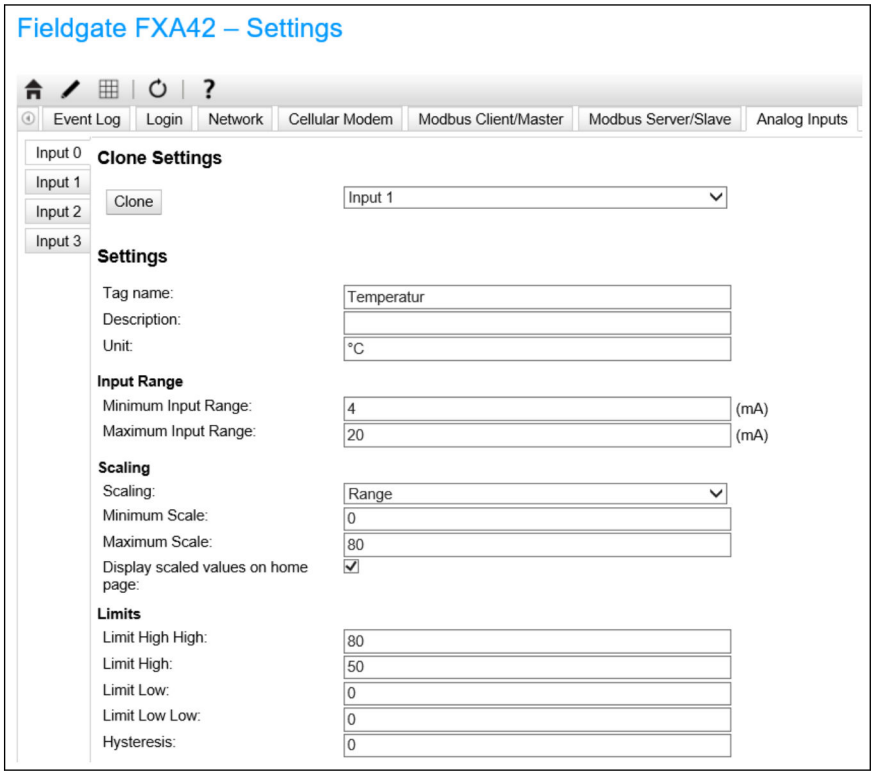
In general, no additional configuration settings are necessary.

Additional configuration settings can be made on the **Analog Inputs** tab on the **Settings** ⚙ page.

Reading out the analog inputs

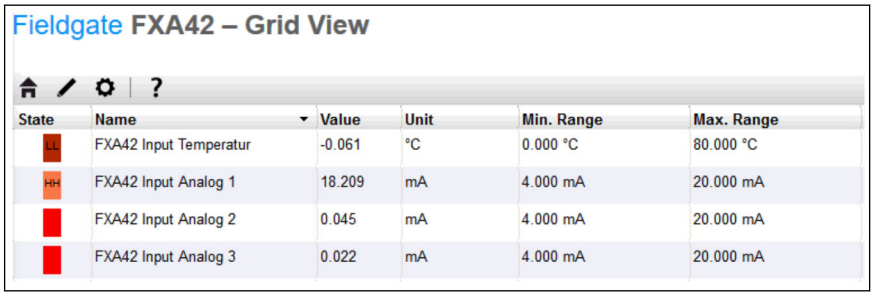
Example

1. On the **Analog Inputs**, select the desired input and edit the **Settings** (**Tag name** = name to be displayed in the application, **Description** = optional description, **Unit** = physical unit to be displayed).
2. Set **Scaling** to **Range** and enter the minimum and maximum values.

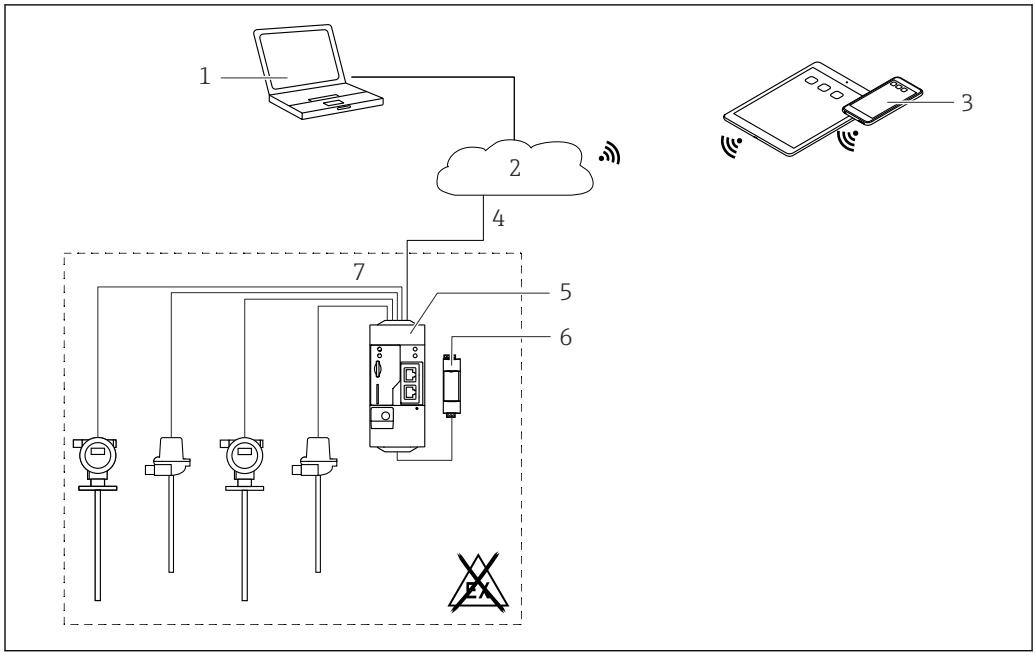


3. Click **OK**:

↳ The calculated values are displayed in the **Grid View**:



7.5.2 Configuration with a digital input



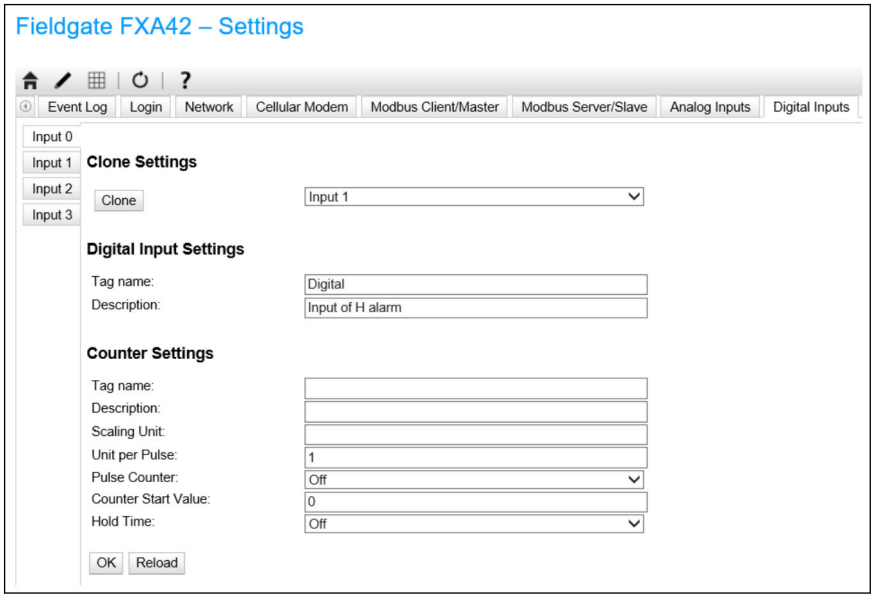
4 *System architecture of a Fieldgate FXA42 with a digital input*

1 *SupplyCare Enterprise / SupplyCare Hosting (via Web browser)*
2 *Internet / LAN*
3 *SupplyCare Enterprise / SupplyCare Hosting on mobile devices (via Web browser)*
4 *Ethernet / WLAN / UMTS / LTE-M / LTE Cat NB1*
5 *Fieldgate FXA42*
6 *Power supply 24 V_{DC}*
7 *4 x digital input and auxiliary voltage output 24 V_{DC}*

Configuring the digital input

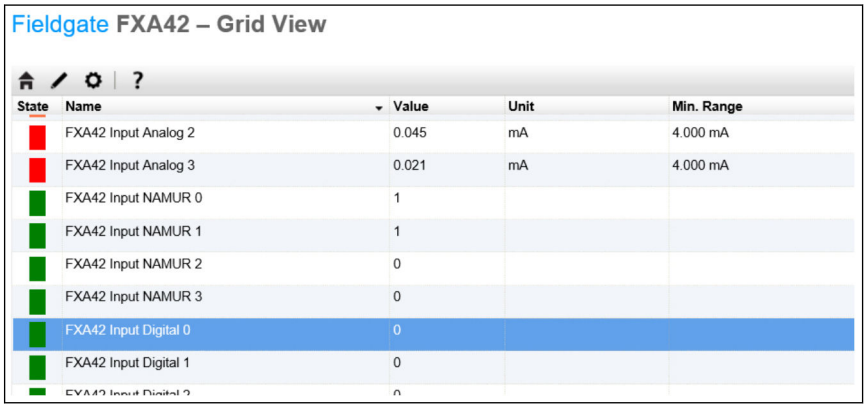
Example

1. On the **Digital inputs** tab, select the desired input and edit the **Settings** (**Tag name** = name to be displayed in the application, **Description** = optional description).



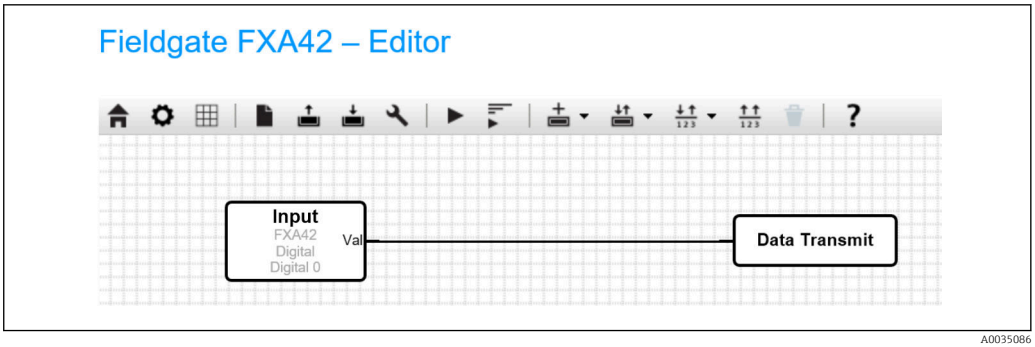
2. Click **OK**:

   The status of the digital inputs is displayed in the **Grid View**:



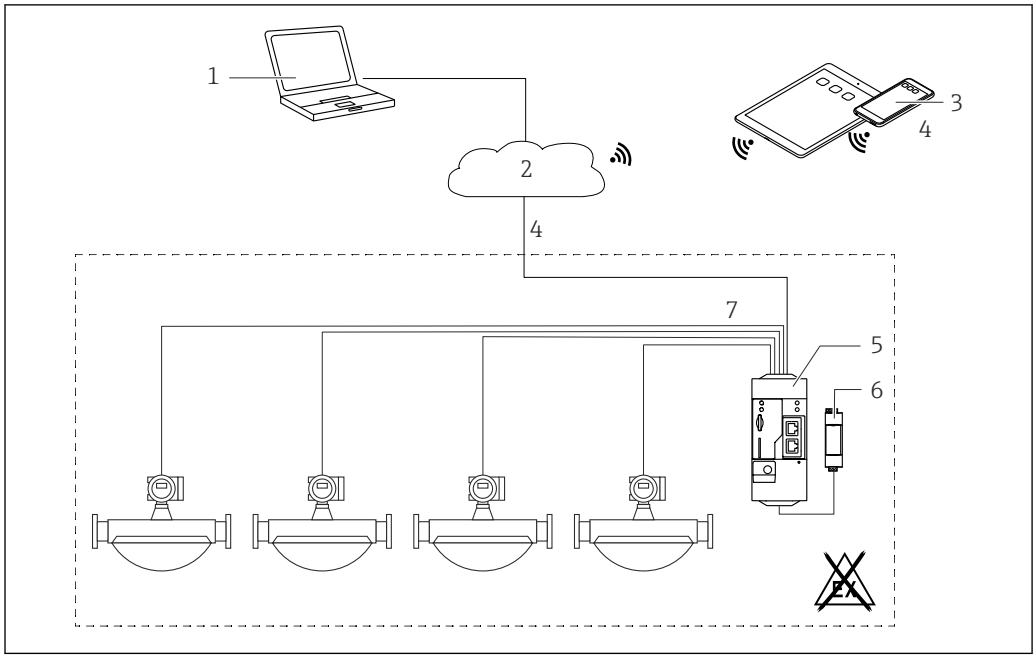
The configured digital input is now available in the editor of the Web-PLC.

Example: The digital input triggers data transmission:



A0035086

7.5.3 Configuration with a pulse counter



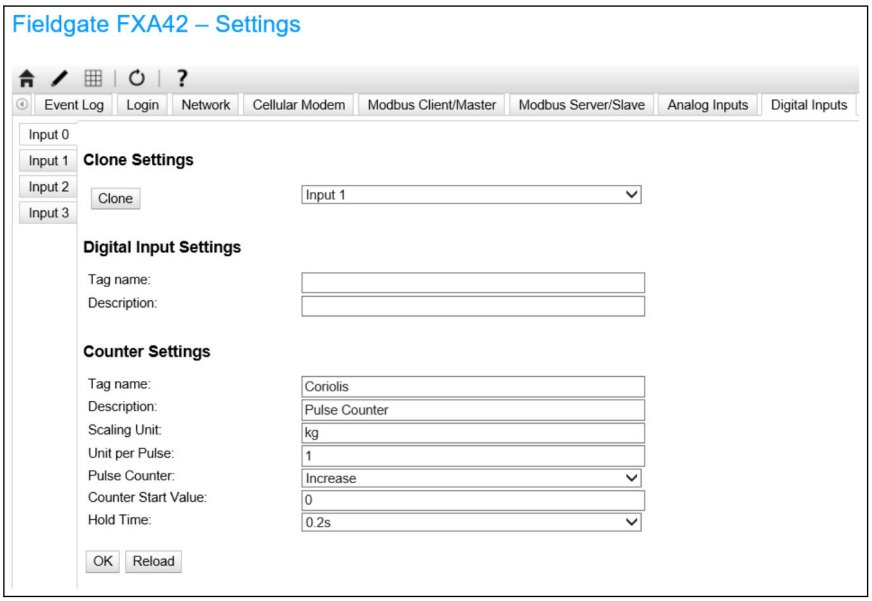
5 *System architecture of a Fieldgate FXA42 with a pulse counter*

1 *SupplyCare Enterprise / SupplyCare Hosting (via Web browser)*
2 *Internet / LAN*
3 *SupplyCare Enterprise / SupplyCare Hosting on mobile devices (via Web browser)*
4 *Ethernet / WLAN / UMTS / LTE-M / LTE Cat NB1*
5 *Fieldgate FXA42*
6 *Power supply 24 V_{DC}*
7 *4 x digital input with pulse counter*

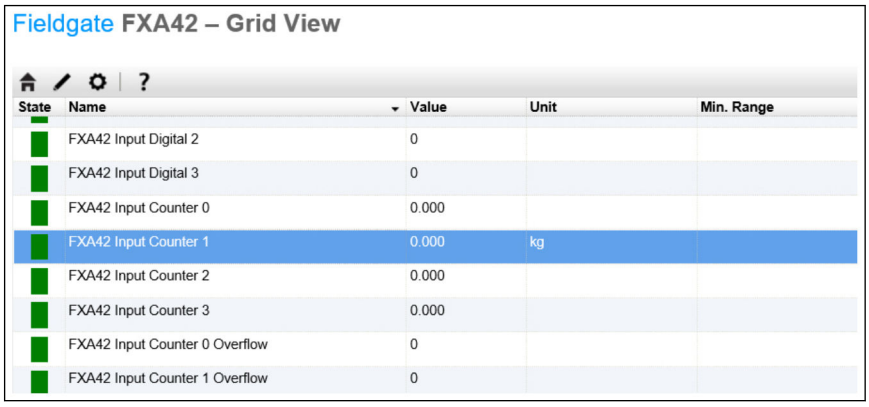
Reading out the pulse counter

Example

1. On the **Digital inputs** tab, select the desired input and edit the **Settings** (**Tag name** = name to be displayed in the application, **Description** = optional description).

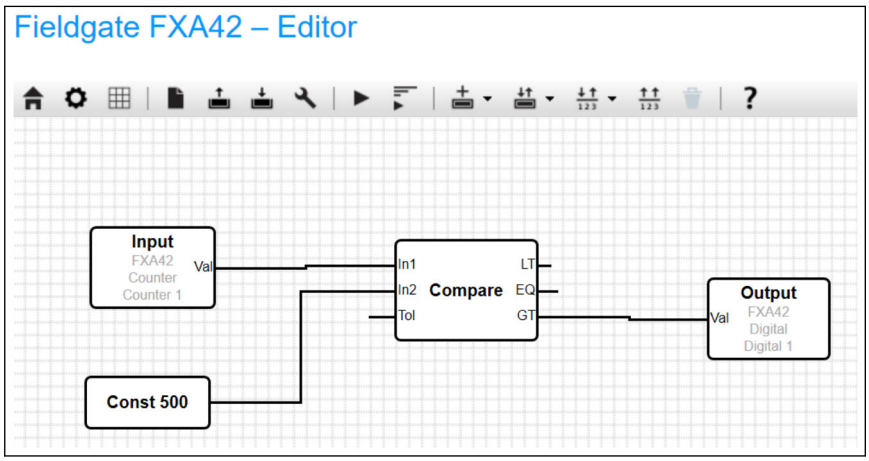


2. Click **OK**:
   ↳ The values of the pulse counter (e.g. FXA42 Input Counter 1 and FXA42 Input Counter 1 Overflow) are displayed in the **Grid View**:



The configured pulse counter is now available in the editor of the Web-PLC.

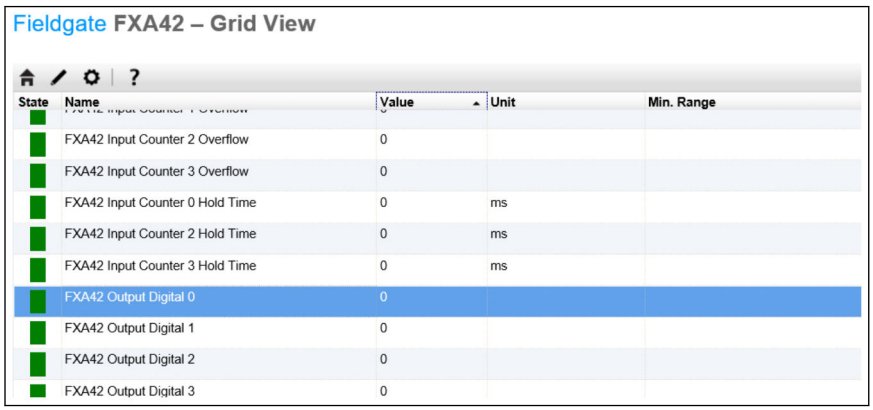
Example: The digital output is switched on as soon as the value "500" is exceeded:



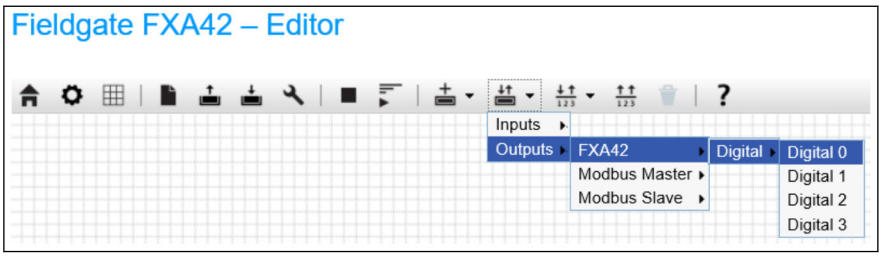
7.5.4 Configuring the digital output

The input of the digital output must be connected to an action that returns a 0 or 1.

Values of the digital outputs are displayed in the **Grid View**:



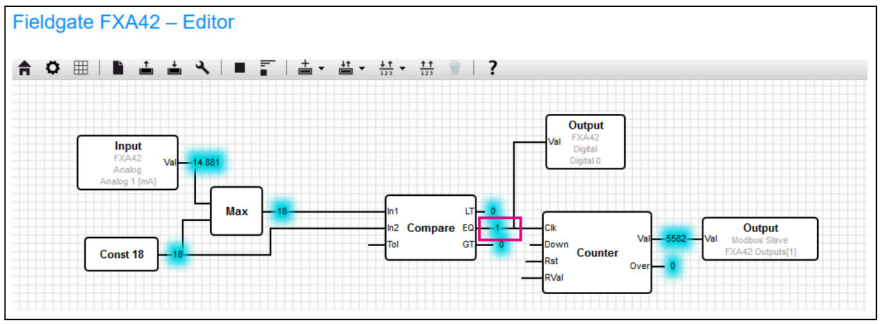
1. Select the editor
2. Select the output:



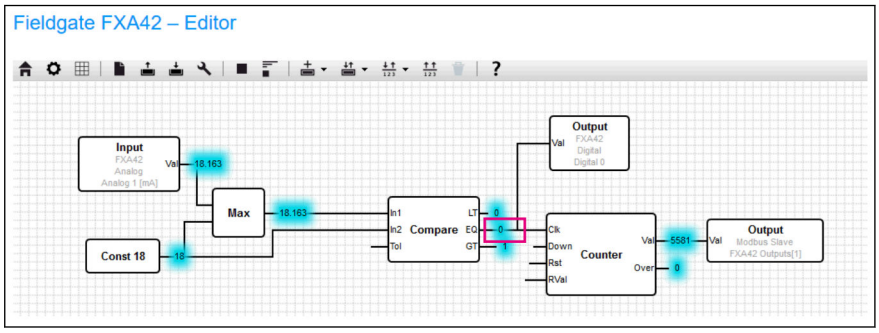
3. Interconnect units in the diagram.
4. Save the diagram:
5. Start Web-PLC:

Examples for the step **Interconnect units**:

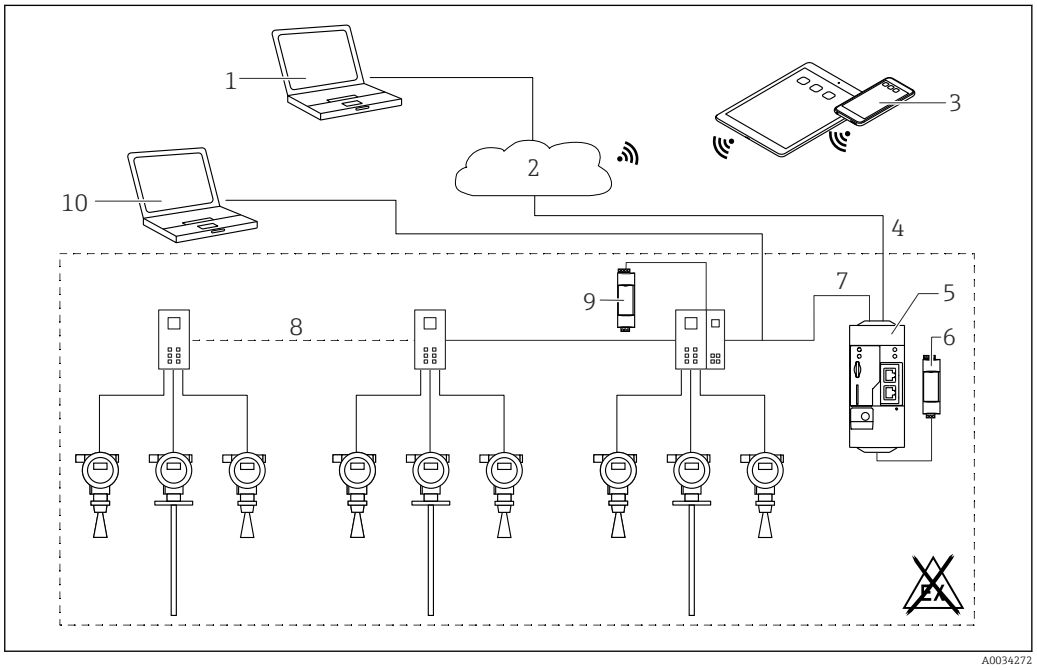
Example for output = 1:



Example for output = 0:



7.5.5 Communication via Modbus TCP



6 *System architecture of a Fieldgate FXA42 with a HART point-to-point multiplexer*

1 *SupplyCare Enterprise / SupplyCare Hosting (via Web browser)*
2 *Internet / LAN*
3 *SupplyCare Enterprise / SupplyCare Hosting on mobile devices (via Web browser)*
4 *Ethernet / WLAN / UMTS / LTE-M / LTE Cat NB1*
5 *Fieldgate FXA42*
6 *Power supply 24 V_{DC}*
7 *Modbus TCP via Ethernet as server/client*
8 *Phoenix Contact multiplexer from Modbus TCP to HART point-to-point. 1 head module and up to 5 extension modules are possible. Extension modules for 4 or 8 HART channels are possible*
9 *External power supply*
10 *FieldCare tunneling via Phoenix Contact multiplexer*

Modbus TCP can be operated as a server and as a client at the Ethernet connection of the Fieldgate FXA42.

When operated as a Modbus client, up to 32 devices and 256 values can be defined. As values can become arrays when reading and writing several registers or coils, the following limit applies: The number of all scalar (non-array) values plus the size of all arrays must not exceed 512.

Configuration of FXA42 as a Modbus TCP client (reading out data from other systems)

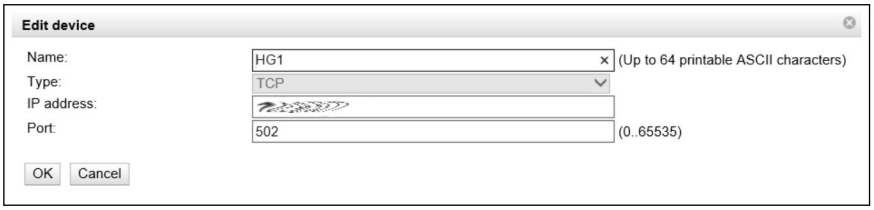
The following examples show how to configure the gateway to read out data using the Modbus TCP. Please refer to the device documentation for additional information.

Suitable devices are:
- Rapsystems HG1 Plus HART to Modbus gateway (accessory)
- Phoenix Contact GW PL ETH/BASIC-BUS HART Ethernet multiplexer head module (accessory)
- Datexel DAT8017-I server module, analog to Modbus TCP converter (accessory)

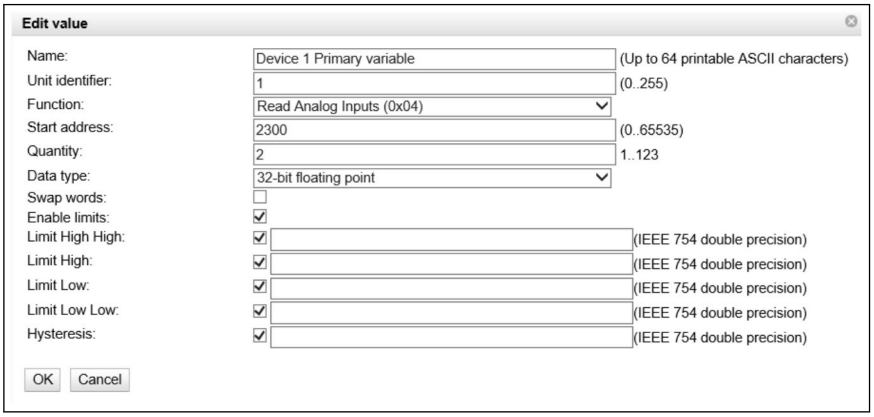
Other devices that can communicate via Modbus TCP can also be connected.

Example with HG1 Plus

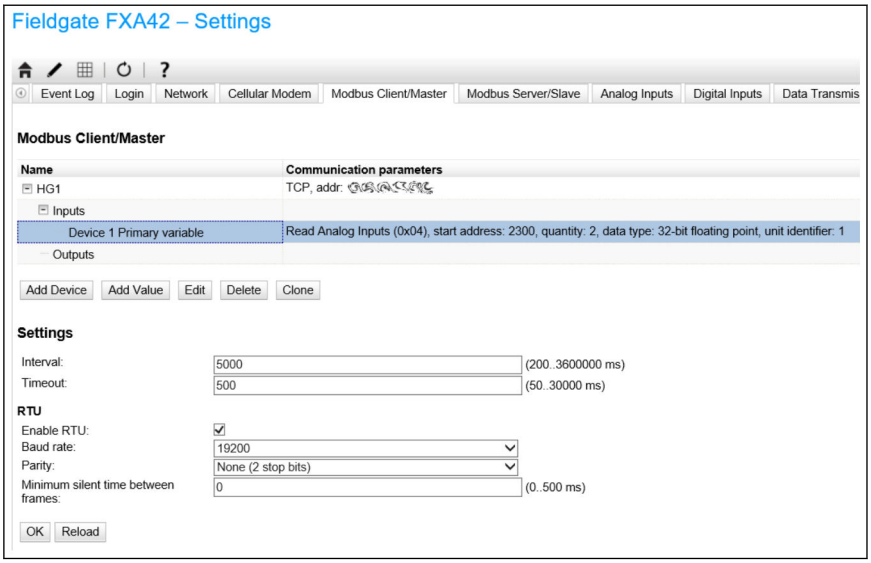
1. Open the ⚙ Settings page.
2. Select the **Modbus Client/Master** tab.
3. Select **Edit device**and enter data:



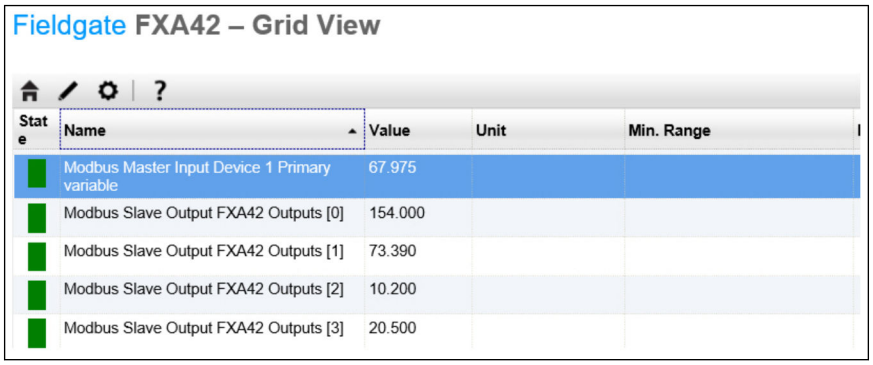
4. Select **Edit value** and enter data. Example: enter Primary Variable (PV) for the first HART device connected to the HG1 Plus (enable and enter limits if necessary):



5. Click **OK**:

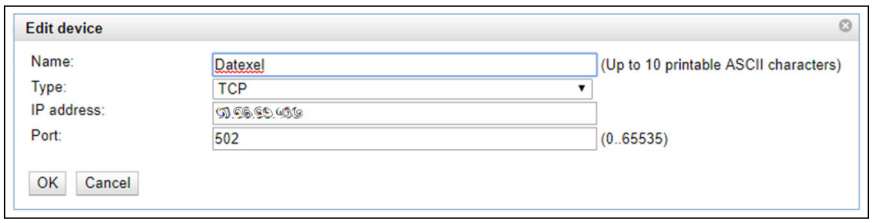


6. Restart the device ↻.
   ↳ The read out values are displayed in the **Grid View**.

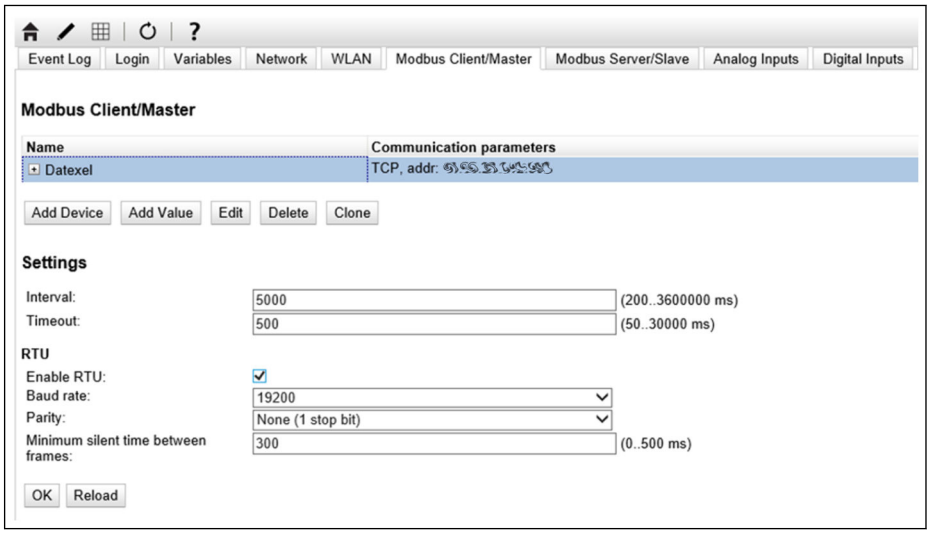


Example with Datexel server module

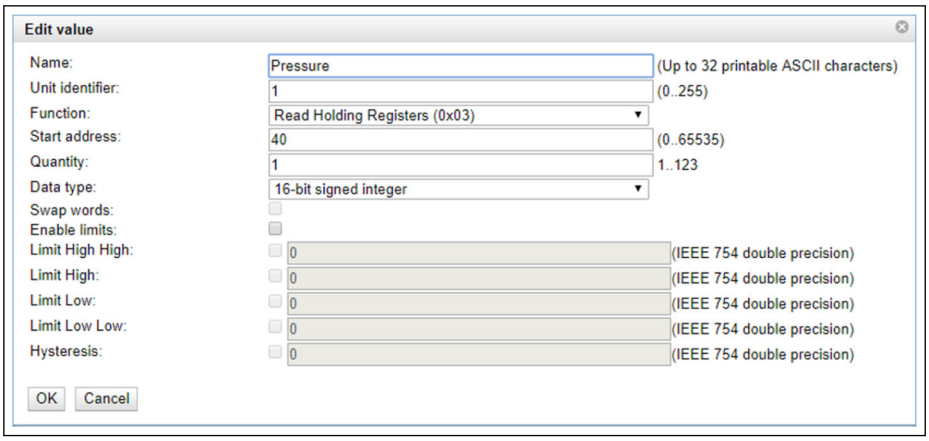
1. Open the ⚙ Settings page.
2. Select the **Modbus Client/Master** tab.
3. Select **Edit device** and enter data:
   ↳



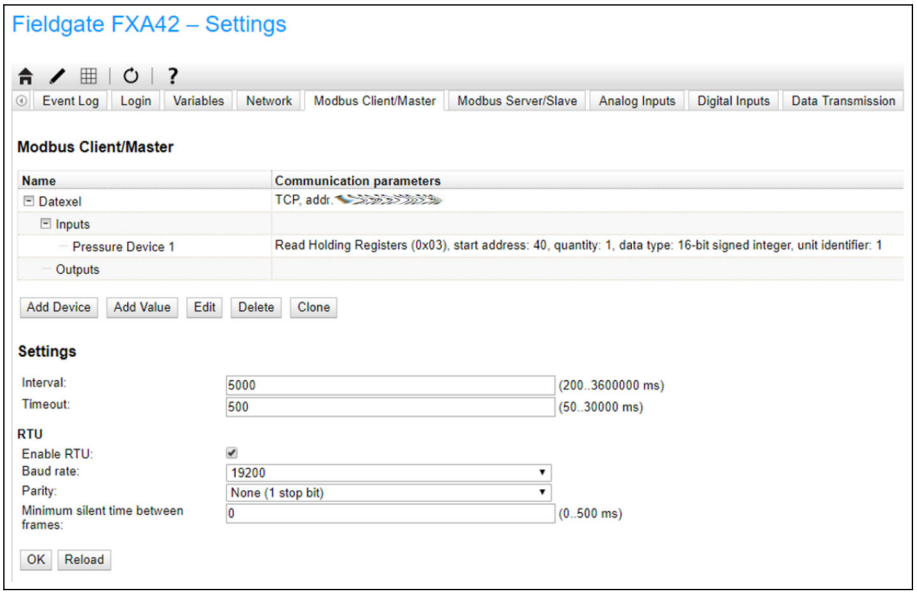
4. Click **OK**:
   ↳



5. Select **Edit value** and enter data. Example: pressure measuring device connected to the first channel of the Datexel server module.



6. Click **OK**:



7. Restart the device ↻.
   ↳ The read out values are displayed in the **Grid View**.

The values read in from the Datexel server module are in the microampere unit. The values in the 4 000 to 20 000 µA measuring range must be converted to the current measured value. The measuring range is linked to the measured pressure range in such a way that a certain microampere value corresponds to a defined pressure value. The following linear functional equation is used for this purpose:

$$f(x) = m \times x + b$$

A0039591

Here, x corresponds to the incoming measured value in microamperes (µA). m corresponds to a constant that is calculated according to the following equation:

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

A0040990

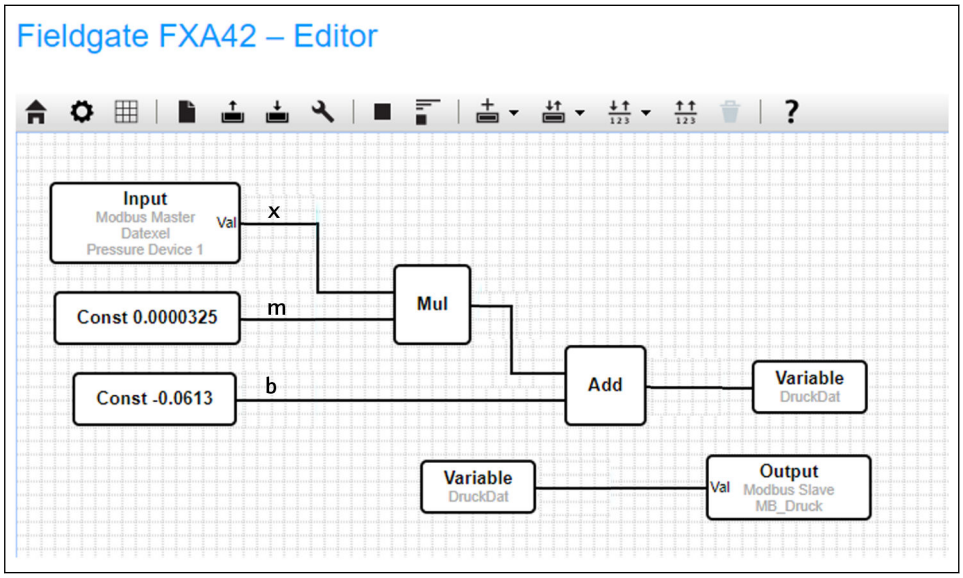
Where:
- x_2 = upper value of the current range in µA = 20000
- x_1 = lower value of the current range in µA = 4000
- y_2 = measured value at 20000 µA (measured value at 20 mA)
- y_1 = measured value at 4000 µA (measured value at 4 mA)

b corresponds to an additional constant that is calculated according to the following equation:

$$b = y_1 - m \times x_1$$

A0040991

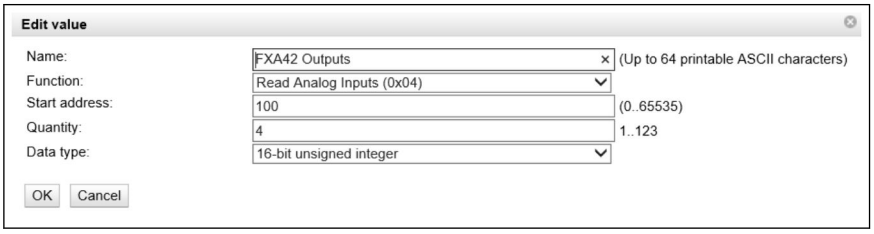
The following diagram for the Web-PLC can be created in the editor program on the basis of this information:



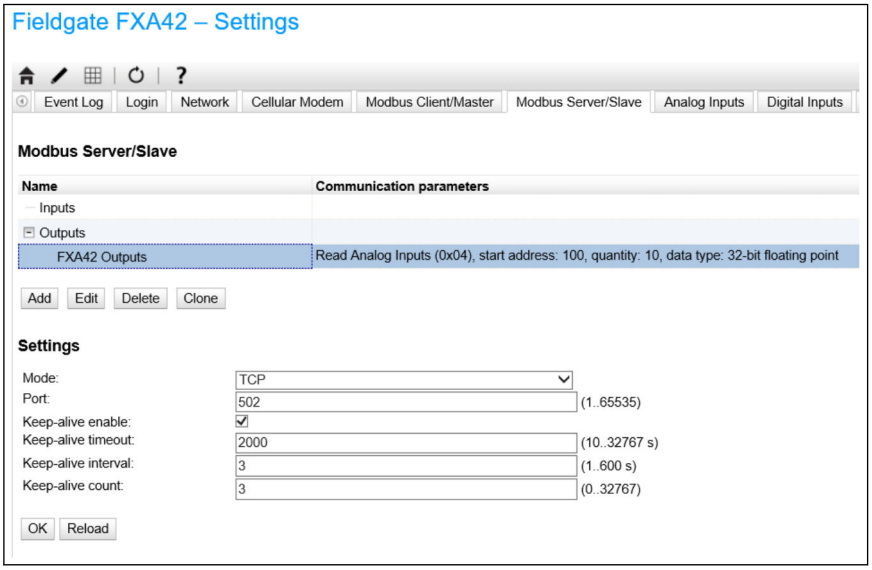
Configuration of FXA42 as a Modbus TCP server (transmitting data to other systems)

The steps in the example below describe how to transmit data to other devices. Please refer to the device documentation for additional information.

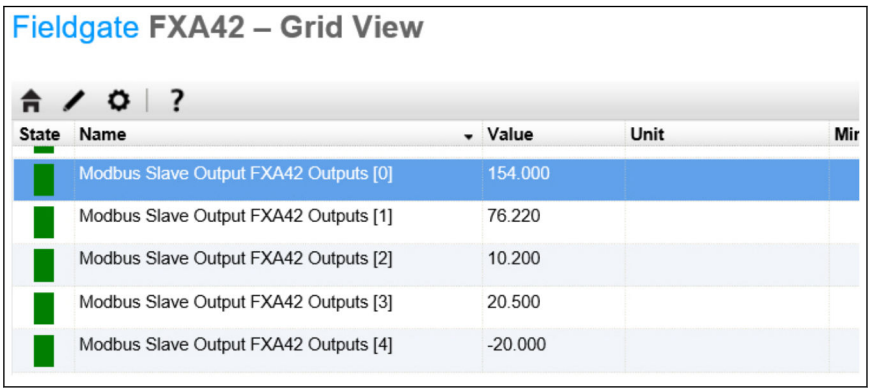
1. Open the ⚙ Settings page.
2. Select the **Modbus Server/Slave** tab.
3. Select **Edit value** and enter data:



4. Click **OK**:

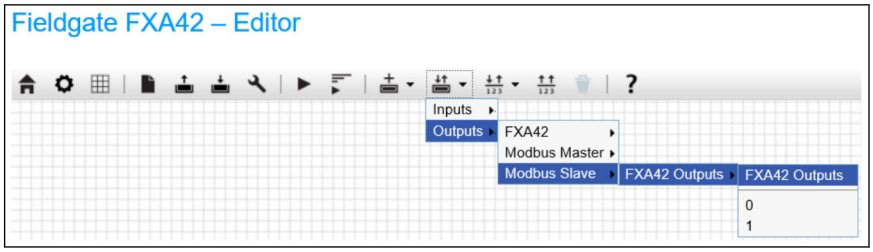


5. Restart the device ↻.
6. The Modbus TCP output values are displayed in the **Grid View**:

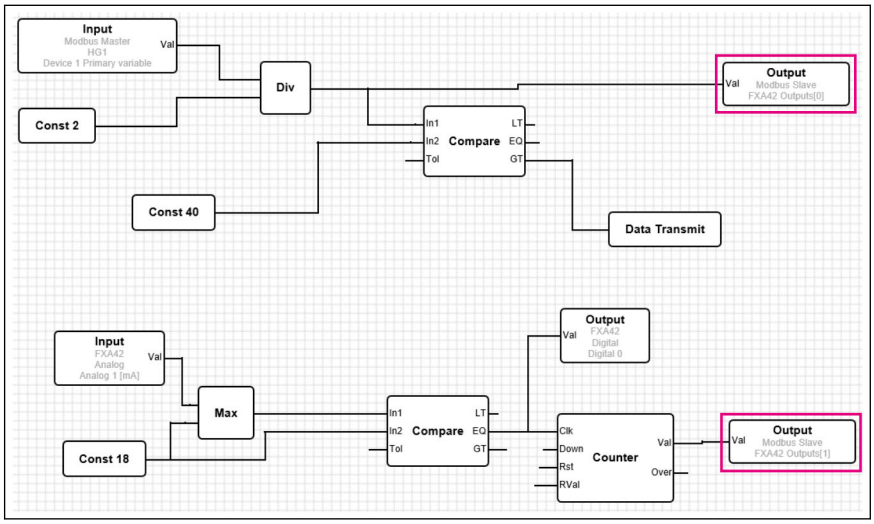


7. Select the editor ✎

8. Select the output:



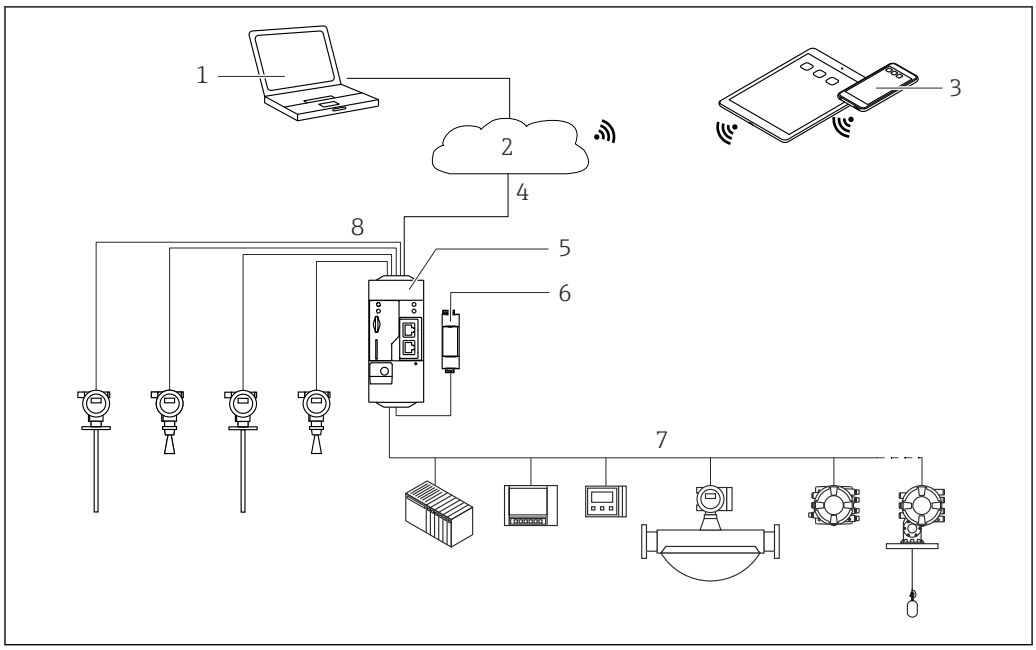
9. Interconnect units, see the following example:



10. Save the diagram:

11. Start Web-PLC: ▶

7.5.6 Configuration with Modbus RS485



7 *System architecture of a Fieldgate FXA42 with Modbus RS485*

1 *SupplyCare Enterprise / SupplyCare Hosting (via Web browser)*
2 *Internet / LAN*
3 *SupplyCare Enterprise / SupplyCare Hosting on mobile devices (via Web browser)*
4 *Ethernet / WLAN / UMTS / LTE-M / LTE Cat NB1*
5 *Fieldgate FXA42*
6 *Power supply 24 V_{DC}*
7 *1 x Modbus RS485 as master or slave*
8 *4 x analog input 4 to 20 mA (2-wire / 4-wire)*

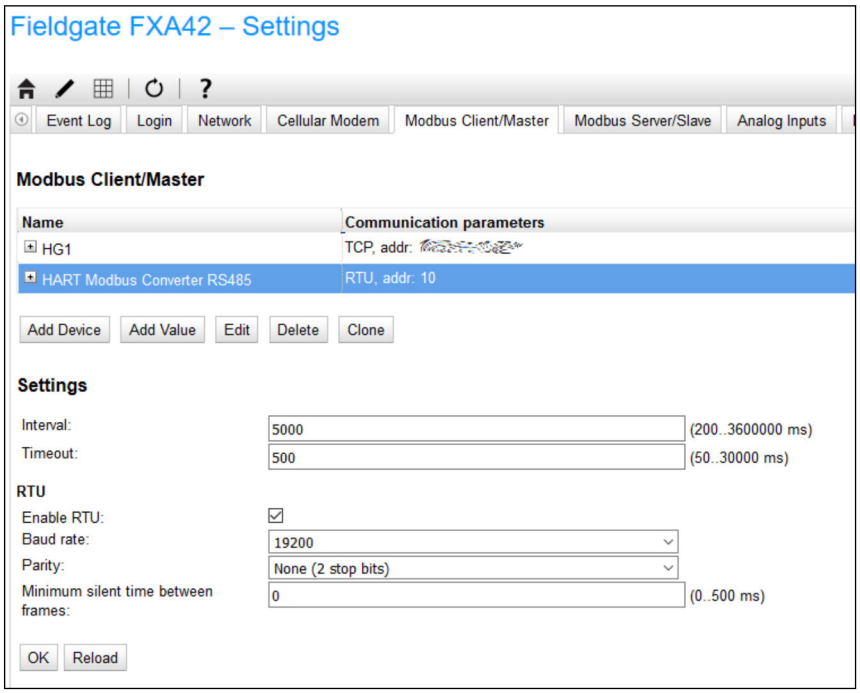
The Modbus RS485 connection can be used as either a master or a slave, but cannot act as both simultaneously.

- When operated as a master, up to 32 devices and 256 values can be defined. As values can become arrays when reading and writing several registers or coils, the following limit applies: The number of all scalar (non-array) values plus the size of all arrays must not exceed 512.
- When operated as a slave, up to 128 values can be defined. As values can become arrays when reading and writing several registers or coils, the following limit applies: The number of all scalar (non-array) values plus the size of all arrays must not exceed 512.

Configuration of FXA42 as a Modbus RS485 master (reading out data from other systems)

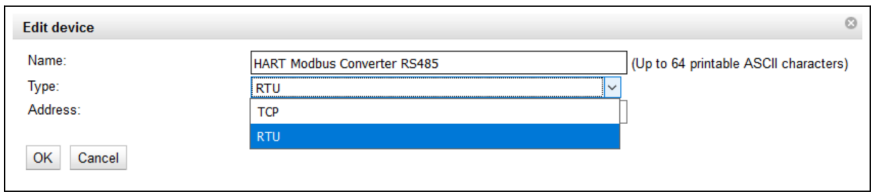
1. Open the ⚙ Settings page.
2. Select the **Modbus Client/Master** tab.

3. Under **Settings**, select the **Enable RTU** function. Enter the interval, timeout, baud rate etc.:

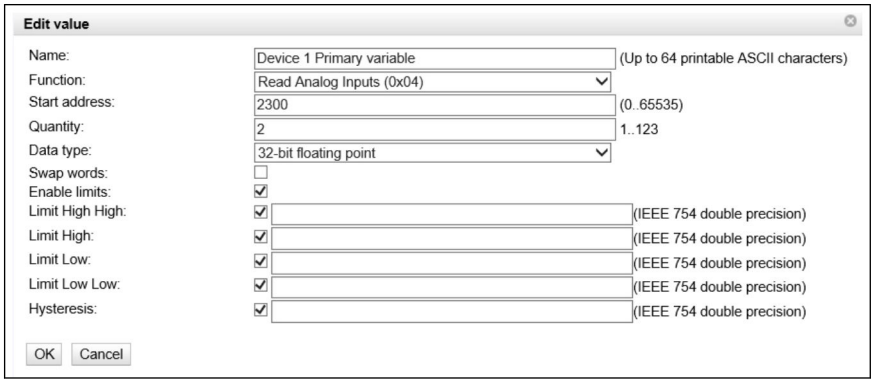


4. Click **OK**:

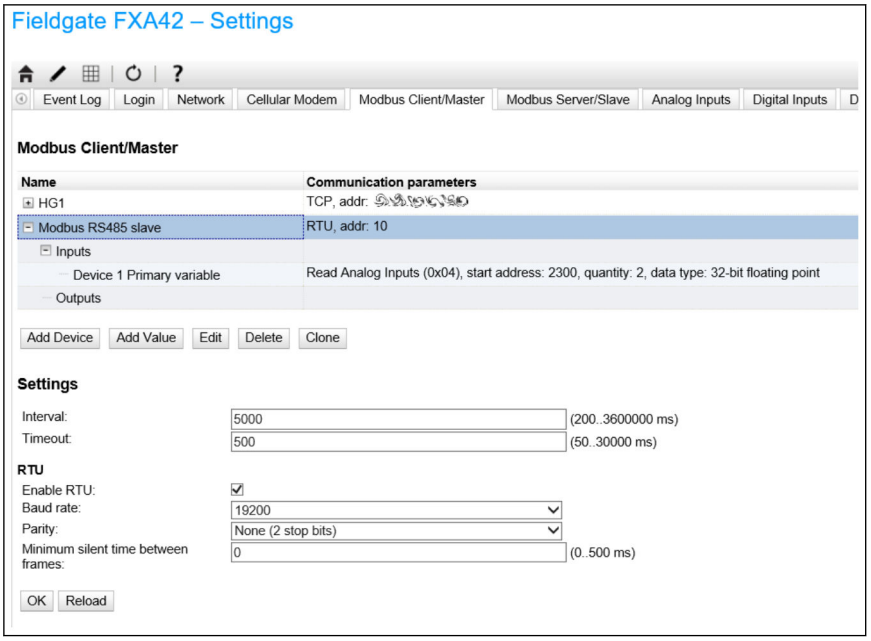
5. Select **Edit device** and enter data:



6. Select **Edit value** and enter data. If necessary, select the **Enable limits**function and enter the limit values:



7. Click **OK**:

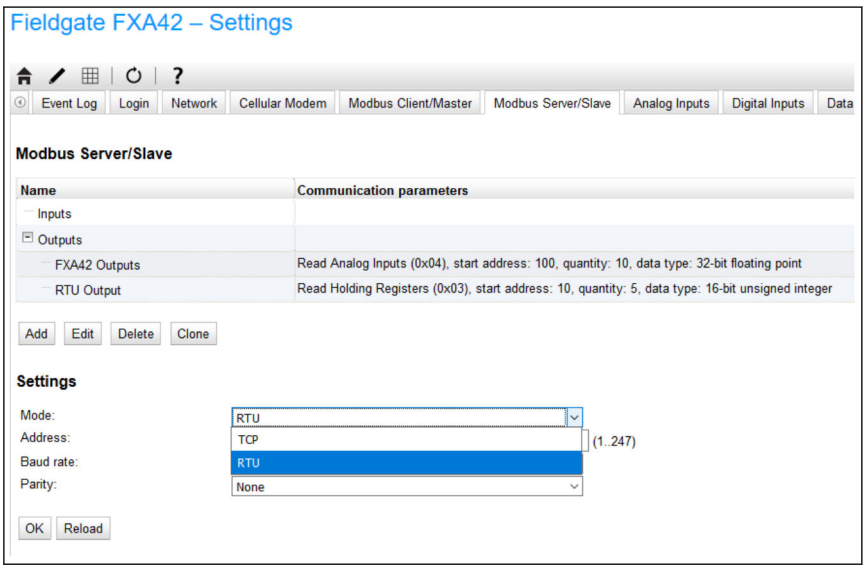


8. Restart the device ↻.

The rest of the configuration is the same as the configuration of the Modbus TCP client → 30).

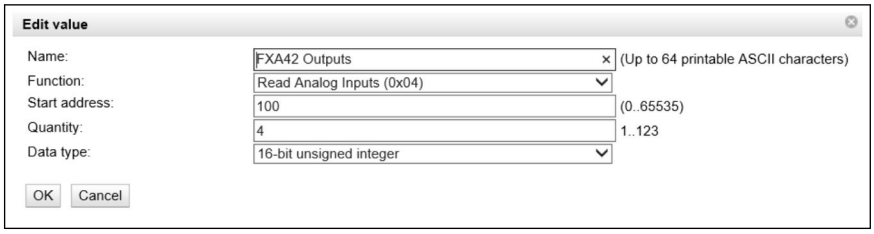
Configuration of FXA42 as a Modbus RS485 slave (transmitting data to other systems)

1. Open the ⚙ Settings page.
2. Select the **Modbus Server/Slave** tab.
3. Under Settings, select the **Enable RTU** function. Enter the interval, timeout, baud rate etc.:

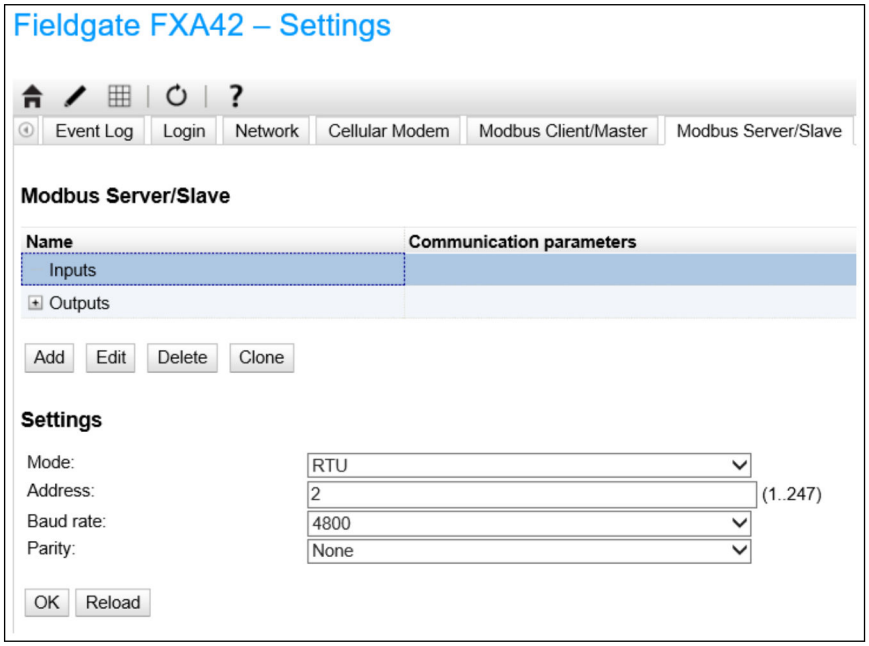


4. Click **OK**:

5. Select **Edit value** and enter data:



6. Click **OK**:

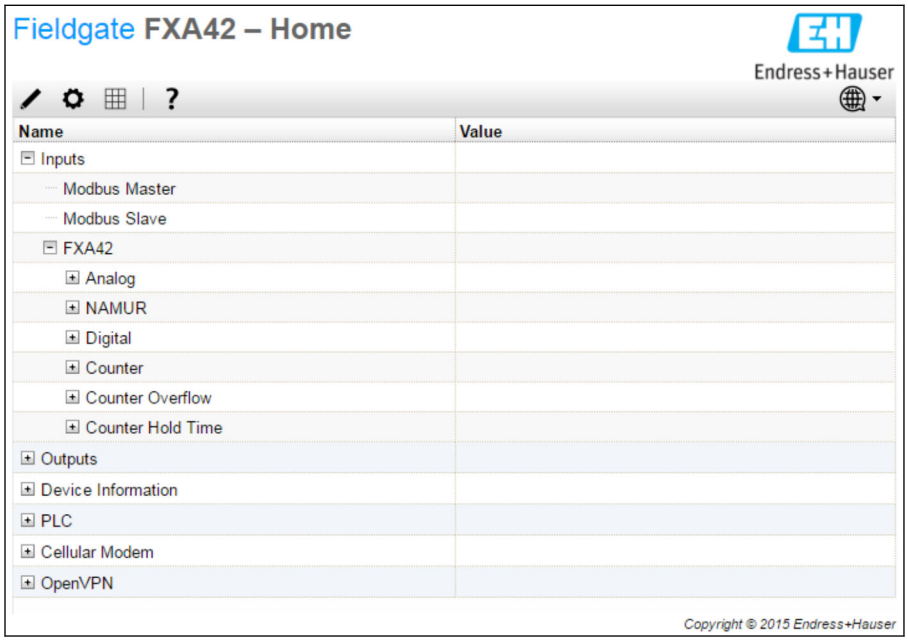


7. Restart the device ↻.
8. The rest of the configuration is the same as the configuration of the Modbus TCP server → 🖹 34).

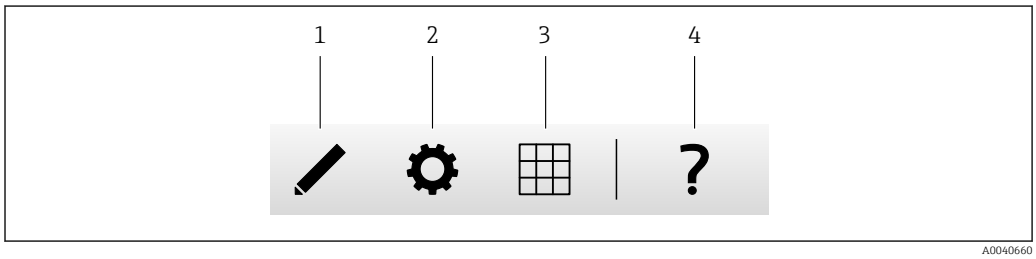
8 Operation

8.1 Home page

Home page provides access to information about the Fieldgate FXA42, its status, its inputs and outputs, and various other components.



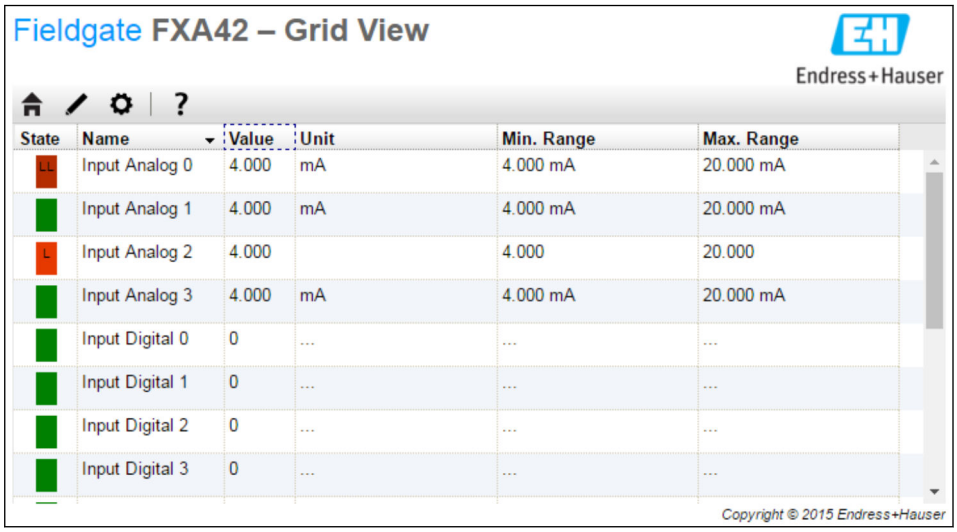
The **Home page** contains a tool bar with the following buttons:



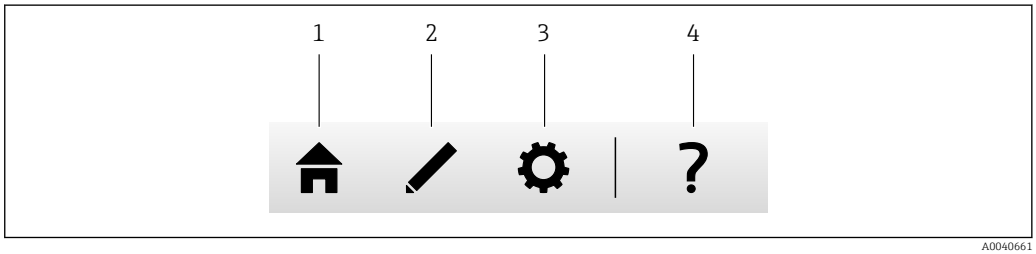
1 *Closes the current page and opens the editor*
2 *Closes the current page and opens the Settings page*
3 *Closes the current page and opens the Grid View page*
4 *Opens the Help*

8.2 Grid View

The values at the inputs and outputs are displayed on the **Grid View** page.



The **Grid View** page contains a tool bar with the following buttons:



1 Closes the current page and opens the home page
2 Closes the current page and opens the editor
3 Closes the current page and opens the Settings page
4 Opens the Help

The **Grid View** page displays all local inputs and outputs in a clearly structured grid.

The following information is displayed:
- **Unit**, **Min. Range**, **Max. Range** of the inputs and outputs
- The state of the analog inputs

The states are as follows:

State **High High**

State **High**

State **OK**

State **Low**

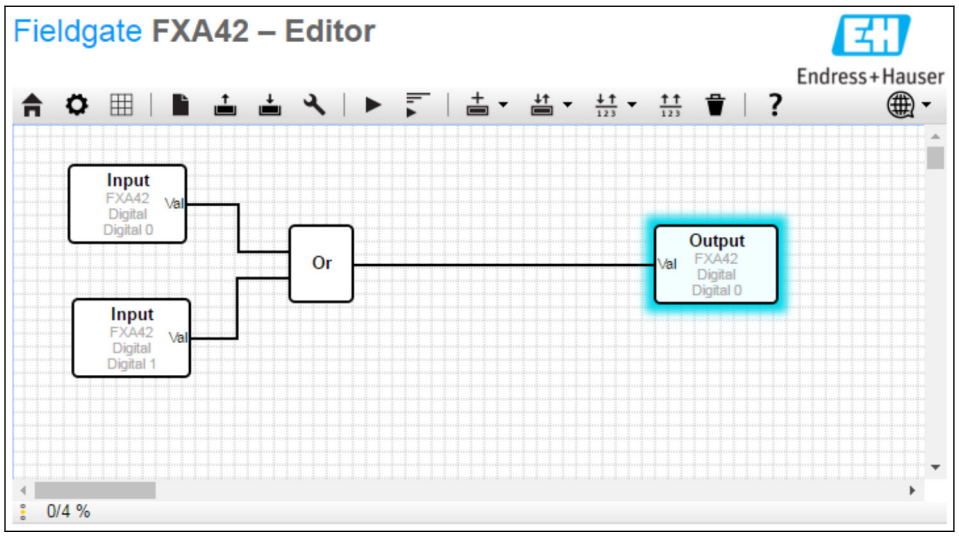
State **Low Low**

State **Erroneous**

State **Warning state**

8.3 Fieldgate FXA42 editor

The device has a graphical editor which can be used to edit function charts – similar to the well-known continuous function charts (CFCs). Function blocks can be used to connect the inputs and outputs of the Fieldgate FXA42 and special variables.



The editor basically consists of 3 parts:

- A toolbar is located at the top.
- Below the toolbar is the Diagram View. The current function diagram can be edited here. Elements can be positioned and connected to one another.
- At the bottom, you can find a status bar that displays information on the state of the PLC.

8.3.1 Toolbar

The following screenshot shows the toolbar of the Fieldgate FXA42 editor:

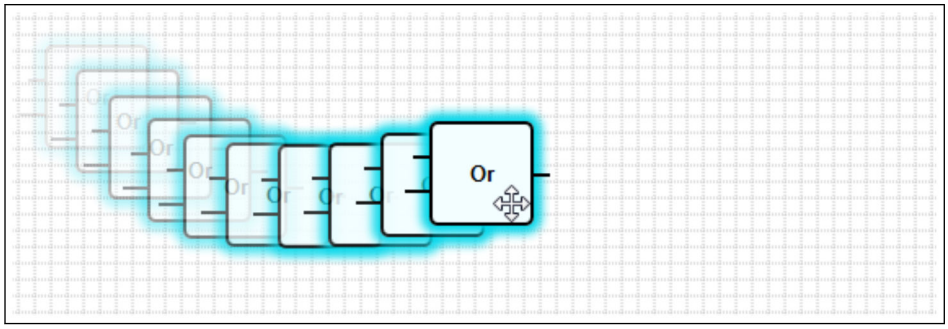
The following commands can be executed with the buttons:

Button	Description
	Close the current page and open the **Home page**.
	Close the current page and open the **Settings** page.
	Clear the diagram. This does not affect the diagram being executed by the PLC.
	Load the diagram from the PLC. Local changes are overwritten.
	Save the current local diagram to the PLC. If the PLC is currently running, it is stopped.
	Open a dialog box in which the diagram settings can be edited.
	Start/stop the PLC. The PLC can only be started if a non-empty diagram has been saved.
	Start/stop the Live view.
	Open a menu to select a unit type to be added to the diagram.
	Open a menu to select inputs or outputs (I/Os) to be added to the diagram. The menu consists of several submenus for inputs/outputs, interfaces, devices and arrays. Note the following for arrays: ▪ To add an I/O array element, select the topmost entry in the submenu. ▪ To add a plain I/O element, select the corresponding index in the submenu. The plain I/O element represents just one element of the array.
	Open a menu to add a variable to the diagram.
	Add a constant to the diagram view.
	Delete the selected element from the diagram view.
	Open the Help.

8.3.2 Editing the diagram

The function diagram consists of up to 256 units, local input and output elements (I/Os), variables and constants.

Elements are added to the diagram via the toolbar. Click an element to select it. A blue shadow around the element indicates that it has been selected. The selected element can be deleted by clicking the *Delete* button in the toolbar or by pressing the *DEL* key on the keyboard. To move an element in the diagram view, drag the element as illustrated in the picture below.



Each element has one or more ports via which it can be connected to other elements. Input ports are shown on the left-hand side and output ports on the right-hand side of the elements. Each port has one of the following data types:

- Boolean [0..1]
- 8-bit unsigned integer [0..255]
- 8-bit signed integer [-128..127]
- 16-bit unsigned integer [0..65,535]
- 16-bit signed integer [-32,768..32,767]
- 32-bit unsigned integer [0..4,294,967,295]
- 32-bit signed integer [-2,147,483,648..2,147,483,647]
- 32-bit floating point number
- 64-bit floating point number
- String (up to 4096 bytes)

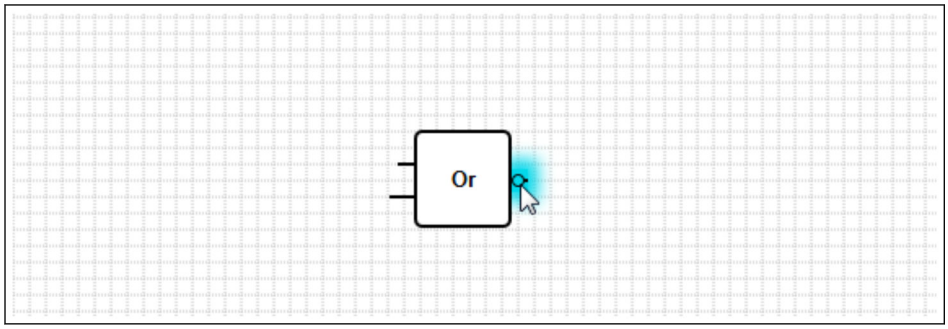
Data types are compared with one other according to this list. *Boolean* is considered the smallest data type, while *String* is the largest data type.

If ports with different data types are connected to one another, the value for the data type of the output port is implicitly converted to the data type for the input port.

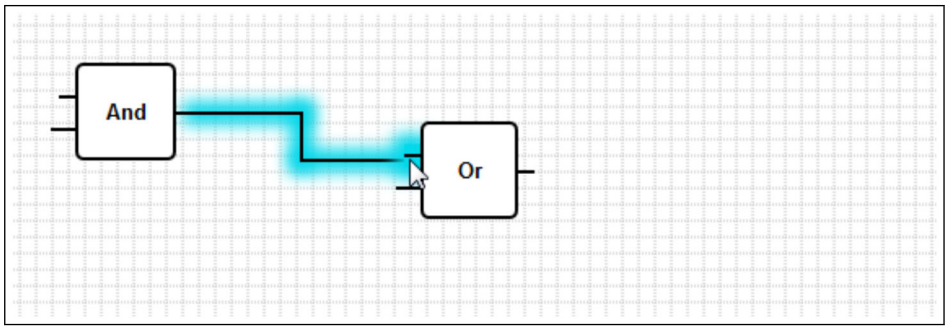
This conversion can lead to loss of data.

Open input ports are defined to have the value *0* (Boolean data type). Double-click a port to negate it. A small circle indicates that the port is negated (see the graphic below).

The negation is performed logically. The value *0* is negated to *1*. A value not equal to *0* is negated to *0*. Negating a string results in an empty string.

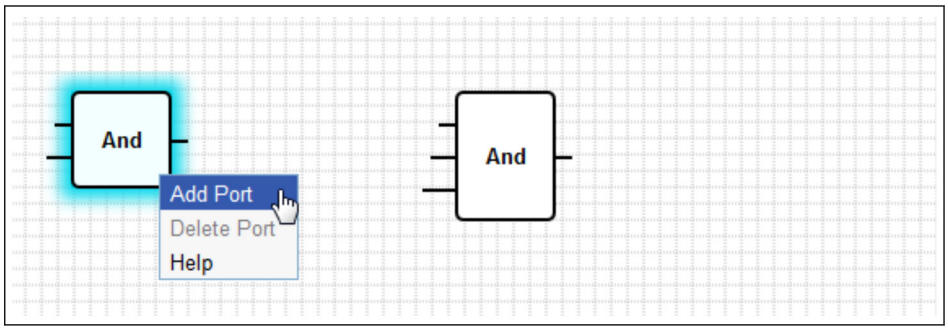


To connect an input port with an output port, click one of the ports, keep the mouse button pressed, drag the blue connector that appears over the other port (see the next graphic), and release the mouse button. Note that one output port can be connected to multiple input ports. However, it is not possible to interconnect two input ports or two output ports. Connectors can be selected just like any other element. Activated connectors can be deleted by clicking the *Delete* button in the toolbar or by pressing the *DEL* key on the keyboard.



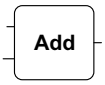
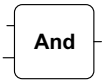
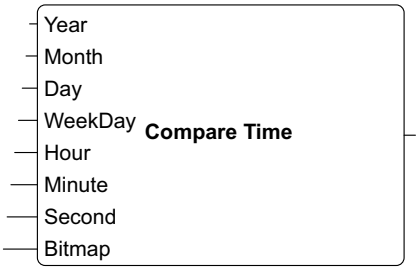
Some elements allow ports to be added or deleted dynamically. To do this, right-click the element. A popup menu appears (see the following graphic). You can add or delete ports here.

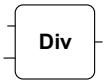
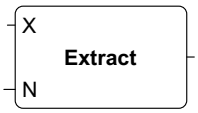
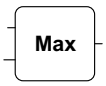
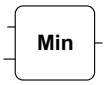
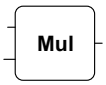
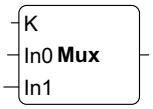
Every element has a minimum and maximum number of ports. You can also use this popup menu to access the help for the particular element.

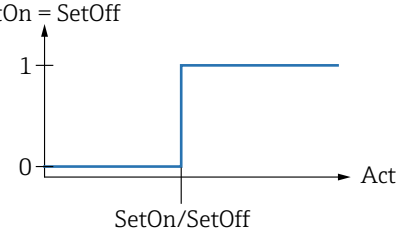
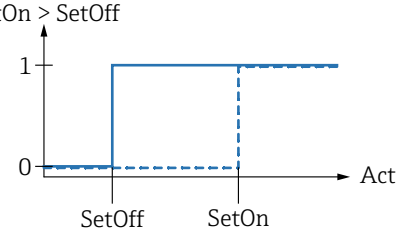
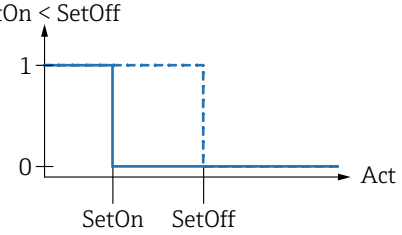


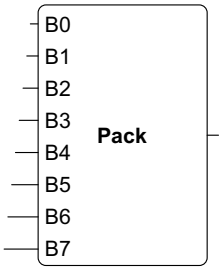
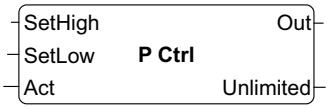
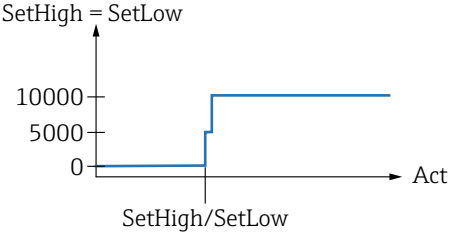
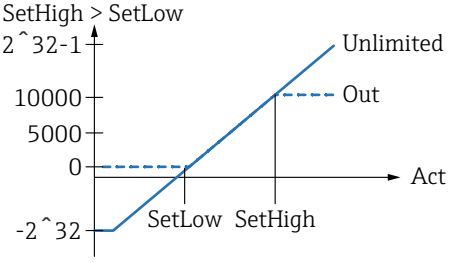
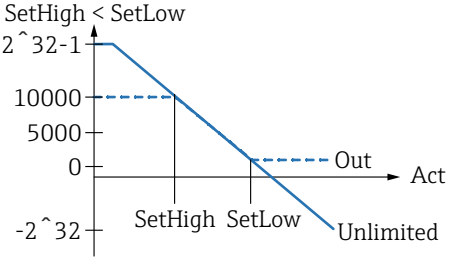
Description of the units

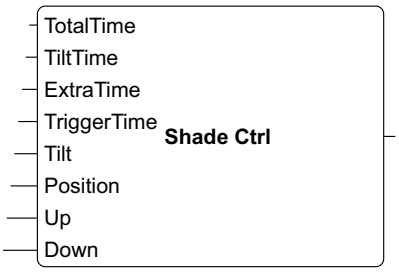
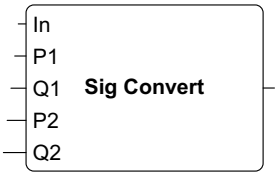
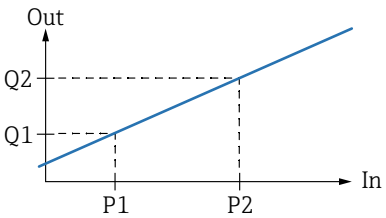
Unless otherwise indicated, units are processed during the processing stage of the IPO cycle .

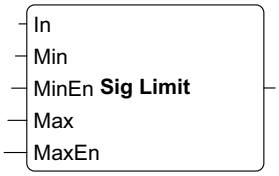
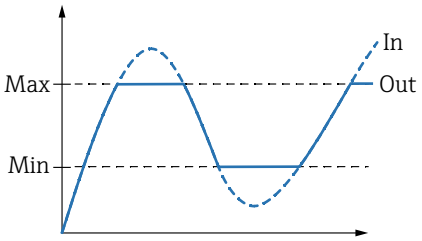
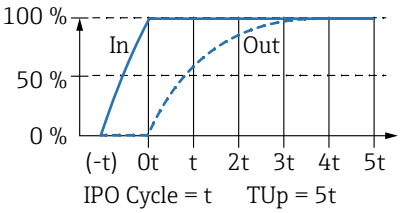
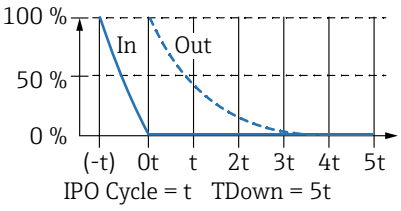
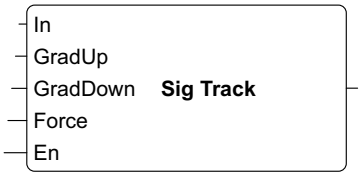
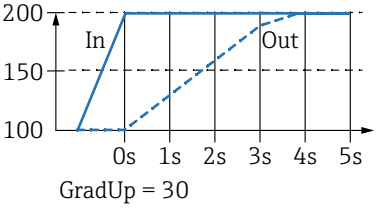
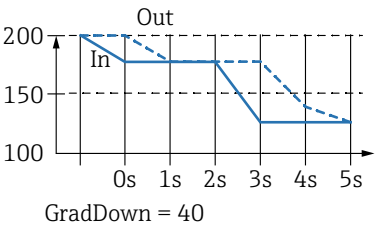
Unit	Description
	This unit performs an addition. It adds the values of its input ports and writes the total to its output port. The addition is performed in the largest numeric data type of all the output ports that are connected to the input ports of the unit. All the ports of the unit adopt this data type. Input ports connected to string output ports are treated as if they were connected to a 64-bit floating point output port. For example, if one input port is connected to an 8-bit unsigned integer output port and another input port is connected to an 8-bit signed integer output port, the addition is performed in an 8-bit signed integer, and this will also be the data type for all the ports.
	This unit performs a binary And. The operation is performed in the largest integer data type of all the output ports that are connected to the input ports of the unit. All the ports of the unit adopt this data type. Input ports connected to floating point or string output ports are treated as if they were connected to a 32-bit signed integer output port. Example: ▪ *0* and *0* ⇒ *0* ▪ *0* and *1* ⇒ *0* ▪ *1* and *1* ⇒ *1* ▪ *11 (1011_2)* and *14 (1110_2)* ⇒ *10 (1010_2)* ▪ *5 (00000005_{16})* and *-15 ($FFFFFFF1_{16}$)* ⇒ *1 (00000001_{16})*
	This unit represents a comparator. It compares the values of the two input ports *In1* and *In2* and assigns values to the three Boolean outputs. The output port *LT* is set to *1* if *In1* is less than *In2*. The output port *EQ* is set to *1* if *In1* is equal to *In2*. A tolerance value for the equation can be specified via the *Tol* input port. This is particularly useful for floating point values where direct comparison may not work on account of rounding errors. With a tolerance value of *0.5*, the values *1.0* and *1.5* are considered equal. If strings are compared, the *Tol* input port is ignored and should be left open. The output port *GT* is set to *1* if *In1* is greater than *In2*. The unit operates in the largest numeric data type of all the output ports that are connected to the input ports of the unit. All the input ports of the unit adopt this data type.
	This unit performs a time comparison. It compares the date and the time specified through its input ports with the current local time. If the two times match, the Boolean output port is set to *1*. The input port *Bitmap* (8-bit unsigned integer) can be used to specify which components of the date and time should be compared; if the value *0* is set, then all the input ports are ignored and the output port is set to *1*. There are input ports for the following date/time components: ▪ *Year:* compared if bit *0* of the input port *Bitmap* (16-bit unsigned integer) is set ▪ *Month:* compared if bit *1* of the input port *Bitmap* is set (8-bit unsigned integer, range [1 to 12]) ▪ *Day:* day of the month – compared if bit *2* of the input port *Bitmap* is set (8-bit unsigned integer, range [1 to 31]) ▪ *WeekDay:* days since Sunday – compared if bit *3* of the input port *Bitmap* is set (8-bit unsigned integer, range [0 to 6]) ▪ *Hour:* compared if bit 4 of the input port *Bitmap* is set (8-bit unsigned integer, range [0 to 23]) ▪ *Minute:* compared if bit *5* of the input port *Bitmap* is set (8-bit unsigned integer, range [0 to 59]) ▪ *Second:* compared if bit *6* of the input port *Bitmap* is set (8-bit unsigned integer, range [0 to 59])
	This unit represents a counter. Each rising edge (transition from *0* to *1*) on the Boolean input port *Clk* increases the numeric value on the output port *Val* (32-bit unsigned integer) by one. If the value on the Boolean input port is *Down 1*, the counter value is reduced by one instead. The maximum value that can be output on the *Val* port is *4,294,967,295 (2^{32}-1)*. The minimum value is *0*. An overflow (from 4,294,967,295 to 0 or vice versa) is indicated by the Boolean output port *Over*. Its value is *1* until the next clock pulse increases or decreases the counter value by one or the counter is reset. If the value on the Boolean input port *Rst* is 1, the counter value is reset to the current value of the input port *RVal* (32-bit unsigned integer).
	This unit represents a demultiplexer. It copies the value of the input port *In* to the output port *Out<K>*. The relevant output port is selected by the input port *K* (8-bit unsigned integer). *Out0* is selected if *K* equals *0*. If the value for *K* is too low, *Out0* is selected. If the value for *K* is too high, the output port with the highest index value is selected. The value of the Boolean input port *Store* determines whether a previously selected output port keeps its value (*Store 1*) or is reset to *0* (*Store 0*). The input port *In* and all the output ports adopt the data type of the output port connected to the input port *In*.

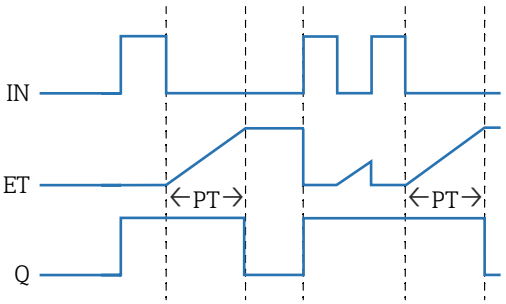
Unit	Description
	This unit performs a division. It divides the first input port by all the subsequent input ports and writes the quotient to its output port. If one of the input ports has the value *0*, the output port is set to *0*. The division is performed in the largest numeric data type of all the output ports that are connected to the input ports of the unit. All the ports of the unit adopt this data type.
	This unit extracts a single bit from the value of its input port *X* (32-bit unsigned integer). The relevant bit is selected by the input port *N* (8-bit unsigned integer). The bit is written to the Boolean output port. Bit numbering starts at 0.
	This unit has a single Boolean output port that is set to *1* only during the first cycle after the PLC has been started. This unit is processed in the input stage of the IPO cycle.
	This unit determines the maximum value of all of its input ports and writes this value to its output port. The function is performed in the largest numeric data type of all the output ports that are connected to the input ports of the unit. All the ports of the unit adopt this data type.
	This unit determines the minimum value of all of its input ports and writes this value to its output port. The function is performed in the largest numeric data type of all the output ports that are connected to the input ports of the unit. All the ports of the unit adopt this data type.
	This unit performs a multiplication. It multiplies the values of its input ports and writes the result to its output port. The multiplication is performed in the largest numeric data type of all the output ports that are connected to the input ports of the unit. All the ports of the unit adopt this data type.
	This unit represents a multiplexer. It copies the value of the input port *In<K>* to the output port. The relevant input port is selected by the input port *K* (8-bit unsigned integer). *In0* is selected if *K* equals *0*. If the value for *K* is too low, *In0* is selected. If the value for *K* is too high, the input port with the highest index value is selected. The input ports *In<K>* and the output port adopt the largest data type of all the output ports connected to one of the input ports *In<K>*.

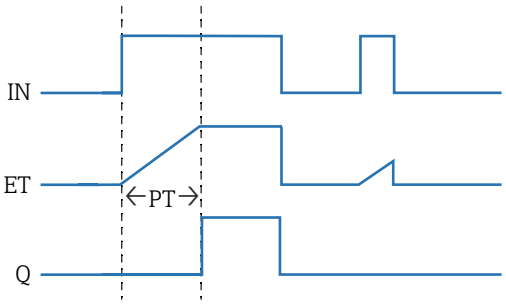
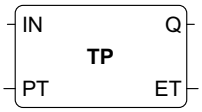
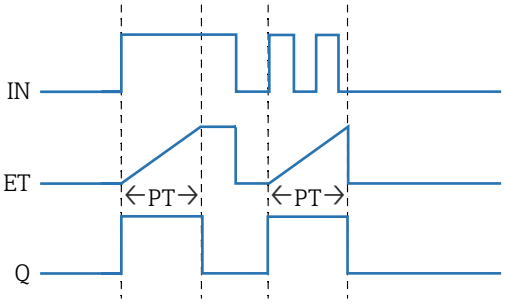
Unit	Description
SetOn SetOff Act En **On/Off Ctrl**	This unit represents an on/off controller. The input ports *SetOn*, *SetOff* and *Act* adopt the largest numeric data type of all the output ports that are connected to one of these input ports. The unit switches its Boolean output port on or off if the value of the input port *Act* exceeds or drops below the values of the input ports *SetOn* and *SetOff* respectively. The Boolean input port *En* can be used to enable the unit. If the value is *0*, the output port is always *0*. If *SetOn* = *SetOff*, the unit behaves as illustrated in the diagram below. The output port is switched on when *Act* > *SetOn*. The output port is switched off when *Act* ≤ *SetOff*. SetOn = SetOff  If *SetOn* > *SetOff*, the unit behaves as illustrated in the diagram below. The output port is switched on when *Act* ≥ *SetOn* (broken blue line). The output port is switched off when *Act* ≤ *SetOff* (solid blue line). SetOn > SetOff  If *SetOn* < *SetOff*, the unit behaves as illustrated in the diagram below. The output port is switched on when *Act* ≤ *SetOn* (solid blue line). The output port is switched off when *Act* ≤ *SetOff* (broken blue line). SetOn < SetOff 
Start Stop **OpenVPN** Running Connected	This unit can be used to control the OpenVPN client. The client is started when the Boolean input port *Start* switches from *0* to *1*. The client is stopped when the Boolean input port *Stop* switches from *0* to *1*. The Boolean output port *Running* indicates whether the client is running. The Boolean output port *Connected* indicates whether the client is connected to a server.
Or	This unit performs a binary OR. The operation is performed in the largest integer data type of all the output ports that are connected to the input ports of the unit. All the ports of the unit adopt this data type. Input ports connected to floating point or string output ports are treated as if they were connected to a 32-bit signed integer output port. Examples: ▪ *0* and *0* ⇒ *0* ▪ *0* and *1* ⇒ *1* ▪ *1* and *1* ⇒ *1* ▪ *3* (0011_2) and *8* (1000_2) ⇒ *11* (1011_2)

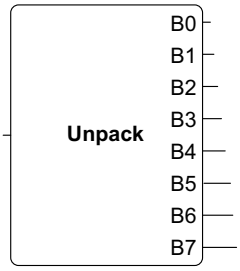
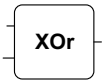
Unit	Description
	This unit packs the values of its 8 Boolean input ports into one octet and writes the octet to its 8-bit unsigned integer output port.
	This unit represents a proportional controller. The input ports *SetLow*, *SetHigh* and *Act* adopt the largest numeric data type of all the output ports that are connected to one of these input ports. On its output port *Out* (16-bit unsigned integer, range [*0..10,000*]), it outputs a percentage that is based on the relation between the value for its input port *Act* and the value range for its input ports *SetLow* and *SetHigh*. If the value of the port *Act* is outside this range, the value for the Out port is limited to the range [*0..10,000*] (*0 %* to *100.00 %*), while the value for the output port *Unlimited* (32-bit signed integer) can be greater than *10,000* or less than *0*. The Boolean input port *En* can be used to enable the unit. If the value is *0*, the output port is always *0*. If *SetOn = SetOff*, the unit behaves as illustrated in the diagram below. The output port is set to *0 % (0)* if *Act < SetLow*. It is set to *50 % (5,000)* if *Act = SetLow*. It is set to *100 % (10,000)* if *Act > SetLow*. *Unlimited* will have the same value as *Out*. SetHigh = SetLow  If *SetHigh > SetLow*, the unit behaves as illustrated in the diagram below. *Out* will be *0 % (0)* if *Act <= SetLow*. It will rise from *0 %* to *100 %* if the value for *Act* rises between *SetLow* and *SetHigh*. It will stay at *100 % (10,000)* if *Act* becomes >= *SetHigh*. *Unlimited* will drop below *0 %* if *Act < SetLow*. *Unlimited* will exceed *100 %* if *Act > SetHigh*. SetHigh > SetLow  If *SetHigh < SetLow*, the unit behaves as illustrated in the diagram below. *Out* will be *100 % (10,000)* if *Act <= SetHigh*. It will drop from *100 %* to *0 %* if the value for *Act* rises between *SetHigh* and *SetLow*. It will stay at *100 % (10,000)* if *Act* becomes >= *SetLow*. *Unlimited* will drop below *0 %* if *Act < SetHigh*. *Unlimited* will exceed *100 %* if *Act > SetLow*. SetHigh < SetLow 

Unit	Description
	This unit takes the binary value of its input port *X* (32-bit unsigned integer), sets the bit selected by the input port *N* (8-bit unsigned integer) to the state of the Boolean input port *B* and writes the resulting value to its output port (32-bit unsigned integer). Bit numbering starts at *0*.
	This unit represents an RS-Flipflop. The Boolean output port starts with a value of *0*. If the value for the Boolean input port *Set* is set to *1*, the value of the output port is also set to *1*. This value remains unchanged even if the value for the input port *Set* is reset to *0*. If the value for the Boolean input port *Rst* is set to *1*, the value of the output port is set to *0*. This value remains unchanged even if the value for the input port *Rst* is reset to *0*. If *Set* and *Rst* are activated at the same time, *Rst* has priority.
	This unit can be used to control window shades or shutters for example. Its first four input ports are used to define a number of time constants. The input port *TotalTime* (32-bit unsigned integer) defines the time (in ms) needed to move the shade (or shutter) from its lowest to its highest position (or vice versa). The input port *TiltTime* (32-bit unsigned integer) defines the time (in ms) needed by the shade to tilt (from the point it starts to ascending to the point it starts descending). This time can be set to zero for simple shutters. The value for the input port *ExtraTime* (32-bit unsigned integer, in ms) is used if the shade should move to its lowest or highest position to ensure it closes or opens fully. If the input port *Up* or *Down* is active for the period of time defined by the value of the input port *TriggerTime* (32-bit unsigned integer, in ms), this causes the shade to move to its highest or lowest position respectively. Note that the shade controller cannot control the motor of the window shade for periods shorter than the cycle time. Therefore, all times should ideally be a multiple of the cycle time. The input port *Tilt* (8-bit signed integer) is used to tell the shade controller to tilt the shade to a certain position. Values between *-100* and *100* are permitted. *-100* represents the extreme tilt position where the slats are lower on the inside. *0* is the horizontal tilt position. *100* represents the extreme tilt position where the slats are lower on the outside. The input port *Position* (8-bit signed integer) is used to tell the shade controller to move the shade to a certain vertical position. Values between *0* and *100* are permitted. *0* represents the highest position of the shade. *100* represents the lowest position of the shade. The unit first tries to reach the vertical target position and then the target tilt position. The Boolean input ports *Up* and *Down* can be used to move the shade manually. The manual input ports have priority over the automatic ports. If either the input port *Up* or *Down* is activated, the automatic operation is paused until either the input port *Tilt* or *Position* changes its value. The Boolean output ports *Up* and *Down* are used to control the shade's motor. The output ports *Tilt* and *Position* (8-bit signed integer) display the current position and tilt of the shade. The unit has an initialization sequence that moves the shade to the lowest position when the diagram is started in order to reach a known position. The output port *Down* is set to the time (*TotalTime* + *TiltTime* + *ExtraTime*) ms. All the inputs are ignored during this time.
	This unit represents a 32-bit-shift register. With every rising edge on the Boolean input port *Clk*, the unit shifts the content of its register to the left or right, depending on the value of the Boolean input port *Right* (*1* ⇒ shift right). The value of the Boolean input port *In* is shifted into the register. The resulting register content is written to the output port (32-bit unsigned integer).
	This unit transforms the value of the input port *In* according to a linear function and writes the result to the output port. The transformation is performed in the largest numeric data type of all the output ports that are connected to the input ports of the unit. All the ports of the unit adopt this data type. The linear function is defined by the two points (*P1*, *Q1*) and (*P2*, *Q2*). 

Unit	Description
	This unit can be used to limit the value of the input port *In*. If *In* is less than *Min* and the minimum limit is activated by the Boolean input port *MinEn*, the indication is set to *Min*. If *In* is greater than *Max* and the maximum limit is activated by the Boolean input port *MaxEn*, the indication is set to *Max*.  The limitation is performed in the largest numeric data type of all the output ports that are connected to the input ports *In*, *Min* and *Max* of the unit. These input ports and the output port adopt this data type.
	This unit is used to smooth a signal. If the value of the input port *In* changes, the value of the output port will be approximated to this new value using an exponential function. The value of the input port *TUp* (32-bit unsigned integer) refers to the time (in ms) that is needed to reach the new value if the old value is less than the new value. The value of the input port *TDown* (32-bit unsigned integer) refers to the time (in ms) that is needed to reach the new value if the old value is greater than the new value.   If the Boolean input port *Force* is set, the value of the input port *In* is copied immediately to the output port. The smoothing is performed in the numeric data type of the output port that is connected to the input port *In* of the unit. The input port *In* and the output port adopt this data type.
	This unit is used to limit the gradient of a signal. If the value of the input port *In* changes, the value of the output port follows this new value using a linear function. The value of the input port *GradUp* defines the maximum slope of this linear function per second if the new value is greater than the old value. The value of the input port *GradDown* defines the maximum slope of this linear function per second if the new value is less than the old value. Both gradients must be positive numbers.   If the Boolean input port *Force* is set, the value of the input port *In* is copied immediately to the output port. The Boolean input port *En* can be used to enable the unit. If the value is *0*, the output port is always *0*. The tracking is performed in the largest numeric data type of all the output ports that are connected to the input ports *In*, *GradUp* or *GradDown*. These input ports and the output port adopt this data type.

Unit	Description
Sel, Next0, Cond0, **State Machine 0**, State, Active	This unit represents the state of a state machine. There are eight different state machine units (*state machine 0* to *state machine 7*), allowing you to implement eight independent state machines. A state machine is implemented by placing various state machine units with the same state machine index (e.g. state machine 0). The value of the input port *Sel* (32-bit signed integer) of the relevant unit determines which state is handled by it. A state machine unit checks its Boolean input ports *Cond<X>* when it becomes active (state = *Sel*). If one of the Boolean input ports is set to *1*, the state machine changes its state – which is determined by the corresponding input port *Next<X>* (32-bit signed integer) – after the current IPO cycle. The output port *State* (32-bit signed integer) displays the current state of the state machine. The Boolean output port *Active* indicates that the corresponding unit is currently active (state of the state machine = *Sel*). The initial state is *0*.
Sub	This unit performs a subtraction. It subtracts the values of its second input port and the subsequent input ports from its first input port and writes the difference to its output port. The subtraction is performed in the largest numeric data type of all the output ports that are connected to the input ports of the unit. All the ports of the unit adopt this data type.
T, **T-FF**, Q, Clk	This unit represents an T-Flipflop. The Boolean output port has the value *0*. If the Boolean input port *T* is set to *1*, the Boolean output port changes its state with each rising edge on the Boolean input port *Clk*. If the input port *T* is set to *0*, the output port retains its previous value.
Int, **Timer**, Clk, En	This unit represents a timer. It outputs a periodic clock signal on the Boolean output port *Clk*. The duration of the signal is specified by the value of the input port *Int* (interval, 32-bit unsigned integer) and must be a multiple (at least twice) of the cycle time of the PLC. If the value of the input port *Int* is less than the cycle time or not divisible by the cycle time, the value is rounded up internally to the nearest multiple of the cycle time. The clock signal is only generated as long as the Boolean input port *En* is set to *1*.
IN, Q, **TOF**, PT, ET	This unit represents a timer off-delay. When the Boolean input port *IN* switches to *1*, the Boolean output port *Q* is set to *1*. The timer is started when the Boolean input port *IN* switches to *0*. The output port *ET* (elapsed time, 32-bit unsigned integer) indicates how much time, in milliseconds, has elapsed since the timer was started. When the value of the output port *ET* reaches the value of the input port *PT* (preset time, 32-bit unsigned integer) the timer is stopped and the output port *Q* is reset.  If the value of the input port *Int* is less than the cycle time or not divisible by the cycle time, the value is rounded up internally to the nearest multiple of the cycle time.

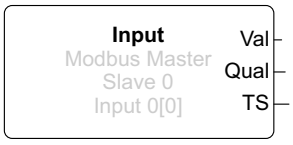
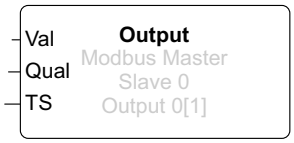
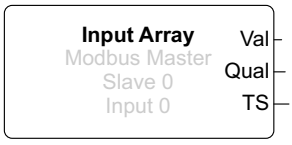
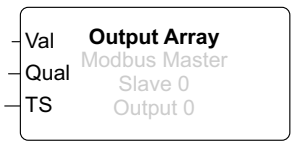
Unit	Description
	This unit represents a timer on-delay. The timer is started when the Boolean input port *IN* switches to *1*. The output port *ET* (elapsed time, 32-bit unsigned integer) indicates how much time, in milliseconds, has elapsed since the timer was started. When the value of the output port *ET* reaches the value of the input port *PT* (preset time, 32-bit unsigned integer) the timer is stopped and the Boolean output port *Q* is reset. The output port *Q* is reset when the input port *IN* switches to *0*.  Note that if the value of the input port *Int* is less than the cycle time or not divisible by the cycle time, the value is rounded up internally to the nearest multiple of the cycle time.
	This unit represents a timer pulse. When the Boolean input port *IN* switches to *1*, the Boolean output port *Q* is set to *1* and the timer is started. The output port *ET* (elapsed time, 32-bit unsigned integer) indicates how much time, in milliseconds, has elapsed since the timer was started. When the value of the output port *ET* reaches the value of the input port *PT* (preset time, 32-bit unsigned integer) the timer is stopped and the output port *Q* is reset to *0*.  Note that if the value of the input port *Int* is less than the cycle time or not divisible by the cycle time, the value is rounded up internally to the nearest multiple of the cycle time.
	This unit represents a trigger. It sets its Boolean output port to *1* for an IPO cycle if it detects a rising edge on one of its Boolean inputs. Negate the input port to detect a falling edge. To detect a rising or a falling edge, connect the same input signal to two of the trigger's input ports and negate one of them.

Unit	Description
	This unit unpacks the 8 bits of the octet value of its input port (8-bit unsigned integer) and writes them to its Boolean output port.
	This unit performs a binary Exclusive Or (Xor). The operation is performed in the largest integer data type of all the output ports that are connected to the input ports of the unit. All the ports of the unit adopt this data type. Input ports connected to floating point or string output ports are treated as if they were connected to a 32-bit signed integer output port. Examples: ▪ *0* and *0* ⇒ *0* ▪ *0* and *1* ⇒ *1* ▪ *1* and *1* ⇒ *0* ▪ *15 (1111_2)* and *8 (1000_2)* ⇒ *7 (0111_2)*

Input and output elements (I/Os)

There is one element for every input (I) and output (O). The number and structure of the I/Os depend on the specific Fieldgate FXA42 device and its configuration.

Properties of the input and output elements:
- Every input or output element has a port - the value. The port can be connected to other elements.
- The port *Val* represents the value of the input or output and has the same data type as the input/output.
- The name of the interface, the device and the value are displayed in gray below the element type.

Unit	Description
	This element represents an input. The value of the input is read from the physical inputs during the input stage of the IPO cycle.
	This element represents an output. The value of the output is written to the physical outputs during the output phase of the IPO cycle.
	This element represents an array of inputs. In contrast to a plain *input* element, it can only be connected to an *output array* of the same data type and size. The values of the inputs are read from the physical inputs during the input stage of the IPO cycle.
	This element represents an array of outputs. In contrast to a plain *output* element, it can only be connected to an *input array* of the same data type and size. The values of the outputs are written to the physical outputs during the output phase of the IPO cycle.

Internally, the inputs/outputs are addressed via an interface index, device index, value index and, optionally, an array index. If the Fieldgate FXA42 has a number of digital inputs/outputs and a Modbus master interface, for example, the interface index will select

one of these two interfaces. The device index can select the Modbus slave, for example, and the value index would therefore select the relevant Modbus register. The array index is also used if the corresponding value addresses an element of an array.

When you hover the cursor over an I/O element, a tool tip appears displaying the indexes, data type and array size.

Variables

The *Variable* element represents variables that are not linked to a physical I/O. A *Variable* element corresponds to a variable with the same name and can be used as either an input or an output. Variables can be configured on the Variable page.

Unit	Description
Variable	This element represents the value of the variable during the input stage of the IPO cycle.
Variable	This element represents a variable as an output. It writes its value to the variable during the output phase of the IPO cycle.

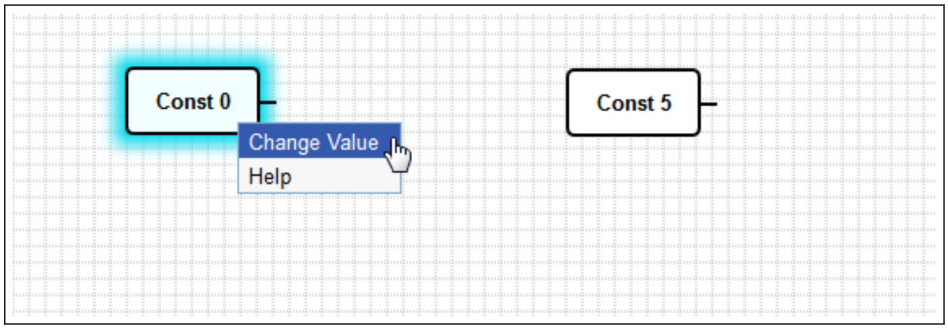
Constants

If you add a constant via the toolbar, a dialog box opens which you can use to enter a fixed value. This value can be a decimal integer, a floating point or a string value. Integer values are limited to the range $[-2^{31}, 2^{32}-1]$. Floating point values are limited to an accuracy of 15 decimal places. Strings are limited to 4096 bytes.

The data type of a constant is the smallest data type that can represent the value of the constant. Here are some examples:
- *0 → Boolean (false)*
- *1 → Boolean (true)*
- *120 → 8-bit unsigned integer*
- *-5 → 8-bit signed integer*
- *500 → 16-bit unsigned integer*
- *-200 → 16-bit signed integer*
- *70000 → 32-bit unsigned integer*
- *-35000 → 32-bit signed integer*
- *1.5 → 32-bit floating point number*
- *3.14159265359 → 64-bit floating point number*
- *5m → String*

Constants are processed in the input stage of the IPO cycle.

The value of the constant can be changed. To change the value of the constant, right-click the element. A popup menu appears (see the following graphic). Select the entry *Change value*.



8.3.3 Diagram settings

Clicking the *Diagram settings* button in the toolbar opens a dialog box where you can change the following diagram settings:

Diagram settings	Description
Description	You can enter a description for the diagram here. The description can comprise up to 1024 printable ASCII characters and line breaks.
Cycle time	Here you can configure the cycle time with which the PLC runs while executing the diagram. A cycle time between 25 and 1000 ms can be configured. Larger values enable a more complex diagram, i.e. more elements. Increase the cycle time if you get a message that the diagram is getting too complex.
Treat all numerical I/O values as 32-bit signed integers	For backward compatibility, select this checkbox so that the diagram treats all I/O values as 32-bit signed integers.

8.3.4 Status bar

The following graphic shows the status bar of the editor. The status bar displays information about the current state of the PLC.

The information that is displayed in the status bar is described in detail in the following section.

Button	Description
	This symbol is displayed if the connection to the device is lost.
	The stoplight indicates the current state of the PLC: Red: No diagram has been loaded. The PLC is not running. Amber: A diagram has been loaded but the PLC is not running. Green: A diagram has been loaded and the PLC is running.
Duty cycle	The duty cycle of the PLC is displayed behind. This indicates both the current duty cycle and the maximum duty cycle since the PLC started. The duty cycle is indicated as a percentage. A duty cycle of 50% means that the PLC is using 50% of the available CPU processing time. Make sure to leave enough CPU processing time for other processes in the system! The duty cycle should be kept below 75%. If the diagram becomes more complex, increase the PLC cycle time in the Diagram Settings. If the duty cycle is close to 100%, it is no longer possible to operate the Fieldgate FXA42.

8.3.5 Running the diagram

Click the **Start** button in the tool bar to start execution of the diagram saved to the PLC. While the PLC is running, the **Start** button changes to the **Stop** button. Click the **Stop** button to stop the PLC.

IPO cycle

While the diagram is being executed, the device's runtime system executes an IPO cycle (Input-Process-Output). This means that the inputs are read out first of all (both the physical inputs and the variables and constants). The units are processed and the outputs

(the physical outputs and the variables) are then written. The cycle time can be configured in the Diagram Settings dialog.

Note that events that persist for a shorter period of time might not be recognized.

Running state at start-up

The PLC stores its current running state in the non-volatile memory. If the PLC is disconnected from the power supply when it is running, it will it will start running after next start-up.

Event log messages

Event log messages are messages that the PLC may log to the event log. All messages are prefixed with the text *PLC Driver*:

The PLC has been started.

The PLC has been started successfully.

The PLC has been stopped.

The PLC has been stopped successfully.

A new diagram has been saved.

A new diagram has been saved successfully to the PLC.

-10	Out of memory
-12	Internal data queue overflow: data was produced faster than it could be processed.

Contact customer support if an error code is displayed that is not listed here.

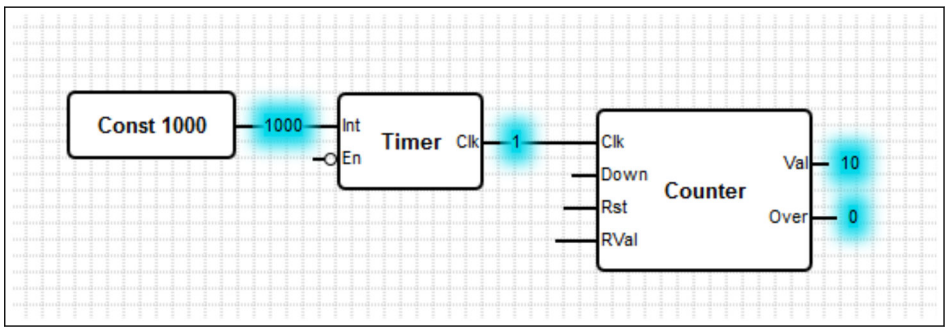
Exception in task: <message>

A fatal exception has occurred inside the PLC task. A detailed description is provided.

Contact customer support.

8.3.6 Live view

Via the Live view function it is possible to see the current state of the PLC directly in the diagram view. Once you click the **Start Live view** button in the tool bar of the Editor program, the actual value of each output port is displayed in a small blue field next to the port (see the following graphic).



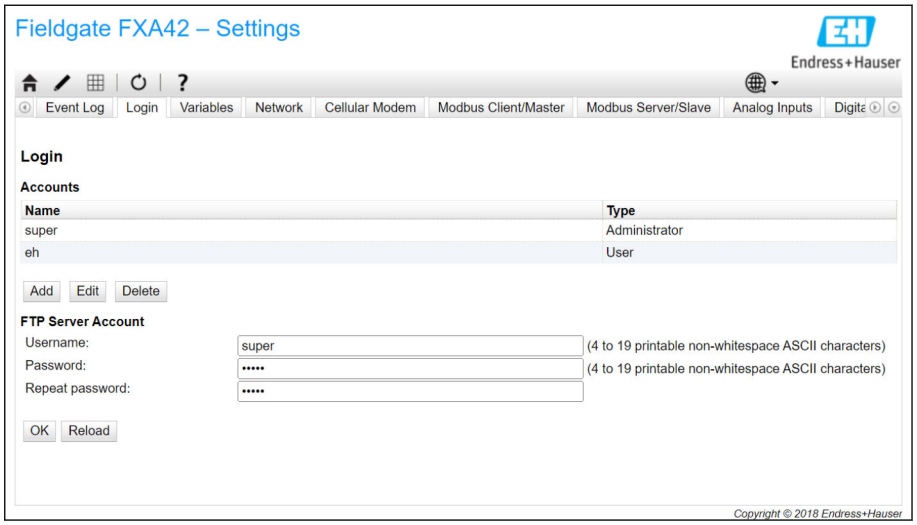
The values are updated as quickly as possible.

If the diagram is changed when Live view is active, this will cause errors to occur because the values received from the PLC will no longer match the diagram. If this happens, the Live view is stopped automatically.

Click the **Start Live view** button again to quit the Live view manually.

8.4 Settings

You can configure your Fieldgate FXA42 on the **Settings** page (see graphic below).



There is a toolbar on the Settings page. The buttons in this toolbar are described in detail in the following section.

Button	Description
	Closes the Settings page and opens the home page.
	Closes the Settings page and opens the Fieldgate FXA42 editor.
	Closes the Settings page and opens the Fieldgate FXA42 Grid View.
	Reboots the Fieldgate FXA42 in order to apply changes.
	Opens the Help.

Tabs are located below the toolbar. Clicking a tab opens a page where settings for a communication protocol or another important function of the device can be made and modified. The individual pages are described in detail in separate sections.

The following tabs may be available in the device, depending on the particular device version:

- **Event log**
- **Login**
- **Variables**
- **Network**
- **Cellular Modem**
- **Modbus Client/Master**
- **Modbus Server/Slave**
- **Analog Inputs**
- **Digital Inputs**
- **Data Transmission**
- **Messages**

- **Time**
- **SMS I/O**
- **OpenVPN**
- **DHCP server**
- **NAT**
- **Firewall**
- **Update**
- **Export**

Functions

Due to the many features and communication protocols that are available on the device, significant response time latencies (particularly if communicating via the cellular modem) and CPU overload may occur if the functions and communication protocols are used extensively.

8.4.1 Event Log

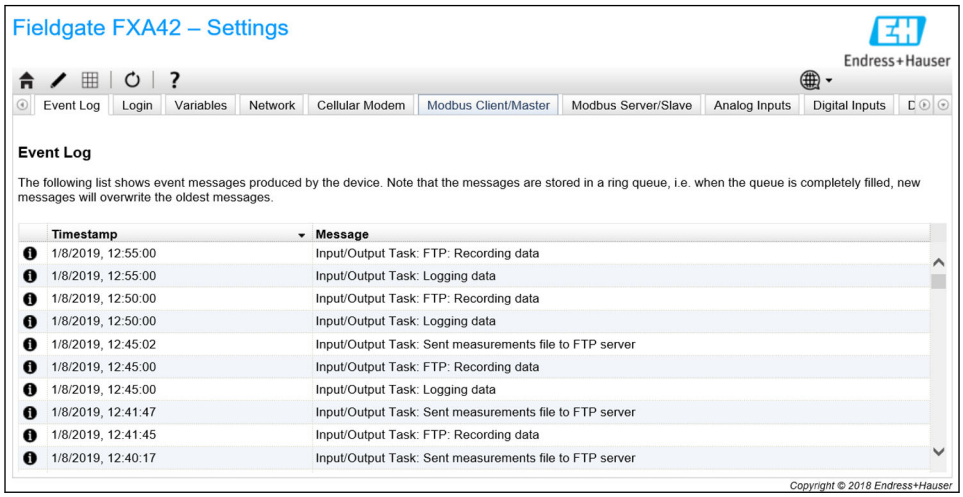
The event log is the central point where all the components of the Fieldgate FXA42 firmware store their event messages.

Each event message consists of the message text, a time stamp and an event type.

Click a message text to open the help and to display more detailed information about the message.

Time stamps are saved in the time zone that is selected in the Fieldgate FXA42. The time zone currently selected can be either the local time zone that is saved or the time zone provided by the FIS (Field Information Server) connection if it is enabled.

The system clock of the Fieldgate FXA42 might not be synchronized. In this case, the time stamps are not displayed correctly.



The event types are represented by specific icons:

Symbol	Description
	Information: provides information about normal operation.
	Warning: informs the user about unexpected but unproblematic events.

Symbol	Description
	Error: informs the user about a failure in one of the firmware's components.
	Fatal error: such errors generally prevent further device operation.

Events are stored in a circular buffer in the RAM. This means that the event log is cleared when the device is restarted and that new events overwrite older events when the buffer is completely full.

Messages index

The following section contains an index of all the messages that can be logged by the Fieldgate FXA42 components.

Running the diagram
- The PLC has been started.
- The PLC has been stopped.
- A new diagram has been saved.
- Exception in task: <*message*>

FIS update
- Update due to FIS command
- Firmware update via FIS request denied: Firmware update via FIS not enabled
- Firmware update via FIS request denied: Update/configuration already in progress

Cellular modem
- Stopped
- Started
- Running
- Deactivated
- Activated
- Powered modem
- Modem initialized (RSSI: <*x*> dBm)
- SIM card ID: <*x*>
- Registered to network
- Roaming
- Data connection established
- Opening fallback connection
- Closing fallback connection
- Invalid PIN or SIM card locked (code <*x*>)
- Modem initialization failed. (code <*x*>)
- Network registration timed out ((not) searching)
- Roaming disallowed
- Network registration failed (code <*x*>, network status <*y*>)
- Data connection failed (code <*x*>)
- Network lost (code <*x*>, network status <*y*>)
- Data connection broken (DCD pin: <*x*>, PPP status: <*y*>, GPRS pin: <*z*>)
- Connection supervision failed.
- Modem reset
- Hanging! (state: <*x*>)

WLAN
- Started
- Running
- Configured IP through DHCP
- Stopping driver
- Stopped
- Connection indication

Modbus client/master
- Connected to TCP device at *<IP address>:<port>*.
- Read/wrote from/to TCP device at *<IP address>*:*<port>* (unit: *<unit identifier>*, function code: *<function code>*, address: *<address>*, quantity: *<quantity>*)
- Read/wrote from/to RTU device *<device address>* (function code: *<function code>*, address: *<value address>*, quantity: *<quantity>*)
- The interval has been violated.
- Could not connect to TCP device at *<IP address>*:*<port>*. (Error code *<code>*).
- Could not read/write from/to TCP device at *<IP address>*:*<port>* (unit: *<unit identifier>*, function code: *<function code>*, address: *<address>*, quantity: *<quantity>*, result code: *<result code>*, error code: *<error code>*, exception code: *<exception code>*)
- Read illegal floating point value from TCP device at *<IP address>*:*<port>* (unit: *<unit identifier>*, function code: *<function code>*, address: *<address>*, quantity: *<quantity>*)
- Could not read/write from/to RTU device *<device address>* (function code: *<function code>*, address: *<value address>*, quantity: *<quantity>*, result code: *<result code>*, exception code: *<exception code>*)
- Read illegal floating point value from RTU device *<device address>* (function code: *<function code>*, address: *<value address>*, quantity: *<quantity>*)
- Portal communication error *<error code>*

Modbus server/slave
Portal communication error *<error code>*

Data transmission and data logging
- Sent FIS data message successfully
- Error on parsing FIS data message
- FIS: Recording data
- FIS event message transmitted successfully
- FIS: Recording event
- HTTP error *<HTTP-Error>* occurred while sending FIS event message
- HTTP connection error occurred while sending FIS event message
- HTTP connection error occurred while sending FIS data message
- FIS data message transmitted successfully
- HTTP error *<HTTP-Error>* occurred while sending FIS data message
- Invalid FIS authentication
- Logging data

Messages
- Sending data e-mail to *<name>*, address: *<name>*
- Sending limit e-mail to *<email>*, address: *<address>*
- Sending alarm e-mail to *<email>*, address: *<address>*
- Sent data e-mail message successfully
- Could not send data e-mail
- E-mail: No data recorded
- E-mail: Recording data
- E-mail: Recording event
- FTP: Recording data
- Could not send file to FTP server
- Sent measurements file to FTP server
- Sending FIS registration message
- Sending configuration to FIS
- Configuration successful
- FIS configuration version: *<Version>*
- Invalid FIS authentication data. Trying again in *<T>* minutes.
- HTTP error *<HTTP-Error>* occurred while sending FIS registration message. Trying again in *<T>* minutes.
- HTTP connection error occurred while sending FIS registration message. Trying again in *<T>* minutes.
- FIS registration successful
- New configuration available: *<Version>*
- Could not apply FIS configuration, update in progress.

- FIS configuration version: *<Version>*
- Downloading new configuration from FIS
- Could not apply configuration
- Re-booting due to FIS command
- Re-registration due to FIS command
- Update due to FIS command
- Time changed from FIS

System time
- Running
- System clock updated via SNTP
- System clock updated from RTC
- Could not get exclusive access to clock(s).
- Daylight saving time rules will be used up within the next two years.
- SNTP client error: *<message>*
- RTC not available
- Could not write to RTC: *<message>*
- Could not read from RTC: *<message>*
- Could not read daylight saving time file.
- No daylight saving time rule found for the current time.
- DNS error (*<error code>*) for server *<server name/IP>*
- Could not open socket for server *<server name/IP>*
- Could not send to server *<server name/IP>*
- Failed to receive reply from server *<server name/IP>*
- Unexpected packet format from server *<server name/IP>*
- Timestamps not plausible from server *<server name/IP>*

OpenVPN
- Driver has been started.
- Driver has been stopped.
- Driver stopped.
- Connection established.
- Connection closed.
- Authority's certificate uploaded.
- Certificate uploaded.
- Private key uploaded.
- User and password file uploaded.
- Diffie-Hellman file uploaded.
- Could not start driver.
- Could not stop driver.
- Driver stopped unexpectedly.
- Upload of authority's certificate failed.
- Upload of certificate failed.
- Upload of private key failed.
- Upload of user and password file failed.
- Upload of Diffie-Hellman file failed.

DHCP server
- Running
- Added static lease IP=*<x>*, MAC=*<y>*
- Discover message received, CI=*<x>*, MAC=*<y>*
- Request message received, CI=*<x>*, MAC=*<y>*
- Leased IP=*<x>*, Leasing Time=*<y>*, Index=*<z>*
- Release message received, CI=*<x>*, MAC=*<y>*
- Release IP=*<x>*, Index=*<y>*
- Network interface not configured
- Failed to send response message, error *<x>*
- No more client addresses available
- Receive Error *<x>*
- Received malformed message
- No interface found for given IP address

- Open socket failed
- Bind socket failed
- Only <*x*> clients possible due to netmask setting
- Failed to allocate client data structure
- Adding static lease IP=<*x*> failed, IP address is in use
- Adding static lease IP=<*x*> failed, no free slot
- Adding static lease IP=<*x*> failed, wrong IP address

Network address translation
- Running
- <*x*> static mapping(s) read from configuration
- No free mapping entry available for incoming connection from internal interface
- No free firewall rule entry available for outgoing connection

Update
- Running
- Package successfully loaded via local web server
- Loading package from remote web server...
- Package successfully loaded from remote web server
- Checking package...
- About to reboot...
- Loading package via local web server timed out
- Target directory for remote update package does not exist
- Target file for remote update package is not accessible
- Loading package from remote web server failed (code <*x*>)
- The type of the package's signature does not match the expected type of signature. (<*signature type*>)
- Invalid package flag(s) (<*flags*>)
- Firmware name does not match. This package is for "<*firmware name*>" firmware.
- This package cannot be applied to the current firmware version.
- Target name does not match. This package is for "<*target name*>" target.
- Variant name does not match. This package is for "<*variant name*>" variant.
- This package is limited to the device with the MAC address <*MAC address*>.
- Invalid package signature
- Could not open package. Message: <*message*>
- Update disallowed by application (<*code*>)
- Could not launch update.
- Portal communication error <*x*>

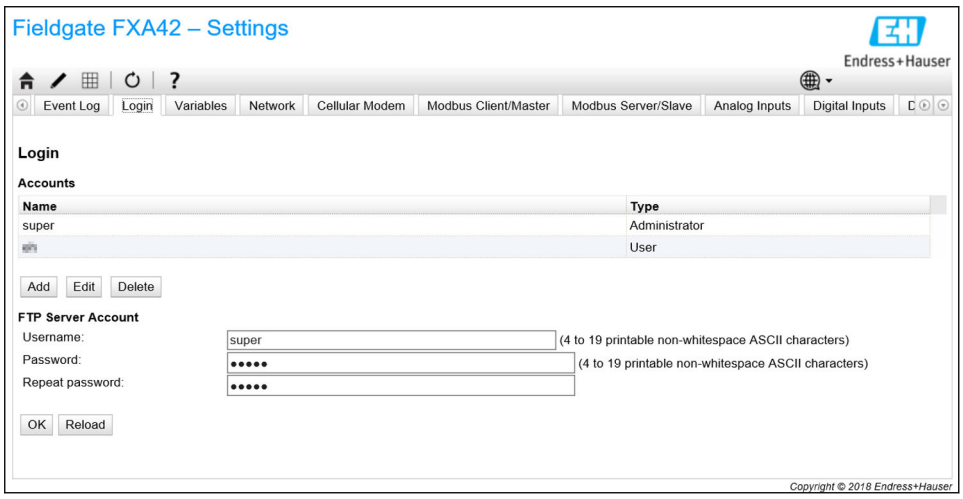
Export
- Preparing export...
- Packing update package...
- Update package has been successfully packed
- Preparation failed. Message: <*message*>
- Packing failed. Message: <*message*>

System start
- Started
- I/O hardware manager initialized
- NAT/firewall service initialized
- Ethernet (1) driver started.
- Cellular modem driver initialized
- Update module initialized
- PLC driver initialized
- Message manager initialized
- DHCP server initialized
- OpenVPN client initialized
- Status web service initialized
- System time manager initialized
- COM Server initialized
- Diagram loaded

- Web configuration modules initialized
- Update exporter module initialized
- Update web service initialized
- Running
- Starting update from external medium.
- Link detected at Ethernet (*<interface index>*).
- Restarting DHCP configuration at Ethernet (*<interface index>*).
- DHCP configuration completed at Ethernet (*<interface index>*).
- Power fail handling not supported
- Not enough power fail capacity
- Retentive data could not be loaded.
- The internal flash drive seems to be weak.
- Flash write error. The internal flash drive is probably defect.
- One or more certificates could not be loaded.
- Could not initialize NAT/firewall service. (*<error code>*)
- Could not start Ethernet (1) driver.
- Unsupported Ethernet (1) interface type. (*<interface type>*)
- Could not initialize NAT/firewall service. (*<error message>*)
- Could not initialize cellular modem driver: *<error message>*
- Could not initialize WLAN driver: *<error message>*
- Could not initialize update module: *<error message>*
- Could not initialize DHCP server.
- Could not initialize OpenVPN client: *<error message>*
- Could not initialize system time manager: *<error message>*
- Could not initialize COM server: *<error message>*
- Could not initialize portal Event Log service: *<error message>*
- Could not load and start diagram.
- Could not initialize web configuration modules: *<error message>*
- Could not initialize update exporter module: *<error message>*
- Could not initialize update web service: *<error message>*
- Task cycle time has been violated.
- Could not start update from external medium.
- Link lost at Ethernet (*<interface index>*).
- RTOS version is not supported. Version (*<version number>*) is required.
- Device is secured with the default password, please change it.
- Fatal error: *<error message>*

8.4.2 Login

You can configure the login data for the Fieldgate FXA42 on this page.



Up to 5 user accounts can be created, which are used as either administrator accounts or normal user accounts. The user list may not be empty. The first account is always an administrator account. At least one administrator account must be defined.

Administrators have access to the secured areas of the local website. Users only have access to the home page and the grid view.

If the credentials of the first administrator correspond to the default access data (user name: "super", password "super"), a system message opens when a configuration website is loaded. The system message contains a prompt to change the access data. **Make sure to make a note of the new access data** and store this information in a safe place!

NOTICE

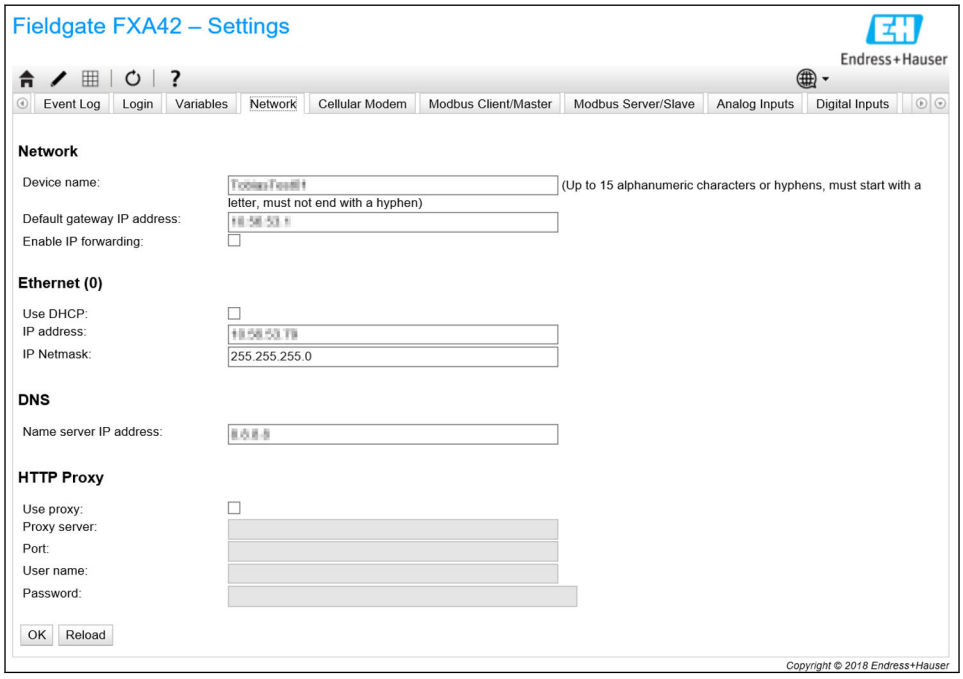
Forgotten your login data?

If you cannot find your login data, the device must be reset to the factory settings (reset). All settings will be lost!

- ▶ Switch off the Fieldgate FXA42 (switch off the supply voltage).
- ▶ Press and hold the reset button. The reset button can be accessed through a small hole in the front.
- ▶ Switch on the Fieldgate FXA42. Press and hold down the reset button while the device is booting until the **Web-PLC** LED flashes twice. The factory settings are restored.

8.4.3 Network

General network settings can be configured on this page.



Device name

The device name is registered as a NetBIOS name. Within the local area network, the name of the device - instead of the IP address - can be used to access the device. In addition to the configurable name, another name composed of the prefix *MAC* and the MAC-ID of the device (e.g. *MAC003056A1DB30*) is registered.

Default gateway IP address

The default gateway can be overwritten via a dynamic IP configuration, e.g. via DHCP or when a cellular modem connection is established.

Enable IP forwarding

If IP forwarding is enabled, the device will forward IP traffic from one network interface to another. This is necessary for NAT, for example.

Ethernet (0)

The IP address settings of the device's Ethernet interface can be configured in this section. Note: once these settings are changed, it may not be possible to reach the device at the same address any more.

DNS

The IP address of a DNS server can be explicitly configured in this section. This setting is not needed if the device is configured to get its IP configuration via DHCP or a cellular modem connection. The DNS server is configured automatically in this case.

HTTP Proxy

A proxy server that should be used for HTTP connections can be configured in this section.

The necessary information can be obtained from your local network administrator.

Open-source software

The following open-source software has been used to implement the NetBIOS name registration:

NetBIOS over TCP/IP (NBT) name registration

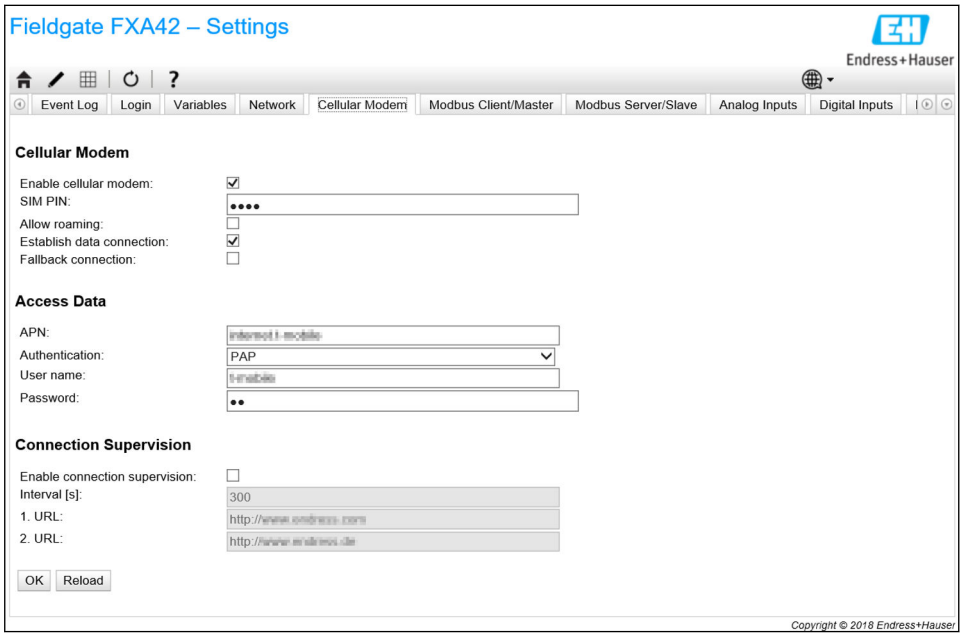
The source code used is based on documentation and code examples by Christopher R. Hertel.

Project website: ubiqx.org/cifs

License: LGPL

8.4.4 Cellular Modem

The cellular modem can be enabled and configured on this page.



To enable the cellular modem, tick the **Enable cellular modem** check box and enter the PIN of the SIM card.

It is possible to allow or disallow the modem to log into a network other than your home network (roaming). To enable roaming, tick the **Allow roaming** check box.

Roaming connections often result in higher costs.

To establish a cellular radio connection, tick the **Establish data connection** check box.

Registering the device for the first time typically takes up to 40 minutes for LTE NBioT.

The cellular radio connection can also be used as **Fallback connection**. In this case, the data connection is only established through the cellular modem if no other network interface provides Internet connectivity.

To use a cellular radio connection as a fallback connection, tick the **Fallback connection** check box.

If the Internet connection is established with the help of a company's own proxy server, then a cellular modem cannot be used as a fallback solution.

To establish a data connection, you must enter **Access Data**. The most important setting here is the APN (access point name). If authentication is required, the authentication type, user name and password can be configured here.

The data for these fields can be obtained from the mobile network provider.

The connection supervision function is used to supervise both the cellular modem connection and the other connections. When the cellular modem connection is established, it is used to check whether one of the other network interfaces provides Internet connectivity again. The cellular modem data connection will only be closed once the connection supervision has succeeded on another network interface 3 times in a row.

Connection Supervision

The connection supervision will try to connect to the first URL whenever there has been no payload traffic for the period of time indicated. The period can be specified between 60 and 60000 seconds. If the connection to the first URL fails, the second URL will be tried. If the second URL also fails the cellular modem connection will be re-established.

- Use the connection supervision function if the cellular modem driver could have problems recognizing the connection. Note that this function may produce additional network traffic.
- Connection supervision may not be disabled if the cellular modem connection is used as a fallback connection.
- The connection supervision must be enabled for applications that require continuous data collection. The connection supervision function supervises the cellular modem connection and resets the modem if the connection is broken.
- The predefined supervision URLs can only be reached with SIM cards that allow access to the Internet.

Signal strength

To ensure a stable connection and an adequate performance of all the communication functions of the device, make sure that the signal level is at least -79 dBm (Good).

Low signal strength may decrease the transfer rate significantly or completely drop the connection and result in a loss of function of the device.

The correlation between signal strength and connection quality is provided in the following table:

Signal strength	Connection quality
Under -101 dBm	Bad
-101 dBm to -90 dBm	Weak
-89 dBm to -80 dBm	Medium
-79 dBm to -65 dBm	Good
Over -65 dBm	Excellent

Critical applications

Cellular telecommunication devices operate using radio signals and therefore are not guaranteed to have a reliable connection in all conditions. For reliable continuous data transmission, do not rely exclusively on a wireless device.

Antenna

Keeping your body close to a cellular antenna might negatively affect your health. The use of antennas with a gain factor of more than 2.3 dBi might require additional approval at the place of operation.

Event log messages

The following section describes the messages that the cellular modem driver may log to the event log. All messages are prefixed with the text *Cellular Modem Driver*.

Stopped

The cellular modem driver has been stopped.

Started

The cellular modem driver has been started.

Running

The cellular modem driver is now running.

Deactivated

The cellular modem driver has been temporarily deactivated.

Activated

The cellular modem driver has been re-activated after temporary deactivation.

Powered modem

The supply voltage for the cellular modem hardware has been switched on.

Modem initialised (RSSI: <x> dBm)

The cellular modem has been successfully initialized. The RSSI value ranges from <= *-113* to >= *-51 dBm*.

SIM card ID: <x>

This message provides information about the SIM card's ID.

Registered to network

The cellular modem has successfully registered to a cellular network.

Roaming

The cellular modem has registered to a network other than the home network. Note that roaming connections will normally produce higher costs.

Data connection established

A data connection has been successfully established.

Opening fallback connection

The cellular modem is being used as a fallback interface. The connection is being established because no other network interfaces provide Internet connectivity.

Closing fallback connection

The cellular modem is being used as a fallback interface. The connection is being closed because another network interface provides Internet connectivity.

Invalid PIN or SIM card locked (code <x>)

Either the SIM PIN is invalid or the SIM card has already been locked because a wrong PIN has been tried too often.

Possible codes:

Code	Description
10	No SIM card has been inserted.
11	Incorrect SIM PIN or SIM PIN not provided.
12	The PUK is required because a wrong PIN has been tried too often. Remove the SIM card, insert it into a cellular phone and unlock it by entering the PUK.
13	The SIM card has been permanently blocked. Contact your mobile network provider.

Modem initialisation failed. (code <x>)

Initialization of the cellular modem hardware failed.

Possible codes:

Code	Description
14	The SIM card is busy.
-102	The cellular modem hardware returned an error.
-103	The cellular modem hardware did not answer.
-105	A reply from the cellular modem hardware was too long.
-134	The cellular modem hardware is invalid.

Contact customer support if an error code is displayed that is not on the above list.

Network registration timed out ((not) searching)

No cellular network could be found within a reasonable time. The message also indicates whether the cellular modem hardware is still searching for networks.

Roaming disallowed

The cellular modem did not connect to any network because the home network was not available and roaming has been disallowed in the configuration.

Network registration failed (code <x>, network status <y>)

The cellular modem could not register to any network.

Possible codes:

Code	Description
0	See network status
14	The SIM card is busy.
-102	The cellular modem hardware returned an error.

Code	Description
-103	The cellular modem hardware did not answer.
-105	A reply from the cellular modem hardware was too long.
-134	The cellular modem hardware is invalid.

The network status can have the following values:

Network status	Description
0	Not registered to any network
1	Registered to home network
2	Not registered to any network; searching for a network to register to.
3	Registration has been denied by the designated network.
4	Unknown network status
5	Registered to a network other than the home network (roaming)

Contact customer support if an error code or network status is displayed that is not on the above lists.

Data connection failed (code <x>)

No data connection could be established.

Possible codes:

Code	Description
-3	Invalid user name or password
-4	The network interface could not be opened. General error For example, it could mean a failed login to the mobile provider's network.
-6	An invalid IP configuration was received from the provider.
-7	No PPP connection could be established.

Contact customer support if an error code is displayed that is not on the above list.

Network lost (code <x>, network status <y>)

The cellular modem lost the connection to the network.

Possible codes:

Code	Description
0	See network status
14	The SIM card is busy.
-102	The cellular modem hardware returned an error.
-103	The cellular modem hardware did not answer.
-105	A reply from the cellular modem hardware was too long.
-134	The cellular modem hardware is invalid.

The network status can have the following values:

Network status	Description
0	Not registered to any network
1	Registered to home network
2	Not registered to any network; searching for a network to register to.
3	Registration has been denied by the designated network.
4	Unknown network status
5	Registered to a network other than the home network (roaming)

Contact customer support if an error code or network status is displayed that is not on the above lists.

Data connection broken (DCD pin: <x>, PPP status: <y>, GPRS pin: <z>)

The data connection has been unexpectedly closed. The message also shows the status values of the cellular modem hardware's DCD pin (1: connected, 0: not connected), the GPRS pin (1: connected, 0: not connected) and the status of the PPP client network interface:

Status	Description
-1	The PPP client is not running.
0	Link is down
1	Link opening in progress
2	Link is established
3	The PPP client has been temporarily paused.

Contact customer support if an error code is displayed that is not on the above list.

Connection supervision failed.

The connection supervision has failed to connect to the configured URLs. The connection will be closed.

Modem reset

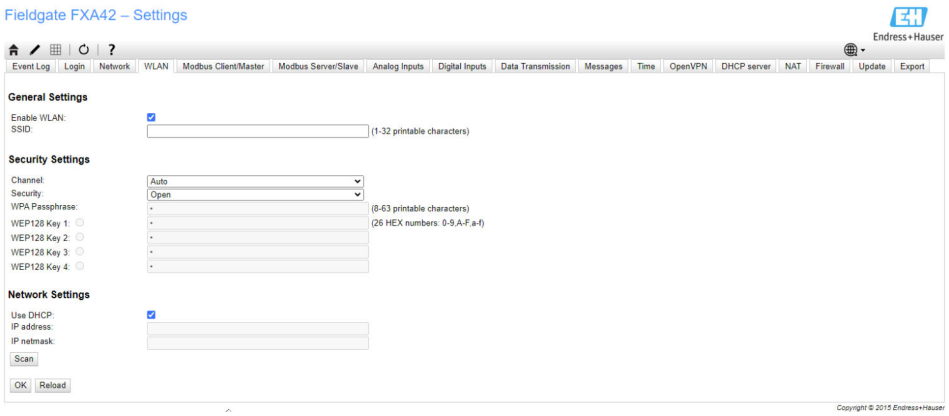
The cellular modem hardware has been reset.

Hanging! (state: <x>)

The cellular modem driver is in an invalid state.

8.4.5 WLAN

If the device has a WLAN interface, it can be activated and configured on this page.



Settings

The following table describes the available settings for the WLAN unit.

Settings	Description
Enable WLAN	Enables the module
SSID	Network name/identifier (0 to 30 printable characters) If no SSID is specified, the driver does not attempt to establish a connection.
Security	Select a security method: **Open**, **WEP128** or **WPA(2)-PSK** (recommended)
WPA Passphrase	The passphrase for WPA(2)-PSK can consist of 8 to 63 characters.
WEP128 Key1 to 4	If the WEP128 security mode is chosen, a valid WEP key (26 Hex characters) has to be entered in the selected key index field.
Use DHCP	If this option is selected, the module gets its IP configuration through DHCP.
IP address	IP address for the WLAN interface.
IP netmask	Netmask for the WLAN interface.

Only modify the WLAN settings via the Ethernet (hard-wired) connection, wherever possible! If the configuration is changed via the WLAN connection itself, this may cause the connection that is currently established to be lost after a device restart.

Wireless scanning

Press the *Scan* button to search for available wireless networks.

The scan takes about 20 seconds. Afterwards the wireless networks found are shown in a dialog.

Select the desired wireless network using the *Select* button or by double-clicking the corresponding entry. The settings of the selected wireless network are applied to the configuration page. Enter the WPA passphrase and the WEP key if necessary.

Event log messages

The following section describes the messages that the WLAN driver may log to the event log. All messages are prefixed with the text *WLAN Driver*.

Started

The WLAN unit driver has been started.

Running

The WLAN unit driver is now running.

Configured IP through DHCP

The WLAN unit driver has configured its IP address through the DHCP protocol.

Stopping driver

The WLAN unit driver is being stopped.

Stopped

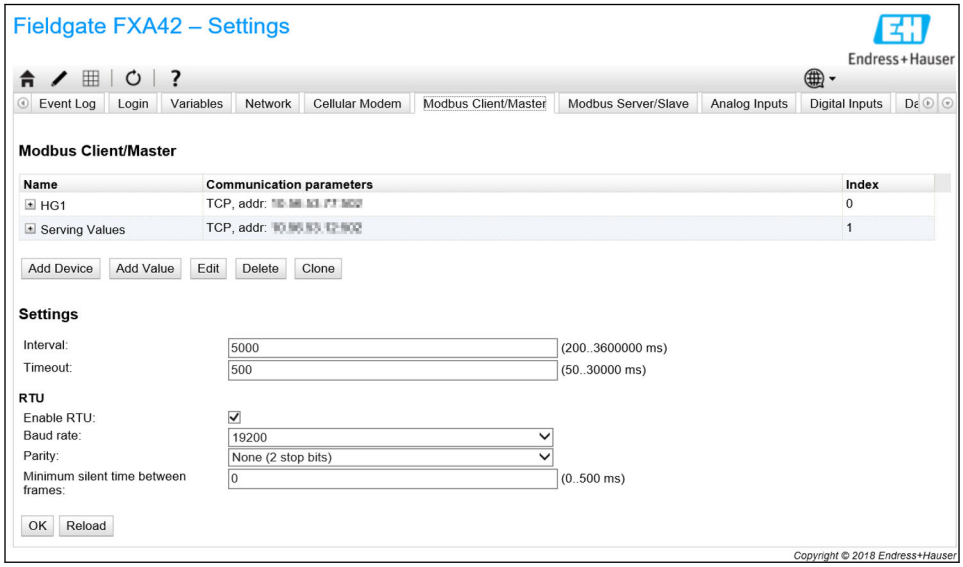
The WLAN unit driver has been stopped.

Connection indication

Message	Description
NOT CONNECTED	No specific indication.
ASSOCIATED	Success, unit is associated (infrastructure mode).
MGMT_ERROR	Internal protocol error occurred (the unit restarts).
MGMT_TIMEOUT	Internal protocol error occurred (the unit restarts).
BAD_PARAMETERS	Bad parameters specified by the executed API function.
SCAN_FAILURE	Scan failure occurred (the unit restarts).
SCAN_NOT_FOUND	Requested BSS was not found by scan.
JOIN_FAILURE	A join failure occurred.
JOIN_TIMEOUT	A join timeout occurred.
AUTH_FAILURE	Authentication error occurred.
DEAUTHENTICATED	Unit was deauthenticated by the access point.
ASSOC_FAILURE	Association failure occurred
DISASSOCIATED	Unit was disassociated by the access point.
WEP_PAIRKEY_FAULT	Setting of WEP pair key failed.
WEP_GROUPKEY_FAULT	Setting of WEP group key failed.
DISCONNECTED	Device is not associated.
TARGET_HUNG	The WLAN unit cannot be accessed by the host driver (the unit restarts).
KEEPALIVE_FAULT	The host driver has detected a keepalive check timeout (the unit restarts).

8.4.6 Modbus client/master

The Modbus client/master can be configured on this page.



Devices and values

The **Modbus Client/Master** list shows Modbus devices and their values. Devices and values (input or output) can be added, edited, deleted or cloned via the buttons below the list. For each device and value the list shows a name, the communication parameter and an index. The name can be freely defined and is shown on the portal, for example. The indexes are used internally to address the devices and their values.

When a device is added or edited, a dialog opens where the following parameters can be configured:

Parameter	Description
Name	The device's name.
Type	Select whether the device will be accessed via Modbus TCP or RTU. The Modbus RTU option is only available once Modbus RTU has been generally enabled.
Address	Only present for Modbus RTU devices Address of the device
IP address	Only present for Modbus TCP devices The device's IP address (e.g. 192.168.0.3)
Port	Only present for Modbus TCP devices The device's TCP port number - typically 502

When you add or edit a value, another dialog will appear. The following parameters can be configured here:

Parameter	Description
Name	The value's name.
Unit identifier	Only present for Modbus TCP servers. For Modbus TCP/RTU gateways this is the address of the RTU device to read from or write to.
Function	Modbus function code used to read or write the value. The function code also defines whether the value is interpreted as an input or output.
Start address	Register/coil address to start reading/writing from/to. Addresses start with 0.
Number	Number of registers/coils to read or write If more registers/coils are read or written than fit into the selected data type, the value will become an array. For example 2 registers would fit into one 32-bit unsigned integer value. The value would be scalar (no array). 4 registers would make up an array with 2 32-bit unsigned integer elements.
Data type	Data type of the value.
Swap words	Modbus transmits the two bytes of one register in network byte order (big endian). Thus for multi-register values, the registers are expected to be in the same order. However, some devices store multi-register values in the opposite order. This option can be used to correct the word order.

Value and device amount limits

Up to 32 devices and 256 values can be defined. As values can become arrays when reading and writing several registers or values, the following limit applies: The number of all scalar (non-array) values plus the size of all arrays must not exceed 512.

Settings

The following settings can be made in the fields below the live list:

Setting	Description
Interval	Defines the interval (in milliseconds) in which all Modbus values are read or written. If a warning message appears in the event log, the interval is too short to read or write all the values. Increase the interval if this occurs. Reading or writing a value may take twice the time specified for the timeout (see below), i.e. if the driver has to connect to a Modbus TCP device (first timeout) before reading or writing the value (second timeout).
Timeout	Defines the maximum time in milliseconds to wait for the reply from a device when reading or writing one of its values or when connecting to a Modbus TCP device.
Enable RTU	Enables Modbus-RTU
Baud rate	Defines the baud rate for Modbus RTU
Parity	Defines the parity (and stop bits) for Modbus RTU. Options: ▪ None (2 stop bits) ▪ Odd ▪ Even ▪ None (1 stop bit)
Minimum silent time between frames	Defines the minimum time for which there has to be silence on the bus between 2 frames. The Modbus RTU driver calculates the silence time depending on the baud rate. This setting can be used to increase the silent time. If the time you configure here is less than the calculated time, your setting will be ignored.

Event log messages

The following section describes the messages that the Modbus driver may log to the event log . All messages are prefixed with the text *Modbus driver*.

Connected to TCP device at <IP address>:<port>.

The driver successfully connected to the Modbus TCP server with the IP address and port indicated. This message will only be shown if the driver failed to connect to the same server before.

Read/wrote from/to TCP device at <IP address>:<port> (unit: <unit identifier>, function code: <function code>, address: <address>, quantity: <quantity>)

The driver has successfully read a value from the Modbus TCP server with the IP address and port indicated or written a value to the Modbus TCP server. This value is identified by the Modbus function code used, its address (starting from 0) and the quantity of registers or coils. This message will only be shown if the driver failed to read or write the same value before.

Read/wrote from/to RTU device <device address> (function code: <function code>, address: <value address>, quantity: <quantity>)

The driver has successfully read a value from the Modbus RTU slave with the address indicated or written a value to the Modbus RTU slave. This value is identified by the Modbus function code used, its address (starting from 0) and the quantity of registers or coils. This message will only be shown if the driver failed to read or write the same value before.

The interval has been violated.

The driver was still busy reading or writing slave/client values when a new cycle should have been started. Increase the interval.

Could not connect to TCP device at <IP address>:<port>. (Error code <code>).

The driver could not connect to the Modbus TCP server with the IP address and port indicated. The message also shows an error code:

Error code	Description
-2	Could not open TCP socket.
-3	Could not switch TCP socket to blocking mode.
-4	Unable to establish the TCP connection.
-5	Setting options on TCP socket failed.

Contact customer support if an error code is displayed that is not listed here.

Could not read/write from/to TCP device at <IP address>:<port> (unit: <unit idenfifier>, function code: <function code>, address: <address>, quantity: <quantity>, result code: <result code>, error code: <error code>, exception code: <exception code>)

The driver could not read a value from the Modbus TCP server with the IP address and port indicated or write a value to the Modbus TCP server. This value is identified by the Modbus function code used, its address (starting from 0) and the quantity of registers or coils. The message also shows a result code, an error code from the TCP/IP stack and a Modbus exception code. Documentation on Modbus exception codes is provided in the Modbus application protocol specification. The following table shows the possible result codes:

Result code	Description
-1	Waiting for server response timed out. Either the server is not available or you should increase the timeout.
-2	Received invalid packet (protocol error).
-5	TCP/IP error

Contact customer support if an error code is displayed that is not listed here.

Read illegal floating point value from TCP device at <IP address>:<port> (unit: <unit idenfifier>, function code: <function code>, address: <address>, quantity: <quantity>)

The driver read an illegal floating point value from the Modbus TCP server with the IP address and port indicated. This value is identified by the Modbus function code used to read it, its address (starting from 0) and the quantity of registers or coils.

Could not read/write from/to RTU device <device address> (function code: <function code>, address: <value address>, quantity: <quantity>, result code: <result code>, exception code: <exception code>)

The driver failed to read/write a value from/to the Modbus RTU slave with the address indicated. The corresponding value is identified by the Modbus function code used to read/write it, its address (starting from 0) and the quantity of registers/coils. The message also shows a result code and a Modbus exception code. For documentation on Modbus exception codes please refer to the Modbus application protocol specification. The following table shows the possible result codes:

Result code	Description
-1	Waiting for slave response timed out. Either the slave is not available or you should increase the timeout.
-2	Received invalid packet (checksum error).
-3	Sending request failed.

Contact customer support if an event code is displayed that is not listed here.

Read illegal floating point value from RTU device <device address> (function code: <function code>, address: <value address>, quantity: <quantity>)

The driver read an illegal floating point value from the Modbus RTU slave with the IP address indicated. This value is identified by the Modbus function code used to read it, its address (starting from 0) and the quantity of registers or coils.

Portal communication error <error code>

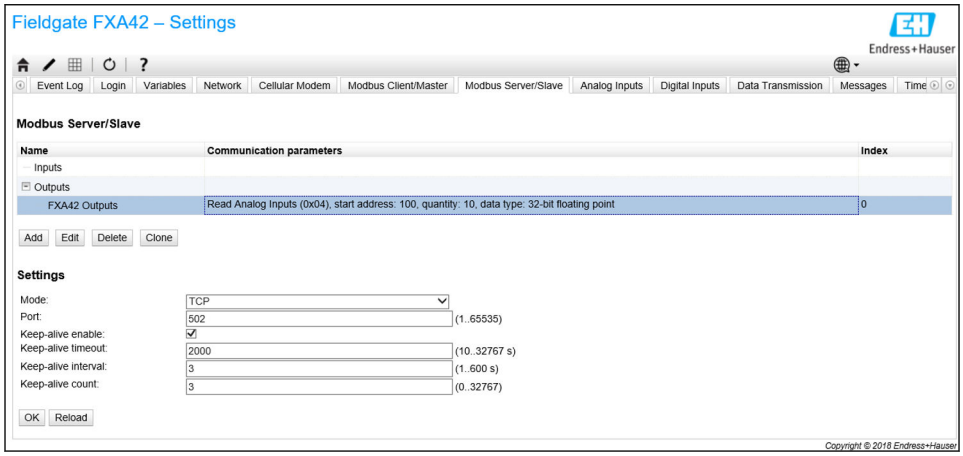
A general error has occurred while exchanging data with the port. Possible error codes:

Error code	Description
-10	Out of memory
-12	Internal data queue overflow: data was produced faster than it could be processed.

Contact customer support if an error code is displayed that is not listed here.

8.4.7 Modbus server/slave

The Modbus server/slave can be configured on this page.



Values

This page displays a list of Modbus values. Settings (input or output) can be added, edited, deleted or cloned via the buttons below the list. For each value the list shows a name, the communication parameters and an index. The name can be freely defined and is shown on the portal, for example. The indexes are used internally to address the values.

When you add or edit a value, a dialog will appear. The following parameters can be configured here:

Parameter	Description
Name	The value's name
Function	Modbus function code used to read or write the value. The function code also defines whether the value is interpreted as an input or output.
Start address	Register or coil address to start reading or writing. Addresses start with 0.

Parameter	Description
Number	Number of registers or coils to read or write If more registers or coils are read or written than fit into the selected data type, the value will become an array. For more information on the number of registers or coils, see the **Limits** section.
Data type	Data type of the value

Limits

Up to 128 values can be defined. As values can become arrays when reading and writing several registers or coils, the following limit applies: The number of all scalar (non-array) values plus the size of all arrays must not exceed 512.

Settings

A number of general settings can be configured using the fields below the value list:

Settings	Description
Mode	Defines whether to operate the device as a Modbus RTU slave or a Modbus TCP server. Depending on the particular setting, 2 different groups of additional settings are available.

TCP settings

Settings	Description
Port	TCP port number where the Modbus TCP server will be listening. The number of the port is generally 502.
Keep-alive enable	Enables the TCP keep-alive mechanism for connections from clients. The keep-alive mechanism is used to detect inactive connections. If an inactive connection is detected, resources used by this connection can be released.
Keep-alive timeout	Idle time in seconds after which the first keep-alive probe will be sent.
Keep-alive interval	Interval in seconds in which keep-alive probes will be sent.
Keep-alive count	Number of keep-alive probes that will be sent before closing the connection.

RTU settings

Settings	Description
Address	RTU slave's address
Baud rate	Defines the baud rate for Modbus RTU
Parity	Defines the parity (and number of stop bits) for Modbus RTU. Options: ▪ None (2 stop bits) ▪ Odd ▪ Even

Event log messages

The following section describes the messages that the Modbus slave driver may log to the event log. All messages are prefixed with the text *Modbus Slv driver*.

Portal communication error <error code>

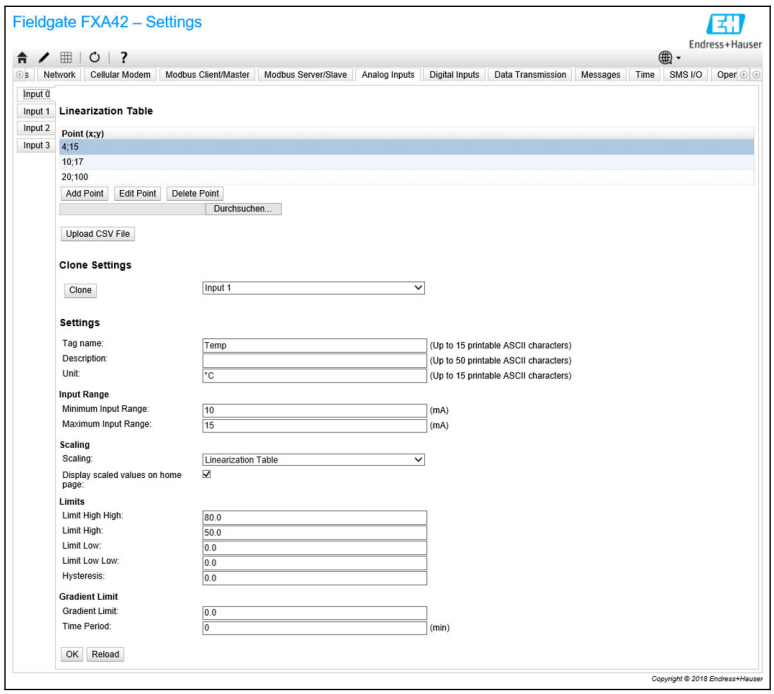
A general error has occurred while exchanging data with the port. Possible error codes:

Error code	Description
-10	Out of memory
-12	Internal data queue overflow: data was produced faster than it could be processed.

Contact customer support if an error code is displayed that is not listed here.

8.4.8 Analog Inputs

The analog inputs of the device can be configured on this page. On the left side of the page the user may select one of the 4 different inputs by clicking the corresponding tab. The settings for each of the 4 inputs are identical.



Linearization table

The user may select to scale the input values via the use of a linearization table. Value pairs (x,y) are entered for this. A maximum of 64 value pairs are possible. Here, the x value corresponds to the value in the scaled unit and the y value corresponds to the measured value in milliampere (mA). Each time a value pair is added or edited, the table is automatically sorted, based on the x values.

Instead of manually adding the value pairs for the linearization table, it is also possible to upload a .csv file containing all the (x,y) value pairs. Once the .csv file is validated and parsed, the table is automatically filled with the given values. A valid .csv file should use the dot "." character as the decimal point and the comma "," character as the (x,y) value separator.

Clone settings

In order to make the configuration easier, the user may copy the current settings of one input to another one. To do this, the user should first select the input from which the settings are to be copied. Once you click the **Clone** button, all the settings from the selected input are copied to the configuration page currently visible.

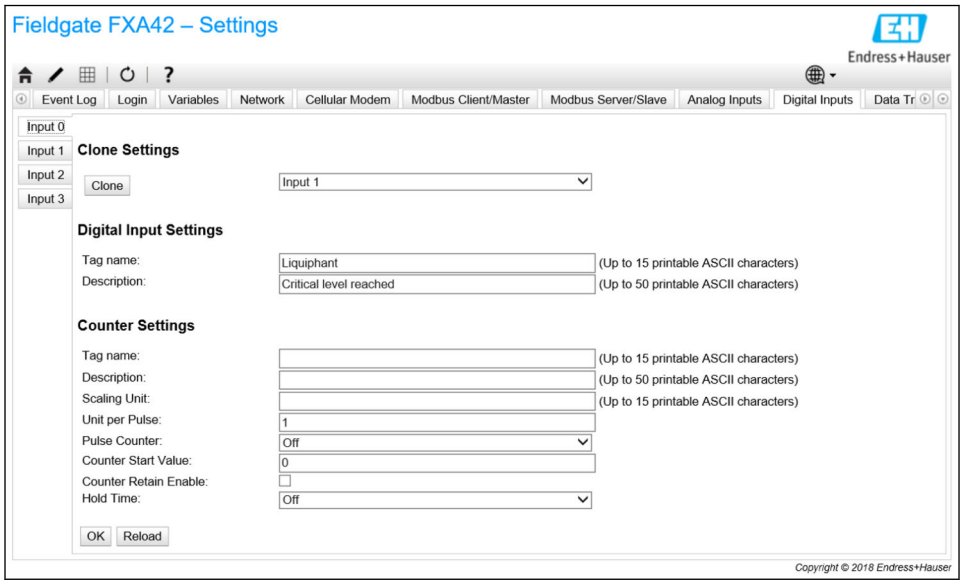
Analog input settings

In this section the user may configure the settings for each analog input. The following settings are available:

Settings	Description
Tag name	The label name of the input
Description	A text describing the input's function
Unit	The input's measurement unit
Minimum Input Range	The input's minimum current value, measured in milliampere
Maximum Input Range	The input's maximum current value, measured in milliampere
Scaling	The scaling may be calculated either by using a Min/Max value pair, or by providing a linearization table.
Minimum Scale	Minimum scaled value This field is enabled when the **Range** option has been selected in the Scaling field.
Maximum Scale	Maximum scaled value This field is enabled when the **Range** option has been selected in the Scaling field.
Display scaled values on home page	This check box defines whether the values on the home page and in the editor are to be displayed in milliampere or in the scaled unit.
Limit High High	The input's **High High** limit, measured in the scaled unit
Limit High	The input's **High** limit, measured in the scaled unit
Limit Low	The input's **Low** limit, measured in the scaled unit
Limit Low Low	The input's **Low Low** limit, measured in the scaled unit
Hysteresis	This value defines an offset value below the **High** and **High High** limits and above the **Low** and **Low Low** limits. The configured offset delays the resetting of an alarm. The value is measured in the scaled unit.
Gradient Limit	The input's gradient limit, measured in the scaled unit. This limit value triggers an alarm if the input's value is above this limit for a certain time.
Time Period	The time after which a Gradient Limit Alarm should be triggered.

8.4.9 Digital Inputs

The digital inputs of the Fieldgate FXA42 can be configured on this page. On the left side of the page the user may select one of the 4 different inputs by clicking the corresponding tab. The settings for each of the 4 inputs are identical.



Clone Settings

In order to make the configuration easier, the user may copy the current settings of one input to another one. To do this, the user should first select the input from which the settings are to be copied. Once you click the **Clone** button, all the settings from the selected input are copied to the configuration page currently visible.

Digital Input Settings

In this section the user may configure the settings for each digital input. The following settings are available:

Settings	Description
Tag name	The label name of the input
Description	A text describing the input's function

Counter Settings

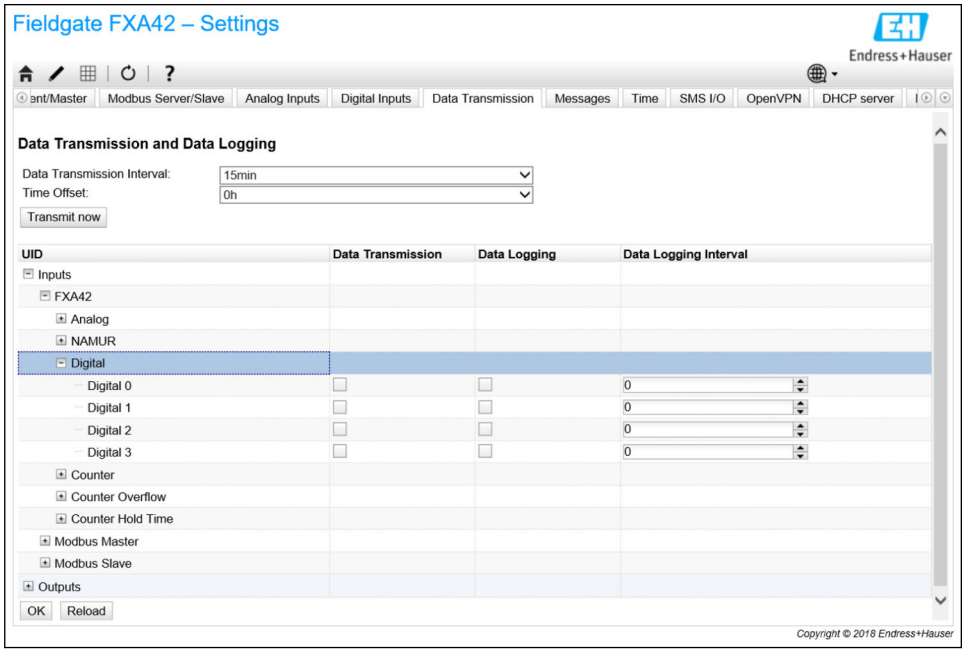
In this section the user may configure the settings for each counter. The following settings are available:

Settings	Description
Tag name	The label name of the counter
Description	A text describing the counter's function
Scaled Unit	Unit used by the counter
Units per Pulse	Scaling factor of the counter
Pulse Counter	This setting defines the operational mode of the counter. The mode options are turned off, counting upwards, or counting downwards.
Counter Start Value	This is the value that the counter has each time it is reset.
Counter Retain Enable	The check box determines whether the counter value is saved and reused when the device is restarted or whether the counter is set to ZERO.
Hold Time	The hold time defines the minimum time that must elapse between 2 consecutive counting events so that they are registered.

8.4.10 Data Transmission and Data Logging

This page is used to configure which data will be transmitted via FIS or the other communication methods, and which data should be logged internally. It is also possible to set time intervals at which the data should be transmitted or logged. Data is internally logged or recorded. Recorded data is communicated via all the enabled communication methods.

Buffering is only possible when the SD card is inserted. If no SD card has been inserted, only the current measured value is transmitted.



The following settings apply to all I/Os for which data transmission is enabled:
- Data transmission interval: The interval in which the recorded data is to be transmitted. Example: A value of 2 hours transmits the data at 00:00, 02:00, 04:00, 06:00 etc.
- Time offset: An offset that is added to the data transmission interval. Example: If an interval of 2 hours and an offset of 1 hour are set, data will be transmitted at 01:00, 03:00, 05:00, 07:00 etc. Caution: This value may not be greater than the transmission interval.
- Transmit now: Transmit all recorded data now.

All the inputs and outputs of the device are visible when you click ⊞. Settings:
- Data transmission: Enables the data transmission for the selected I/O.
- Data logging: Enables the data logging for the selected I/O.
- Data logging interval: The interval (in minutes) in which data is to be logged and recorded.

Event log messages

Messages relating to the data transmission and data logging functionalities are created by the I/O Task of the device.

Sent FIS data message successfully

A FIS data message was sent.

Error on parsing FIS data message

XML error when generating a FIS data message. Contact customer support.

FIS: Recording data

FIS data is being recorded.

FIS event message transmitted successfully

A FIS event message was sent.

FIS: Recording event

An event has been recorded.

HTTP error <HTTP-Error> occurred while sending FIS event message

HTTP communication error with the FIS server.

HTTP connection error occurred while sending FIS event message

An error occurred while trying to transmit an event message to the FIS server. Check the device's connection status.

HTTP connection error occurred while sending FIS data message

An error occurred while trying to transmit a data message to the FIS server. Check the device's connection status.

FIS data message transmitted successfully

The data message was correctly transmitted to the FIS server.

HTTP error <HTTP-Error> occurred while sending FIS data message

HTTP communication error with the FIS server.

Invalid FIS authentication

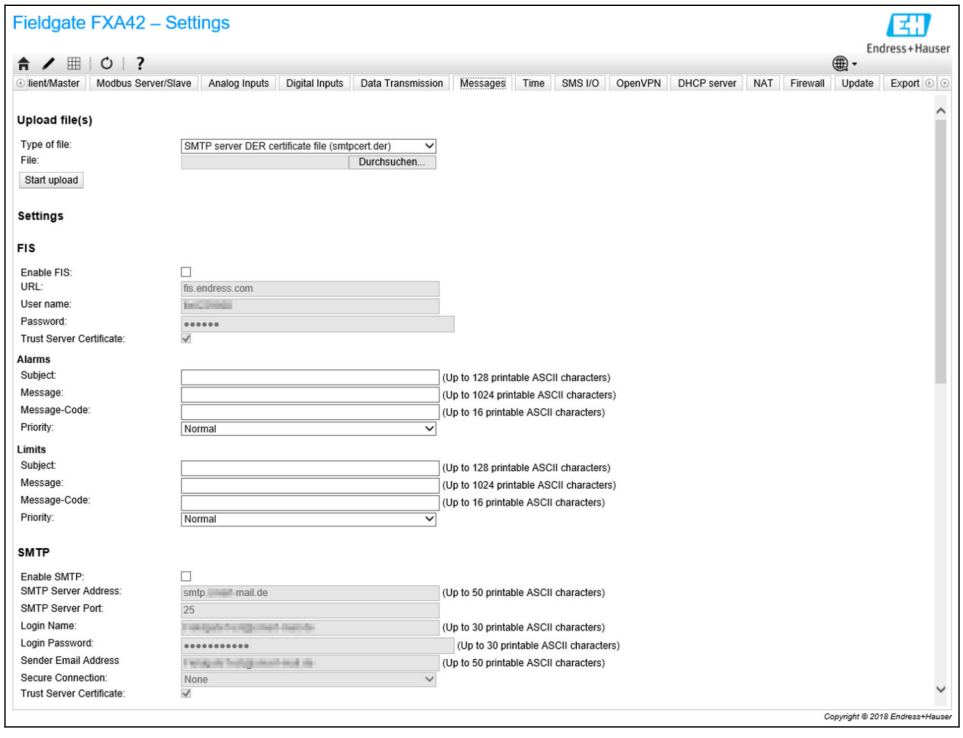
The device's access data to the FIS are not correct.

Logging data

The device is logging data.

8.4.11 Messages

The various communication options for the device can be configured via this page.



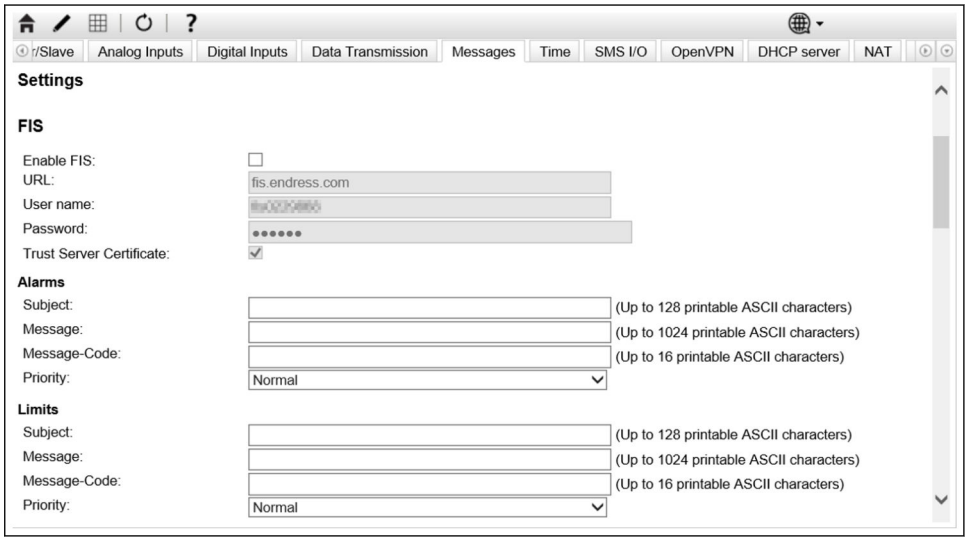
Upload file(s)

This section can be used to upload certificate files for encrypted SMTP and FTP connections. DER certificates can be used. The DER format is a binary certificate format. The file names of the DER certificate files mostly end with .cer or .der.

1. From the drop-down list select the file type to be uploaded.
2. Select the file in the local file system and click the **Start upload** button.

FIS

The access data for the FIS portal can be enabled and configured on this page. The values to enter here are the FIS server URL, the user name and the corresponding password. The device can register itself on the server with the default settings. If the registration fails, consult the FIS portal documentation.



If the registration fails, the device will make another attempt after <*T*> minutes. <*T*> is the next number of the Fibonacci sequence starting from 1. The maximum number of minutes between 2 attempts is 1440.

Configuration exchange

The device is able to transmit its current configuration to the FIS in the form of a *.cup package. The transmission takes place after every reboot of the device that was not caused by a remote configuration change by the FIS.

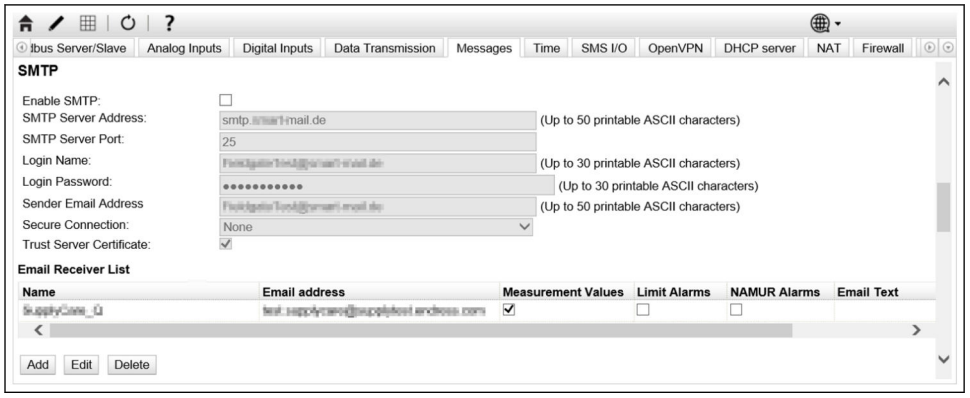
The FIS server is able to remotely change the configuration of the device. The FIS server can command the device to download a new configuration and apply it. After the configuration has been downloaded the device will reboot and register itself with the new configuration version.

In this section the user may configure the settings for FIS Alarms and Limits messages. The following settings are available for each of the two types of messages:

Settings	Description
Subject	Message subject
Message	Message text
Message-Code	Message code
Priority	Message priority

SMTP

In this section the user may configure the settings for SMTP (e-mail) communication.



The following settings are available:

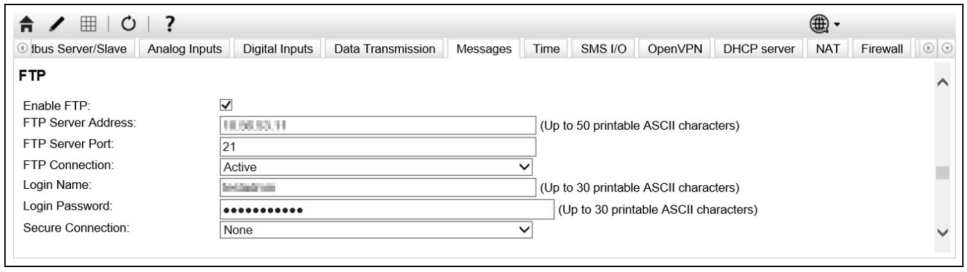
Settings	Description
Enable SMTP	Enable/disable the SMTP function
SMTP Server Address	The address of the remote SMTP server It may be either a host name or an IP string.
SMTP Server Port	The port of the SMTP server.
Login Name	This is the user name that should be used when connecting to the SMTP server.
Login Password	This is the password that should be used when connecting to the SMTP server.
Sender Email Address	The e-mail address of the sender
Secure Connection	For activating TLS encryption for the SMTP communication.
Trust Server Certificate	The server certificate is not validated.

Email Receiver List

Up to five different e-mail recipients can be defined. An individual text can be defined for each recipient. In addition, the user can specify what type of information the recipient should receive (measured values, limit alarms, NAMUR alarms).

FTP

The FTP settings are made in this section.



The following settings are available:

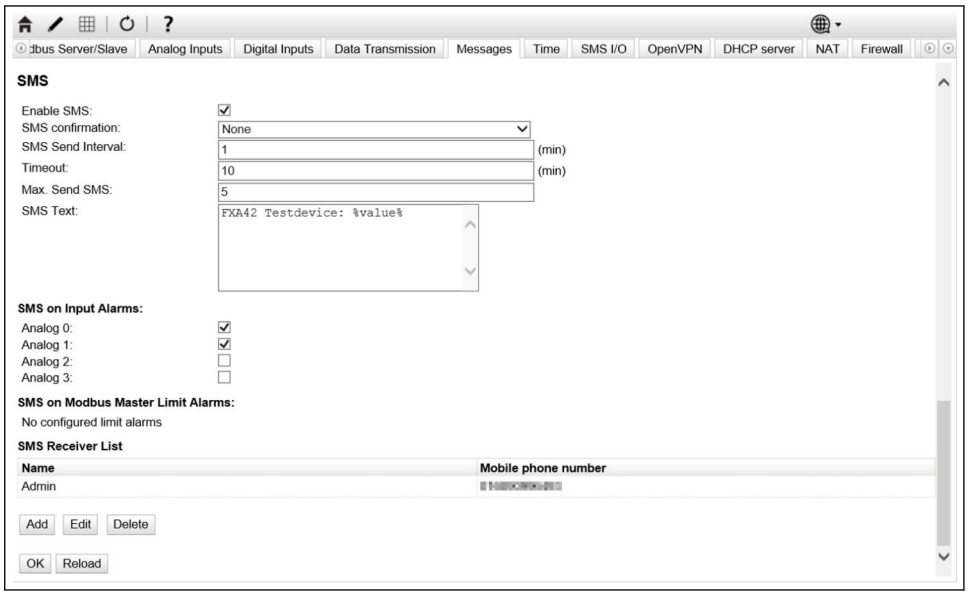
Text	Description
Enable FTP	Enable/disable the FTP function
FTP Server Address	The address of the remote FTP server It may be either a host name or an IP string.

Text	Description
FTP Server Port	The port of the FTP server.
FTP Connection	Set the FTP connection to be active or passive.
Login Name	This is the user name that should be used when connecting to the FTP server.
Login Password	This is the password that should be used when connecting to the FTP server.
Secure Connection	For activating TLS encryption for the FTP communication.

SMS

In this section the user may configure the settings for the transmission of SMS messages (alarm events).

Note that the SMS function must have been agreed when selecting the contract in order to use this function. The mobile telecommunications contract for the device must support this function.



The following settings are available:

Settings	Description
Enable SMS	Enable/disable the SMS function
SMS confirmation	This setting defines the way that the Alarm SMS messages should be acknowledged so that the SMS escalation stops. There are 3 possible SMS confirmation options: ▪ None: No acknowledgment is expected for stopping the SMS escalation. ▪ Automatic: As soon as an SMS delivery confirmation arrives, the SMS escalation is stopped. ▪ Manual: The SMS escalation is stopped when one of the recipients sends an empty SMS to the device.
SMS Send Interval	Time to wait before attempting to resend an SMS in the event of a send error. Measured in minutes.
Timeout	Time to wait before sending the SMS to the next recipient of the escalation. Measured in minutes.
Max. Send SMS	Maximum number of SMS send retries in the event of a send error.

SMS Receiver List

Up to 5 different SMS recipients can be defined. The name and telephone number of each recipient must be provided. The SMS text that is to be sent is generated automatically. It contains the information on the analog input for which "by alarm notification" was selected on the Data Transmission Configuration page.

The phone number for the SMS recipients must contain the country code, prefixed with the plus (+) sign, e.g. +49123456789. Separating characters are not allowed.

Event log messages

Messages relating to the Messages tab are created by the I/O Task of the device.

Sending data Email to <name>, address: <name>

A data e-mail has been sent to the recipient indicated.

Sending limit Email to <email>, address: <address>

A limit e-mail has been sent to the recipient indicated.

Sending alarm Email to <email>, address: <address>

An alarm e-mail has been sent to the recipient indicated.

Sent data Email message successfully

A data e-mail has been sent successfully.

Could not send data Email

A data e-mail could not be transmitted.

Email: No data recorded

No saved data to transmit via e-mail.

Email: Recording data

E-mail data has been recorded.

Email: Recording event

An event e-mail has been recorded.

FTP: Recording data

FTP data has been recorded.

Could not send file to FTP server

An FTP message could not be sent to the server.

Sent measurements file to FTP server

An FTP message was sent to the server.

Messages relating to the FIS registration and configuration are created by the I/O Task of the device.

Sending FIS registration message

A registration message is being transmitted to the FIS server.

Sending configuration to FIS

A configuration message is being transmitted to the FIS server.

Configuration successful

The configuration on the FIS server was successful.

FIS configuration version: <Version>

The configuration version on the FIS server.

Invalid FIS authentication data. Trying again in <T> minutes.

During this FIS registration attempt a wrong user name/password was used.

HTTP error <HTTP-Error> occurred while sending FIS registration message. Trying again in <T> minutes.

HTTP communication error with the FIS server during the registration attempt.

HTTP connection error occurred while sending FIS registration message. Trying again in <T> minutes.

An error occurred during the registration attempt. Check the device's connection status.

FIS registration successful

Registration attempt was successful. Device is now registered on the FIS.

New configuration available: <Version>

A new configuration is available on the FIS server. The device will try to download and apply this configuration.

Could not apply FIS configuration, update in progress.

The device could not be configured via FIS. An update is in progress.

FIS configuration version: <Version>

A new configuration is available on the FIS server. The device will not try to download and apply this configuration.

Downloading new configuration from FIS

The device is downloading a configuration from the FIS.

Could not apply configuration

The device could not be configured via FIS.

Re-booting due to FIS command

The device is rebooted due to a FIS command.

Re-registration due to FIS command

The device will re-register itself on the FIS due to a FIS command.

Update due to FIS command

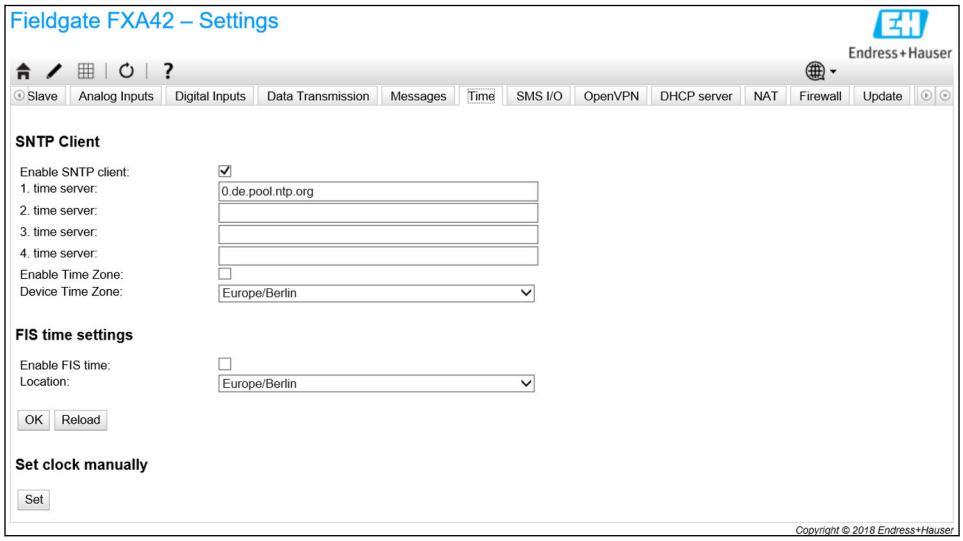
The device will update itself from the configured URL due to a FIS command.

Time changed from FIS

The current time settings have been set by the FIS.

8.4.12 Time

The system time can be configured on this page.



It is also possible to configure whether and how the system time should be synchronized via the Simple Network Time Protocol (SNTP) or FIS.

If the FIS is activated on the **Messages** page, the system uses the FIS communication to set the time. The time then cannot be set in the **Time** tab.

The SNTP client can be enabled and configured in the first section. If the client is enabled, the specified time servers will be contacted several times a day to determine the current time and date. Then the system clock will be updated accordingly.

Up to 4 time servers can be specified. These servers will be queried one after the other until one of them answers.

The server names can be given either as host names (e.g. ntp.company.org) or as IP addresses (e.g. 192.168.0.23).

Contacting the time servers produces data traffic.

FIS time settings

The FIS time settings can be enabled and configured here. If FIS time is enabled, the device will request the current time information from the FIS server on each registration. The device is registered at least once daily.

The device's location and timezone can be selected from the drop-down list.

Set clock manually

The system time can be set manually here. Click the **Set** button to set the system time based on the current time on the connected PC.

Event log messages

The following section describes the messages that the system time manager and the SNTP client may log to the event log. All messages are prefixed with the text *System Time Manager:* or *SNTP Client:*

Running

The system time manager is now running.

System clock updated via SNTP

The system clock (and if available the real-time clock) has/have just been updated with the time obtained via SNTP.

System clock updated from RTC

The system clock has just been updated with the time from the real-time clock.

Could not get exclusive access to clock(s).

The system time manager could not get exclusive access to the system clock and (if available) the real-time clock. Thus the system clock could not be set or the real-time clock could not be read.

Daylight saving time rules will be used up within the next two years.

The firmware of the device includes daylight saving time rules for a limited time period. New rules will be added with new firmware versions. This message indicates that the rules will be used up within the next 2 years. Run a firmware update to get new rules.

SNTP client error: <message>

The SNTP client has returned the error message shown.

RTC not available

The device should feature a real-time clock, but it cannot be accessed.

Could not write to RTC: <message>

Failed to set the real-time clock. The message also shows an error message returned by the real-time clock driver.

Could not read from RTC: <message>

The real-time clock could not be read. The message also shows an error message returned by the real-time clock driver.

Could not read daylight saving time file.

The daylight saving time file for this time zone is missing or corrupted.

No daylight saving time rule found for the current time.

No daylight saving time rule could be found for the current time. This means that either the daylight saving time rules are outdated or that the device's time is set incorrectly.

DNS error (<error code>) for server <server name/IP>

The SNTP client could not determine the IP address of the server with the name indicated. The message also shows the error code returned by the TCP/IP stack.

Could not open socket for server <server name/IP>

The SNTP client could not open a UDP socket in order to contact the time server with the name or IP address indicated.

Could not send to server <server name/IP>

The SNTP client could not send a request to the time server with the name or IP address indicated.

Failed to receive reply from server <server name/IP>

The SNTP client could not receive a reply from the time server with the name or IP address indicated.

Unexpected packet format from server <server name/IP>

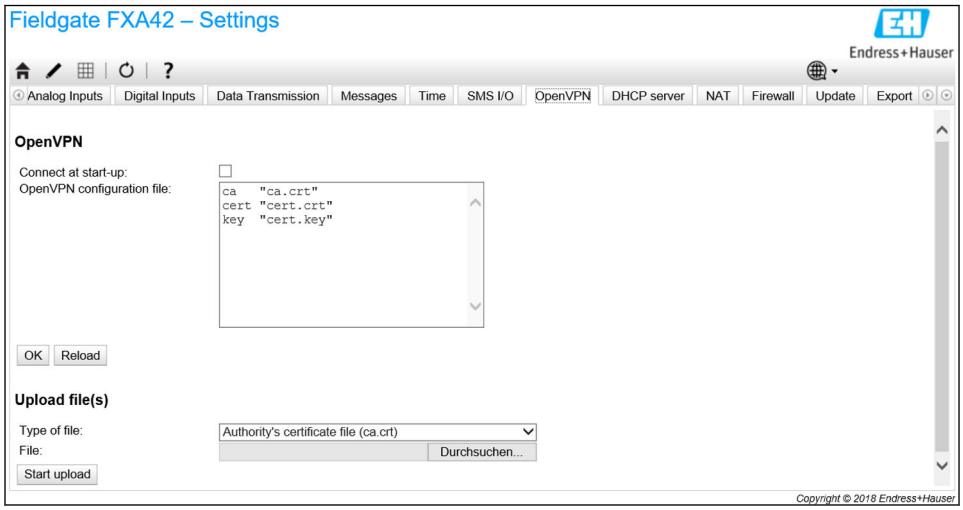
The SNTP client received an invalid reply from the time server with the name or IP address indicated.

Timestamps not plausible from server <server name/IP>

The SNTP client received a reply with implausible timestamps from the time server with the name or IP address indicated.

8.4.13 OpenVPN

The firmware of the device includes OpenVPN. The device can be integrated into a virtual private network with OpenVPN.



There are 2 ways to start OpenVPN. OpenVPN can either be executed automatically at system start-up or be started manually via the portal. The device has a portal node at the address. OpenVPN starts if the value of this node is set to 1. OpenVPN can be terminated by resetting the value to 0.

The large text input field can be used to edit the OpenVPN configuration file. More detailed information is provided in the OpenVPN documentation. Certificate files can be referenced without any path prefix.

Changes to the OpenVPN configuration may take effect before the device is restarted if the OpenVPN connection is (re-)established. Reboot the device shortly after changing the configuration in order to ensure consistency.

Upload file(s)

1. From the drop-down box select the file to be uploaded.
2. Select the file in the local file system and click the *Start upload* button.

The drop-down list displays the file names which can be used to reference the uploaded files in the configuration (see above).

If the device features an external storage medium, it is possible that the files will be temporarily stored on it. The files will be deleted later. It may be possible to restore them, however. For this reason, always store the external storage medium in a safe place.

Event log messages

The following section describes the messages that the OpenVPN driver may log to the event log. All messages are prefixed with the text *OpenVPN*: Messages from OpenVPN itself are also displayed.

The following list is not complete.

More detailed information is provided in the OpenVPN documentation.

Driver has been started.

The OpenVPN driver has been successfully started.

Driver has been stopped.

The OpenVPN driver has been successfully stopped.

Driver stopped.

The OpenVPN driver has exited.

Connection established.

An OpenVPN connection has been established.

Connection closed.

An OpenVPN connection has been closed.

Authority's certificate uploaded.

The certification authority's certificate file (*ca.crt*) has been successfully uploaded.

Certificate uploaded.

The certificate file (*cet.crt*) has been successfully uploaded.

Private key uploaded.

The private key file (*cert.key*) has been successfully uploaded.

User and password file uploaded.

The user and password file (*userpass.txt*) has been successfully uploaded.

Diffie-Hellman file uploaded.

The Diffie-Hellman file (*dh.pem*) has been successfully uploaded.

Could not start driver.

The OpenVPN driver could not be started.

Could not stop driver.

The OpenVPN driver could not be stopped.

Driver stopped unexpectedly.

The OpenVPN driver has stopped unexpectedly. This can happen, for example, if the configuration is invalid. Pay attention to error messages from the OpenVPN driver.

Upload of authority's certificate failed.

The certification authority's certificate file (*ca.crt*) could not be uploaded.

Upload of certificate failed.

The certificate file (*cert.crt*) could not be uploaded.

Upload of private key failed.

The private key file (*cert.key*) could not be uploaded.

Upload of user and password file failed.

The user and password file (*userpass.txt*) could not be uploaded.

Upload of Diffie-Hellman file failed.

The Diffie-Hellman file (*dh.pem*) could not be uploaded.

Open-source software

The following open-source software has been used to implement the OpenVPN functionality:

LZO

The LZO compression library is used in OpenVPN.

LZO is copyright © Markus F.X.J. Oberhumer.

Project website: www.oberhumer.com/opensource/lzo

License: GPL

OpenSSL

OpenSSL is used in OpenVPN.

Project website: www.openssl.org

License: OpenSSL-Lizenz

OpenVPN

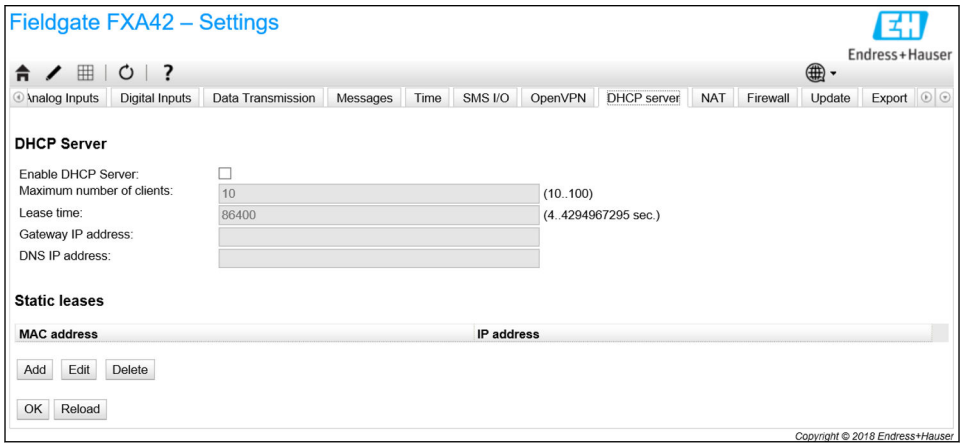
"OpenVPN" is a trademark of OpenVPN Technologies, Inc.

Project website: openvpn.net

License: OpenVPN licence

8.4.14 DHCP server

The device's firmware features a Dynamic Host Configuration Protocol (DHCP) server which can be enabled and configured on this page.



The following parameters must be configured for the DHCP server:
- **Maximum number of clients**: Maximum number of clients to be served The maximum number of clients is 100, including static mappings.
- **Lease time**: Lease time
- **Gateway IP address**: IP address of gateway for IP communication in other networks
- **DNS IP address**: IP address of the dynamic name server in the network for local name resolution

The server will lease IP addresses from the particular network (except for its own IP address). In addition, it is possible to specify a gateway IP address and a DNS IP address that are also distributed.

Static leases

Up to 10 static leases can be configured in this section. A static lease will ensure that a client with a specific MAC address will be given a predefined IP address and that this IP address is not leased to another client. The MAC address of the client must be specified without any delimiters (e.g. 003056A1DB30).

Event log messages

The following section describes the messages that the DHCP server may log to the event log. The messages are prefixed with the text *DHCP server*:

Running

The DHCP server has been successfully started.

Added static lease IP=<x>, MAC=<y>

A static lease has been added. The message also shows the IP and MAC address.

Discover message received, CI=<x>, MAC=<y>

A DHCP discover message was received from a client. The message also shows the client identifier as a hex string and the client's MAC address.

Request message received, CI=<x>, MAC=<y>

A DHCP request message was received from a client. The message also shows the client identifier as a hex string and the client's MAC address.

Leased IP=<x>, Leasing Time=<y>, Index=<z>

The IP address indicated has been leased to the client. The message also shows the leasing time in seconds and the internal leasing table index.

Release message received, CI=<x>, MAC=<y>

A DHCP release message was received from a client. The message also shows the client identifier as a hex string and the client's MAC address.

Release IP=<x>, Index=<y>

The IP address indicated has been released. The message also shows the internal leasing table index.

Network interface not configured

The network interface that the DHCP server is to use does not have a valid IP configuration.

Failed to send response message, error <x>

A DHCP response message could not be sent. The message also shows the error code returned by the TCP/IP stack.

No more client addresses available

A client's request could be not served because all the available addresses are already leased to or reserved for other clients.

Receive Error <x>

No DHCP message could be received. The message also shows the error code returned by the TCP/IP stack.

Received malformed message

A malformed DHCP message was received from a client.

No interface found for given IP address

The DHCP server could not find a network interface for the configured IP address at start-up.

Open socket failed

The DHCP server could not open a UDP socket at start-up.

Bind socket failed

The DHCP server could not bind its UDP socket to the designated port at start-up.

Only <x> clients possible due to netmask setting

The configured netmask allows fewer IP addresses than configured.

Failed to allocate client data structure

The DHCP client failed to allocate memory for its internal leasing table at start-up.

Adding static lease IP=<x> failed, IP address is in use

A static lease could not be added because the IP address indicated is already in use. The message also shows the IP address of the static lease that should be added.

Adding static lease IP=<x> failed, no free slot

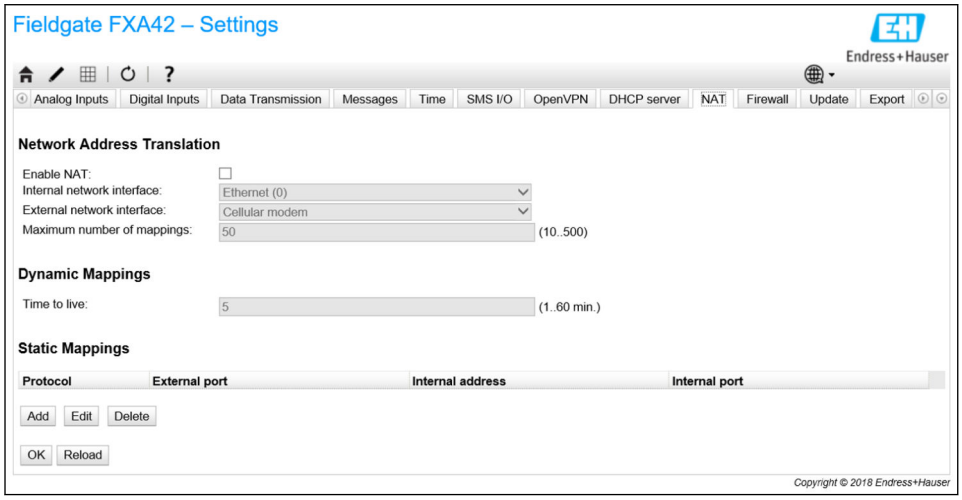
A static lease could not be added because there was no free space in the internal leasing table. The message also shows the IP address of the static lease that should be added.

Adding static lease IP=<x> failed, wrong IP address

A static lease could not be added because the IP address indicated did not match the network address. The message also shows the IP address of the static lease that should be added.

8.4.15 Network address translation

The firmware of the device is able to perform network and port address translation (aka NAT/PAT) in order to route traffic between a local (internal) and a global (external) network. This feature can be used, for example, to give another device in the local area network access to the gateway's cellular modem Internet connection (global network). The device must be connected to the Ethernet interface of the Fieldgate FXA42 for this purpose.



The following operations can be performed here:

- **Enable NAT**: Activate NAT service
- **Internal/External network interface**: Configure internal and external network interface
- **Maximum number of mappings**: Configure maximum number of mappings. Maximum number of mappings means incoming and outgoing connections that can be routed.

IP forwarding is implicitly enabled because it is needed in order to use the NAT function. If NAT is later disabled, IP forwarding will not be automatically disabled. IP forwarding can be disabled in the network settings.

Dynamic Mappings

Dynamic mapping is used to enable devices from the local area network to access the global network. Requests from the local area network will be given the global IP address of the Fieldgate FXA42 and the replies will be routed to the respective local device.

You have to configure the validity period of the dynamic mappings in minutes (time to live).

Static Mappings

Static mappings are used to make a local device's services accessible from the global network under the global IP address of the Fieldgate FXA42. Up to 10 static mappings can be configured. You have to configure the following options for each mapping:

Option	Description
Protocol	TCP or UDP
External port	The port of the Fieldgate FXA42 at which the service should be reachable from the global network.
Internal address	The IP address of the device in the local area network whose service should be reachable from the global network.
Internal port	The port number at which the service is available on the device in the local area network

Event log messages

The following section describes the messages that the NAT service unit may log to the event log. The messages are prefixed with the text *NAT service*:

The NAT service also implements the firewall service, which is why there are also some messages related to the **Firewall** function.

Running

The NAT service unit has been successfully started.

<x> static mapping(s) read from configuration

The static mapping entries have been successfully read from the configuration. The message also shows the number of static mappings read.

No free mapping entry available for incoming connection from internal interface

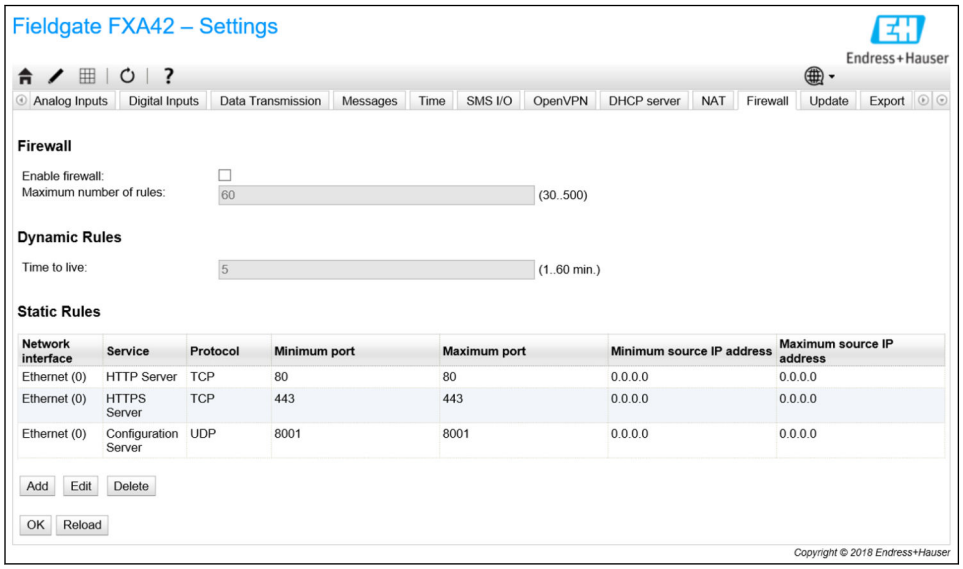
A client from the internal network tried to open a connection through the NAT service unit but there was no free entry in the mapping table. Therefore the connection could not be established. Increase the maximum number of mappings if possible.

No free firewall rule entry available for outgoing connection

A new dynamic rule has to be added to the firewall to allow an outgoing connection to be established. However, there was no free entry in the internal rules table. Therefore the connection could not be established. Increase the maximum number of rules if possible.

8.4.16 Firewall

The device features a firewall which improves the system's security by analyzing network traffic and blocking disallowed traffic.



The firewall of the device has a blocking policy. This means that while outgoing connections are generally allowed, incoming connections will be generally blocked. Only specific incoming connections are allowed if there is a rule allowing the connection.

The firewall can be enabled and the maximum number of rules configured on the **Firewall** page. This determines the number of incoming and outgoing connections that can be handled simultaneously.

When enabling the firewall, always make sure that a number of static rules are defined that allow to access the web server. This is important to be able to disable the firewall if necessary. If the firewall is enabled without any appropriate rules, it will not be possible to access the device in any way. If this occurs, the device must be reset to the factory settings.

Dynamic Rules

Dynamic rules are created by the firewall for outgoing connections. The validity period of the dynamic rules (**Time to live**) must be configured in minutes.

Static Rules

Up to 30 static firewall rules can be added. Static rules allow access to a specific service on the device from the network. Static rules have the following parameters:

Network interface
Determines the network interface from which connections should be accepted. For example, if access to the device's web server should only be allowed from the local area network, select the Ethernet interface here. If a rule is not intended for a specific network interface, select the *Any* option.

Service
This selection provides a set of predefined services to which connections can be permitted. If the desired service is not on the list, select the *Other* option in order to manually specify the service's protocol and port(s).

Protocol
This parameter is only displayed if the *Other* option is selected under *Service*. It determines which base protocol (TCP or UDP) is used by the service that should be allowed.

Minimum/Maximum port
These parameters are only displayed if the *Other* option is displayed under *Service*. They determine the port(s) that run the service that should be allowed.
A single port (set minimum and maximum port to the same value) or a port range (e.g. 10000 to 10005) can be specified. Both parameters can also be set to 0. This means that connections are permitted on every port (wildcard).

Minimum/Maximum source IP address
Determines the IP addresses that should be permitted to connect to the specified services. A single IP address (set minimum and maximum address to the same value) or an IP address range (e.g. 192.168.0.1 to 192.168.0.10) can be specified. Both parameters can also be set to 0.0.0.0. This means that connections are permitted from every IP address (wildcard).

Event log messages

The firewall is implemented inside the NAT service unit. Event log messages are documented there.

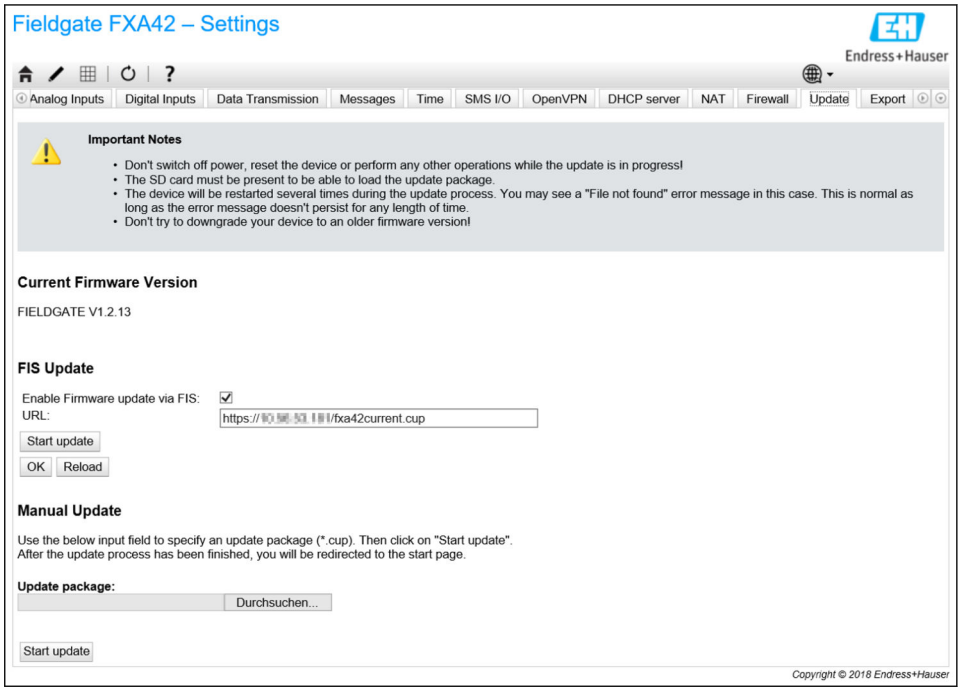
8.4.17 Update

Due to storage and transportation times, the latest firmware version might not be installed on your device. It is therefore advisable to update the firmware when commissioning the device.

Click the following link to download the latest firmware:

https://weupcmasafgfirmware.blob.core.windows.net/fxa42/fxa42_current.cup

An updated firmware version can be installed on the device using the settings and buttons on this page. The installed version of the firmware is displayed. Firmware settings that were made before an update and have been saved by rebooting the device are retained.



It is possible to run an update in 3 different ways:
- FIS update: the update is triggered by the FIS (Field Information Server) and then runs automatically. Only possible in conjunction with SupplyCare Hosting.
- Manual update with Web GUI.
- Manual update with SD card.

NOTICE

A complete device failure can occur if a live update process is interrupted.
If this happens, the device then does not transmit any more data and can no longer be configured.

- Pay attention to the warnings on the **Update** page of the device user interface.
- It is important to wait until the update is finished. This can take a few minutes. Once the update is finished, the device is automatically restarted and the device home page is displayed in the Web browser.
- Ensure that the power supply to the device is not disconnected during the update process.

An SD card with sufficient free space is required to download and unpack the new firmware. The card must be inserted in the device. If this memory is not available, it is not possible to run an update. An error message is displayed.

If the SD card is only inserted after start-up, the new firmware is not uploaded. In this case, reboot the device with the SD card plugged in.

While the device is being programmed, the website may not be able to contact it. Therefore communication errors might be reported. This is normal as long as the error message does not persist for any length of time.

While accessing the SD card, the device may not be able to update the physical I/Os.

Formatting the SD card

The SD card included in the delivery is already formatted.

To be able to update the firmware of the Fieldgate FXA42, an SD card (card type: microSD) formatted by the device itself must be provided. The SD card is formatted with the Power-Loss-Protection (PLP) format. The PLP format is compatible with FAT16/FAT32.

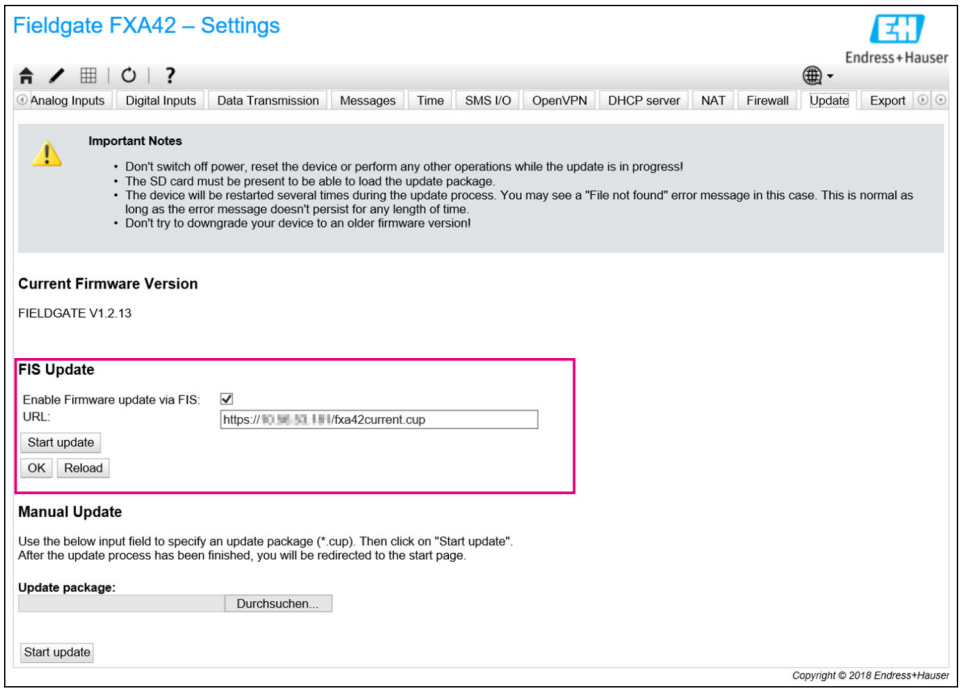
Formatting the SD card for updates

1. Switch off the device (disconnect it from the supply voltage).
2. If an SD card is inserted in the slot, remove the SD card. Insert the new, unformatted SD card in the slot.
3. Switch the device back on (connect it to the supply voltage).
   ↳ The Fieldgate FXA42 starts and formats the SD card. This process also creates the *fxa42* directory into which the update package (*.cup) is subsequently written.

FIS update

With this procedure, the update is triggered with the help of the FIS (Field Information Server). The update then runs automatically on the device itself. This option is only possible in conjunction with SupplyCare Hosting.

This procedure has the major advantage that Endress+Hauser can run an update remotely (following prior agreement).



Prerequisites for a FIS update

1. Insert an SD card in the slot of the device. The SD card must have been formatted beforehand by the Fieldgate FXA42. An SD card with sufficient free space is required to download and unpack *.cup files.
2. Tick the **Enable Firmware update via FIS** check box if it is not already ticked. The check box is on the **Settings** > **Update** page, in the **FIS Update** section.
3. In the **URL:** field, enter the following URL if a URL has not yet been entered:
   ↳ https://weupcmasafgfirmware.blob.core.windows.net/fxa42/fxa42_current.cup

A FIS update can also be started manually by clicking the **Start update** button on the **Update** page.

Event log messages

Update due to FIS command

Starting update due to FIS command. The device is restarted after a successful update.

Firmware update via FIS request denied: Firmware update via FIS not enabled

The update request was denied. The "**Enable Firmware update via FIS**" setting is not enabled.

Firmware update via FIS request denied: Update/configuration already in progress

The update request was denied. An update is already in progress.

Updating the firmware manually

Preconditions for a manual update:
- The device is connected to a stable power supply.
- The SD card has been formatted by the device.
- The latest firmware has already been downloaded or can be downloaded via an Internet connection.
  Click the following link to download the latest firmware:
  https://weupcmasafgfirmware.blob.core.windows.net/fxa42/fxa42_current.cup

The SD card included in the delivery is already formatted.

NOTICE

A complete device failure can occur if a live update process is interrupted.
If this happens, the device then does not transmit any more data and can no longer be configured.

- Pay attention to the warnings on the**Update** page of the device user interface.
- Once the update has started, make sure to wait until it has finished. This can take a few minutes. Once the update is finished, the device is automatically restarted and the device home page is displayed in the Web browser.
- Ensure that the power supply to the device is not disconnected during the update process.

Manual update with Web GUI

Comply with the conditions for a manual update specified at the start of this chapter.

1. Open a Web browser and log into the Web GUI of the device.
2. Open the **Settings** page.
3. Open the **Update** page. Pay attention to the warning on the page that opens.
4. Click the **Browse...** button in the **Manual Update** section.
   ↳ A dialog box opens where you can select the update file.
5. Select the update package.
6. To start the update, click the **Start update** button.
   ↳ Once the update has started, make sure to wait until it has finished. This can take a few minutes.

Once the update is finished, the device is automatically restarted and the device home page is displayed in the Web browser.

Manual update with SD card

If there is no data connection to the device, the user can also copy the current firmware to the SD card using the PC.

Comply with the conditions for a manual update specified at the start of this chapter.

The SD card included in the delivery is already formatted.

1. Download the current version of the firmware (update package (*.cup)) and save it.
2. Insert the SD card formatted by the device into a card reader or into a suitable interface on the PC.
3. Open a file management program (e.g. Explorer) and write the update package to the SD card. File path: b:\FXA42\update.cup
4. Insert the SD card into the slot provided on the device.
5. Using a suitable tool (e.g. a piece of wire), press the reset button until the **Web-PLC** LED flashes twice.
   ↳ Once the update has started, make sure to wait until it has finished. This can take a few minutes.

When the update is finished, the device reboots automatically.

Open-source software

The following open-source software has been used to implement the update functionality:

libarchive

libarchive is used to extract update packages.

Project website: www.libarchive.org

License: LGPL

zlib

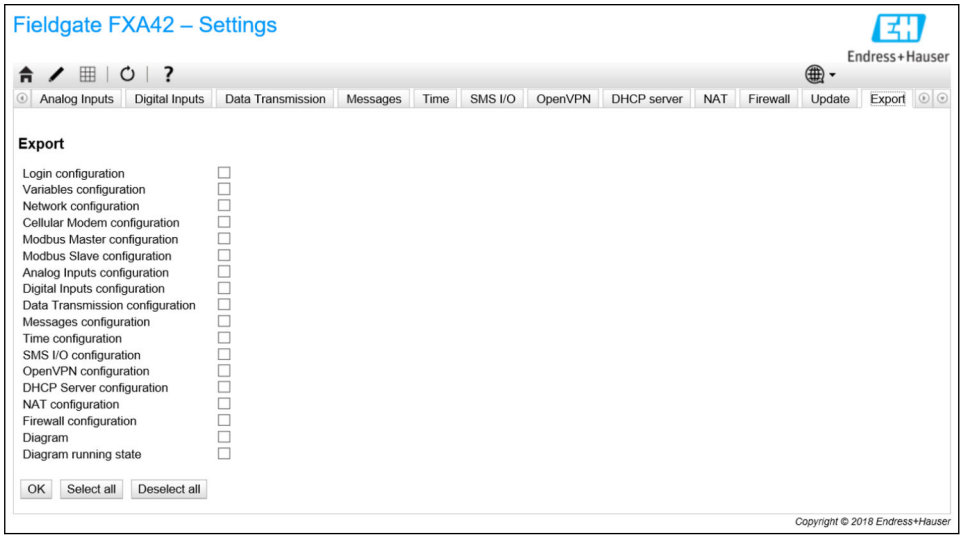
zlib is used to extract update packages.

Project website: www.zlib.net

License: zlib-Lizenz

8.4.18 Export

The configuration of your device can be exported on this page.



A update package is created that can be used for other devices of the same type. To apply the exported packet to a second device, use the Update page.

Select the settings to be exported and click the *OK* button. The update package is created and made available for download.

Event log messages

The following section describes the messages that the update system may log to the event log. The messages are prefixed with the text *Update Exporter*:

Preparing export...

Preparing to export the configuration of the device.

Packing update package...

The configuration is now being packed into an update package.

Update package has been successfully packed

The configuration has been successfully packed into an update package.

Preparation failed. Message: <message>

The preparation of the configuration export failed. A detailed error description is appended to the message.

Packing failed. Message: <message>

Packing the configuration into an update package failed. A detailed error description is appended to the message.

Open-source software

The following open-source software has been used to implement the export functionality:

libarchive

libarchive is used to create update packages.

Project website: www.libarchive.org

License: Neue BSD-Lizenz

zlib

zlib is used to compress update packages.

Project website: www.zlib.net

License: zlib-Lizenz

8.5 Event log messages at system start-up

Messages that the firmware may log to the event log are displayed. All messages are prefixed with the text *Run Time System*:

Started

The firmware has been started.

I/O hardware manager initialized

The I/O hardware manager that manages the physical I/O hardware has been successfully initialized.

NAT/firewall service initialized

The NAT and firewall service has been successfully initialized.

Ethernet (1) driver started.

The driver for the second Ethernet interface has been successfully started.

Cellular modem driver initialized

The cellular modem driver has been successfully initialized.

Update module initialized

The update unit, which manages the loading and programming of update packages, has been successfully initialized.

PLC driver initialized

The PLC driver has been successfully initialized.

Message manager initialized

The message manager, which handles the sending and reception of messages, has been successfully initialized.

DHCP server initialized

The DHCP server has been successfully initialized.

OpenVPN client initialized

The OpenVPN client has been successfully initialized.

Status web service initialized

The status web service, which provides the data to be displayed on the home page, has been successfully initialized

System time manager initialized

The system time manager has been successfully initialized.

COM Server initialized

The COM server has been successfully initialized.

Diagram loaded

A diagram has been successfully loaded.

Web configuration modules initialized

The web configuration modules, which accept the configuration data from the Settings page, have been successfully initialized.

Update exporter module initialized

The update exporter module, which exports the configuration to an update package, has been successfully initialized.

Update web service initialized

The update web service, which manages the upload of update packages via the local web server, has been successfully initialized.

Running

The run-time system has finished initialization.

Starting update from external medium.

The user has triggered an update from the external medium.

Link detected at Ethernet (<interface index>).

The Ethernet interface with the index indicated has been connected to the network.

Restarting DHCP configuration at Ethernet (<interface index>).

The run time system is trying to get a new IP configuration for the Ethernet interface with the index indicated from a DHCP server.

DHCP configuration completed at Ethernet (<interface index>).

The run time system has received a new IP configuration for the Ethernet interface with the index indicated from a DHCP server.

Power fail handling not supported

The device is not equipped with a power fail circuit. Data (e.g. portal variables) cannot be stored retentively.

Not enough power fail capacity

The device is equipped with a power fail circuit, but the capacity supplied is not sufficient to store data (e.g. portal variables) retentively.

Retentive data could not be loaded.

Retained data (e.g. portal variables) could not be loaded although the device is equipped with a power fail circuit. This message appears when the device is started for the very first time. If it occurs later, there is probably a problem with the power fail circuit.

The internal flash drive seems to be weak.

A write operation to the internal flash drive needed to be retried several times. This is an indication that the flash drive is reaching the end of its life.

Flash write error. The internal flash drive is probably defect.

A write operation to the internal flash drive failed. The flash drive seems to have reached the end of its life. The device is no longer usable.

One or more certificates could not be loaded.

At least one of the SSL certificate files could not be loaded.

Could not initialize NAT/firewall service. (<error code>)

The NAT and firewall service could not be initialized. The message also shows an internal error code returned by the service's initialization routine.

Could not start Ethernet (1) driver.

The driver for the second Ethernet interface could not be started.

Unsupported Ethernet (1) interface type. (<interface type>)

The Fieldgate FXA42 firmware could not find a driver for the second Ethernet interface. The message also shows the numerical Ethernet interface type.

Could not initialize NAT/firewall service. (<error message>)

The NAT and firewall service could not be initialized. The message also shows an error message returned by the service's initialization routine.

Could not initialize cellular modem driver: <error message>

The cellular modem driver could not be initialized. The message also shows an error message returned by the driver's initialization routine.

Could not initialize WLAN driver: <error message>

The WLAN driver could not be initialized. The message also shows an error message returned by the driver's initialization routine.

Could not initialize update module: <error message>

The update module, which manages the loading and programming of update packages, could not be initialized. The message also shows an error message returned by the module's initialization routine.

Could not initialize DHCP server.

The DHCP driver could not be initialized.

Could not initialize OpenVPN client: <error message>

The OpenVPN client could not be initialized. The message also shows an error message returned by the client's initialization routine.

Could not initialize system time manager: <error message>

The system time manager could not be initialized. The message also shows an error message returned by the manager's initialization routine.

Could not initialize COM server: <error message>

The COM server could not be initialized. The message also shows an error message returned by the server's initialization routine.

Could not initialize portal Event Log service: <error message>

The portal event log service could not be initialized. The message also shows an error message returned by the service's initialization routine.

Could not load and start diagram.

A diagram could not be loaded and therefore the PLC could not be started.

Could not initialize web configuration modules: <error message>

The web configuration modules, which accept the configuration data from the Settings page, could not be initialized. The message also shows an error message returned by the modules' initialization routines.

Could not initialize update exporter module: <error message>

The update export module, which exports the configuration to an update package, could not be initialized. The message also shows an error message returned by the module's initialization routine.

Could not initialize update web service: <error message>

The update web service, which manages the upload of update packages via the local web server, could not be initialized. The message also shows an error message returned by the service's initialization routine.

Task cycle time has been violated.

The cycle time of the PLC task has been violated, i.e. the task was still busy with the previous IPO cycle when it was supposed to the next IPO cycle.

Could not start update from external medium.

The user has triggered an update from the external medium but the update could not be started.

Link lost at Ethernet (<interface index>).

The Ethernet interface with the index indicated has been disconnected from the network.

RTOS version is not supported. Version (<version number>) is required.

The current RTOS version is not the version required. Please install the version specified in the event log.

Device is secured with the default password, please change it.

This message is shown when the default password is still used. For security reasons, it is recommended to change the password. You can do so via the login settings.

Fatal error: <error message>

A fatal error prevented firmware start-up. The message also shows an error message describing the error.

8.6 Dojo Toolkit

The Dojo Toolkit has been used to implement these web sites.

Project website: dojotoolkit.org

License: Dojo license

8.6.1 Other open-source software

FileSaver.js

Project website: github.com/eligrey/FileSaver.js

License: FileSaver.js license

9 Diagnostics and troubleshooting

9.1 Faults indicated by the LEDs

⚠ WARNING

Danger! Electric voltage!
Risk of electric shock and injury from startle response.
- ▶ De-energize all power sources before disconnecting and connecting.
- ▶ Only work with insulated tools.

The **Power** LED is not lit.
Possible cause: No power
- Action: Check to ensure that the power supply is wired correctly
- Action: Check to ensure that the supply voltage corresponds to the voltage indicated on the nameplate
- Action: Check to ensure that the power is switched on

The **modem / WLAN / Ethernet** LED is not lit.
Possible cause: The power supply for the modem / WLAN unit / Ethernet interface is interrupted
Action: Switch off the power supply, wait 30 s seconds, then switch the power supply back on

The **Network** LED is not lit.
Possible cause: Fieldgate FXA42 Ethernet: the Ethernet data connection is interrupted. A valid fixed IP address has not been configured or DHCP was not completed successfully.
- Action: Check to ensure that the configured IP address is valid
- Action: Check to ensure that the dynamic allocation of IP addresses (DHCP) works correctly in the connected network
- Action: Check to ensure that the Ethernet connections are correctly engaged and that the cables are OK

9.2 Restoring factory settings

The reset button (→ 🖹 8) can be accessed through a small hole in the front.

1. Switch off the Fieldgate FXA42 (switch off the supply voltage).
2. Press and hold the reset button.
3. Switch on the Fieldgate FXA42. Keep the reset button pressed during the booting procedure.
   ↳ The factory settings are restored.

10 Maintenance

No special maintenance work is required.

10.1 Exterior cleaning

Clean the device with a dry cloth.

NOTICE

Caustic cleaning agents or solvents corrode surfaces.
Important information on the housing may become illegible, surfaces become corroded.
- ▶ Do not use caustic cleaning agents or solvents.

⚠ CAUTION

Danger from electric voltage when cleaning with water.

Risk of electric shock and injury from startle response.

- ▶ Do not clean the device with water.

11 Repair

11.1 General information

11.1.1 Repair concept

Repairs are not possible.

11.2 Return

The requirements for safe device return can vary depending on the device type and national legislation.

1. Refer to the web page for information: https://www.endress.com
2. If returning the device, pack the device in such a way that it is reliably protected against impact and external influences. The original packaging offers the best protection.

11.3 Disposal

If required by the Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), the product is marked with the depicted symbol in order to minimize the disposal of WEEE as unsorted municipal waste. Do not dispose of products bearing this marking as unsorted municipal waste. Instead, return them to the manufacturer for disposal under the applicable conditions.

12 Accessories

12.1 Device-specific accessories

Power unit
Power unit for power supply
Material number: 71327426

Antenna
Antenna with SMA connection for mobile telecommunications or WLAN operation
Material number: 71327395

SD card (card type: microSD)
On request

Communication modules
- Datexel DAT8017-I server unit: analog to Modbus TCP converter
  Material number: 71375710
- Rapsystems HG1 Plus: HART to Modbus gateway
  Material number: 71327424
- Phoenix Contact: HART Ethernet multiplexer head module
  Material number: 71363548
- Phoenix Contact: 4-channel HART extension module
  Material number: 71363561
- Phoenix Contact: 8-channel HART extension module
  Material number: 71363582

12.2 Communication-specific accessories

SupplyCare Enterprise SCE30B
Inventory management software that displays the level, volume, mass, temperature, pressure, density or other parameters of tanks. The parameters are recorded and transmitted using the Fieldgate FXA42 or other types of gateways.
This Web-based software is installed on a local server and can also be visualized and operated with mobile devices such as a smartphone or tablet.

For details, see Technical Information TI01228S and Operating Instructions BA00055S

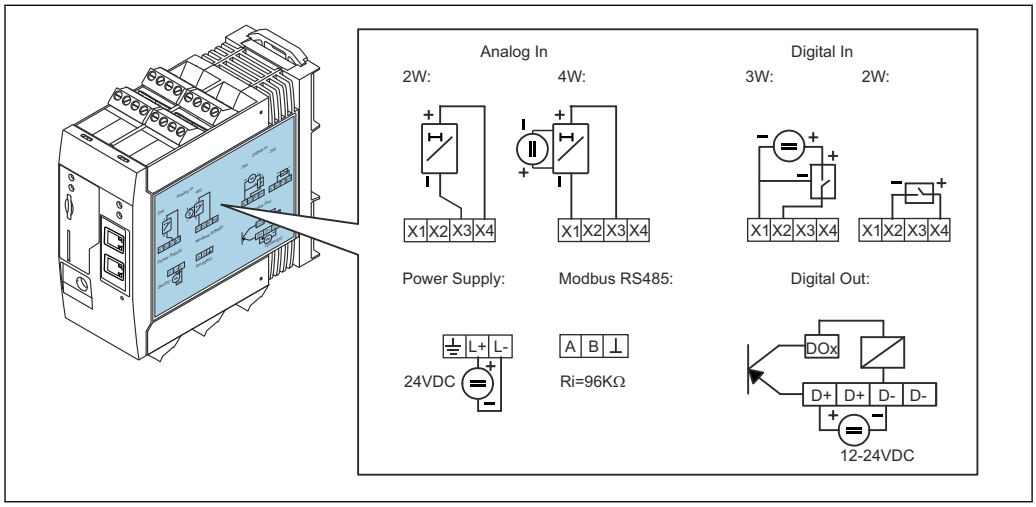
SupplyCare Hosting SCH30
Inventory management software that displays the level, volume, mass, temperature, pressure, density or other parameters of tanks. The parameters are recorded and transmitted using the Fieldgate FXA42 or other types of gateways.
SupplyCare Hosting is offered as a hosting service (Software as a Service, SaaS). In the Endress+Hauser portal, the user is provided with the data over the Internet.

For details, see Technical Information TI01229S and Operating Instructions BA00050S

13 Technical data

13.1 Input

13.1.1 Terminal assignment



8 Labeling on the housing for terminal assignment

13.1.2 Weight

Approx.300 g (10.6 oz)

13.1.3 Materials

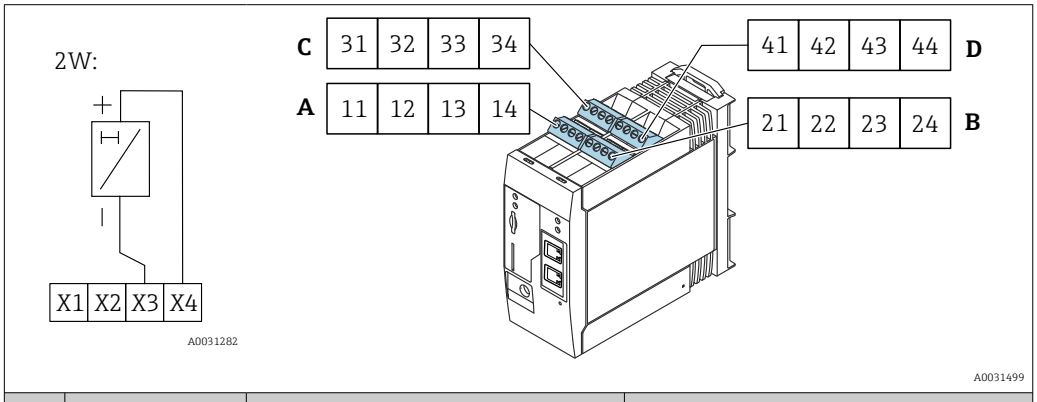
Housing: plastic PC-GF10

13.1.4 Terminals

Plug-in screw terminals, 2.5 mm^2 (14 AWG), 0.1 to 4 mm^2 (30 to 12 AWG), torque 0.5 to 0.6 Nm (0.37 to 0.44 lbf ft)

13.1.5 4 to 20 mA analog input

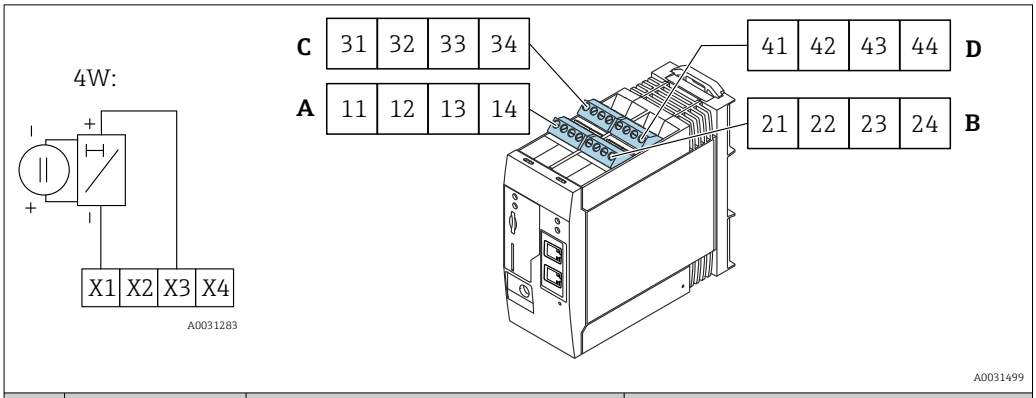
4 to 20 mA analog input (2-wire) with auxiliary voltage output



	Terminal block	Function	Properties

	A	B	C	D		
X1 =	11	21	31	41	4 x GND	
X3 =	13	23	33	43	4 x 4 to 20 mA analog input	Maximum input voltage: 35 V Maximum input current: 22 mA Internal resistance: 250 Ω (suitable for HART communication) Measuring range: 3.8 to 20.5 mA Resolution: 16 bit Accuracy: 0.1% of measuring range
X4 =	14	24	34	44	4 x auxiliary voltage output for transmitter loop power supply	Output voltage: 28 V_{DC} (no-load) 26 V_{DC} @ 3 mA 20 V_{DC} @ 30 mA Output current: max. 160 mA

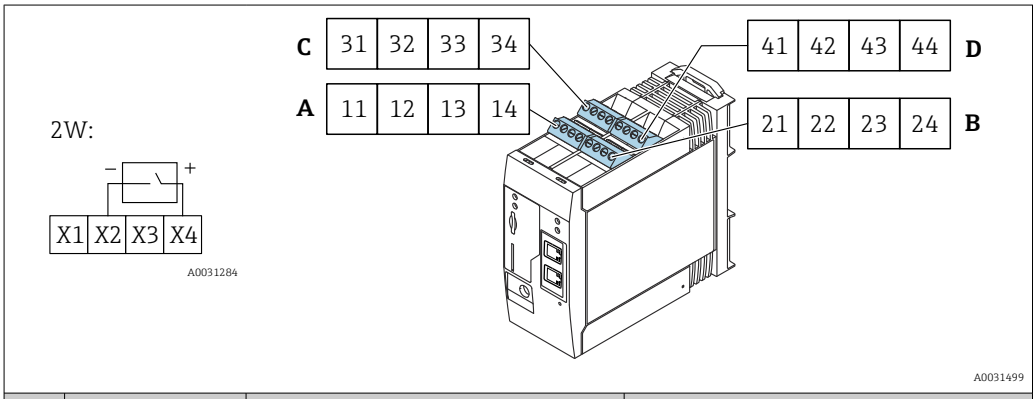
4 to 20 mA analog input (4-wire)



	Terminal block				Function	Properties
	A	B	C	D		
X1 =	11	21	31	41	4 x GND	
X3 =	13	23	33	43	4 x 4 to 20 mA analog input	Maximum input voltage: 35 V Maximum input current: 22 mA Internal resistance: 250 Ω (suitable for HART communication) Measuring range: 3.8 to 20.5 mA Resolution: 16 bit Accuracy: 0.1% of measuring range

13.1.6 Digital input

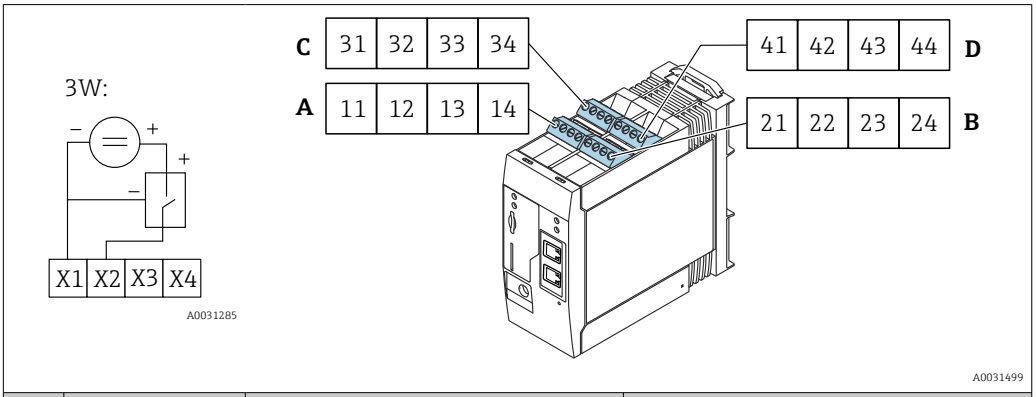
Digital input (2-wire) with auxiliary voltage output



	Terminal block	Function	Properties

	A	B	C	D		
X2 =	12	22	32	42	4 x digital input	Input voltage L: < 5 V Input voltage H: > 11 V Input current: < 5 mA Maximum input voltage: 35 V
X4 =	14	24	34	44	4 x auxiliary voltage output to control the digital inputs	Output voltage: 28 V_{DC} (no-load) 26 V_{DC} @ 3 mA 20 V_{DC} @ 30 mA Output current: max. 160 mA

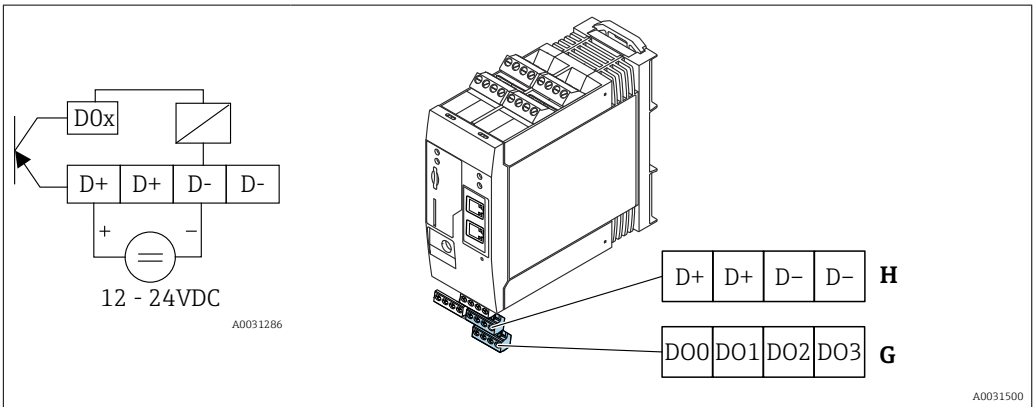
Digital input (3-wire)



	Terminal block				Function	Properties
	A	B	C	D		
X1 =	11	21	31	41	4 x GND	
X2 =	12	22	32	42	4 x digital input	Input voltage L: < 5 V Input voltage H: > 11 V Input current: < 5 mA Maximum input voltage: 35 V

13.2 Output

13.2.1 Digital output



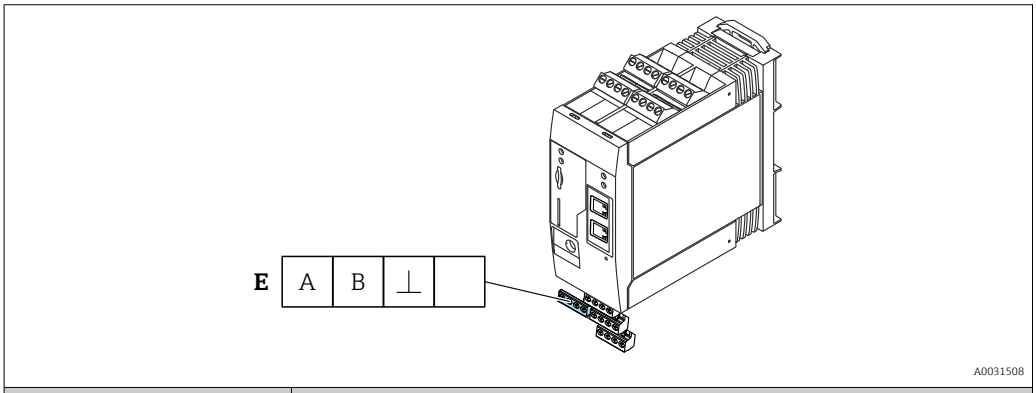
Terminal block	G	Properties
DO0 DO1 DO2 DO3 Digital output	DO0	High-side driver, sourcing, DC-PNP. Output current:500 mA
	DO1	
	DO2	
	DO3	

Terminal block	H	Properties
D+ D+ D− D−	D+	12 to 24 V_{DC}
	D+	12 to 24 V_{DC}
Power supply for digital output [1]	D-	GND
	D-	GND

1) You may only use power units that ensure safe electrical isolation according to DIN VDE 0570-2-6 and EN61558-2-6 (SELV / PELV or NEC Class 2) and that are designed as limited-energy circuits.

13.2.2 RS485 serial interface (Modbus)

- Internal resistance: 96 kΩ
- Protocol: Modbus RTU
- External termination required (120 Ω)



A0031508

Terminal block	E	Properties
A B ⊥	A	Signal
	B	Signal
Serial interface RS485	⊥	Ground / optional shield connection
		Not assigned

13.3 Environment

13.3.1 Ambient temperature range

Normal operation (EN 60068-2-14; Nb; 0.5 K/min): −20 to 60 °C (−4 to 140 °F)

Side by side installation: −20 to 50 °C (−4 to 122 °F)

13.3.2 Transportation and storage temperature

EN 60068-2-1; Ab; 0.5K/min / EN 60068-2-2; Bb; 0.5K/min: −25 to 85 °C (−13 to 185 °F)

13.3.3 Humidity

EN 60068-2-30; Db; 0.5 K/min: 5 to 85%; non-condensing

13.3.4 Condensation

Not permitted

13.3.5 Climate class

To IEC 60654-1, Class B2

13.3.6 Installation height as per IEC61010-1 Ed.3

Generally up to 2 000 m (6 560 ft) above sea level

13.3.7 Degree of protection

IP20, NEMA1

13.3.8 Shock resistance

DIN EN 60068-2-27: ±15 g; 11 ms

13.3.9 Vibration resistance

EN 60068-2-64 / IEC60068-2-64: 20..2000 Hz 0.01 g^2/Hz

13.3.10 Electromagnetic compatibility

- Interference immunity: as per IEC 61326, industrial environment
- Interference emissions: as per IEC 61326, Class B

13.4 Certificates and approvals

Current certificates and approvals for the product are available at www.endress.com on the relevant product page:

1. Select the product using the filters and search field.
2. Open the product page.
3. Select **Downloads**.

13.4.1 CE mark

The device meets the legal requirements of the applicable EC directives. These are listed in the corresponding EC declaration of conformity together with the standards applied.

13.4.2 UKCA marking

The device meets the legal requirements of the applicable UK regulations (Statutory Instruments). These are listed in the UKCA Declaration of Conformity along with the designated standards. By selecting the order option for UKCA marking, Endress+Hauser confirms a successful evaluation and testing of the device by affixing the UKCA mark.

Contact address Endress+Hauser UK:
Endress+Hauser Ltd.
Floats Road
Manchester M23 9NF
United Kingdom
www.uk.endress.com

13.4.3 RoHS

The measuring system meets the substance restrictions of the Directive on the Restriction of the Use of Certain Hazardous Substances 2011/65/EU (RoHS 2) and the Delegated Directive (EU) 2015/863 (RoHS 3).

13.4.4 External standards and guidelines

Other standards and guidelines that have been considered in the design and development of the device:

- EN 60529
  Degrees of protection provided by enclosure (IP code)
- EN 61010-1
  Safety requirements for electrical equipment for measurement, control and laboratory use
- IEC/EN 61326
  "Emission in accordance with Class A requirements" Electromagnetic compatibility (EMC requirements)

13.5 Telecommunications approval

13.5.1 Europe

This device meets the requirements of the Radio Equipment Directive (RED) 2014/53/EU.

13.5.2 USA and Canada

This device complies with Part 15 of the FCC rules.

Federal Communications Commission Notice

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

To ensure that the unit complies with current FCC regulations and safety requirements limiting both maximum RF output power and human exposure to radio frequency radiation, use an antenna with a maximum gain of 2 dBi and a separation distance of at least 20 cm must be maintained between the unit's antenna and the body of the user and any nearby persons at all times and in all applications and uses.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Endress+Hauser may void the user's authority to operate the equipment.

Federal Communications Commission Statement

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Wireless Notices

In some situations or environments, the use of wireless devices may be restricted. Such restrictions may apply aboard airplanes, in vehicles, in hospitals, near explosives, in

hazardous locations, etc. If you are uncertain of the policy that applies to the use of this device, please ask for authorization to use it prior to turning it on.

13.5.3 Other certificates

Other national approvals are available on request.

- **Bulgaria**
  General authorization required for use outdoors and in public.
- **Italy**
  General authorization is required for use outside of own premises.
- **Norway**
  Use can be limited within a 20-km radius of the center of Ny-Alesund.
- **Romania**
  Use as a secondary device; special license required.
- **Latvia**
  A national permit is required for outdoor use of the 2.4 GHz frequency.

Index

A
Application 6

C
CE mark (declaration of conformity) 7
Cleaning 108

D
Declaration of conformity 7
Disposal 110

E
Exterior cleaning 108

F
Field of application
  Residual risks 6
Frequency bands 8

I
Intended use 6

M
Maintenance 108

O
Operational safety 6

P
Product safety 7

R
Registered trademarks 5
Repair concept 110
Requirements for the personnel 6
Return 110

S
SD card
  Formatting 100

U
UKCA marking 116
Update
  Firmware 99
  FIS update 100
  Manual 101
  Manually with SD card 102
  Manually with Web GUI 102
Use of the measuring devices
  Borderline cases 6
  Incorrect use 6

W
Workplace safety 6

www.addresses.endress.com

For more Endress+Hauser product please visit: www.ainstru.com
Mail: Sales@ainstru.com

Endress+Hauser
People for Process Automation