SIEMENS

FDE
SIMATIC FDE Gateway V1.2

Equipment Manual

Preface 1

Siemens Industry Online Support 2

Introduction 3

Overview of the technical documentation 4

Installing and connecting a device 5

Software and commissioning 6

Certificates and approvals 7

Directives and declarations 8

Technical specifications 9

Dimension drawings A

05/2024
A5E52683268-AF

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E52683268-AF
Ⓟ 06/2024 Subject to change

Copyright © Siemens 2024.
All rights reserved

Table of contents

1 Preface 5

2 Siemens Industry Online Support 6

3 Introduction 7

3.1 Cybersecurity information 7

3.2 Physical protection 7

3.3 IT security on the northbound side 8

3.4 IT security on the southbound side 9

3.5 Personal data 9

3.6 Incident reporting 9

4 Overview of the technical documentation 10

4.1 SIMATIC products 10

4.2 SINAMICS products 10

4.3 SENTRON products 12

5 Installing and connecting a device 14

5.1 Scope of supply 14

5.2 Information on the software license 14

5.3 Description 14

5.4 Device design 17

5.5 Analog input and digital input/output 18

5.6 Operating modes and LED display 19

5.7 Changing the operating mode 22

5.8 Preparing for installation 23

5.9 Installing the device 25

5.9.1 Professional installation guide 25

5.9.2 Mounting instructions 25

5.9.3 DIN-rail mounting 26

5.10 Connecting the device 28

5.10.1 Notes for connecting 28

5.10.2 Connecting interfaces to connecting terminal X4 29

5.10.3 Connecting the power supply 30

5.10.4 Securing cables 30

5.10.5 Connecting a device to the RS232 interface 31

5.10.6 Connecting a device to the RS485 interface 33

6 Software and commissioning 34
6.1 Establishing a connection to the device 34
6.2 Device configuration 37
6.3 Network settings 40
6.4 Connectivity settings 45
6.4.1 MQTT settings 45
6.4.2 Enable analog & digital input and digital output 52
6.4.3 USS settings 57
6.4.4 Activate Modbus TCP (X2) 60
6.4.5 Activating Modbus RTU (RS485) 64
6.5 MQTT parameters 65
6.6 MQTT payload examples 70
6.7 Basic settings 74
6.7.1 Date & time 75
6.7.2 Resetting to factory settings 75
6.7.3 System upgrade 76
6.7.4 Antenna settings 78
6.7.5 Access point 79
6.8 Settings for operation on the BFC Gateway 79
6.9 Settings for operation on the Industrial Edge device 81
6.10 Settings for operation in MindSphere 82
7 Certificates and approvals 83
7.1 CE (Industry) 83
7.2 UKCA 83
7.3 RCM Declaration of Conformity for Australia/New Zealand 84
7.4 FCC and Canada (USA) 84
8 Directives and declarations 87
8.1 Overvoltage category 87
8.2 Pollution degree for electrical equipment 87
8.3 Electromagnetic Compatibility industrial area +A1:2011 87
8.4 ESD guideline 87
9 Technical specifications 90
9.1 General technical specifications 90
9.2 Ambient conditions 93
A Dimension drawings 94
A.1 Dimension drawings 94

Preface

1

The following operating instructions contain all the required information required for commissioning and operating a device from the SIMATIC family.

Basic knowledge required

A prerequisite for understanding this manual is knowledge of how to use a PC. Basic knowledge of automation technology as well as IoT technologies is also recommended.

Scope of this document

These operating instructions apply to the SIMATIC FDE Gateway device.

For the EU market: MLFB **6ES7617-0BA01-0AB0**

For the U.S. market: MLFB **6ES7617-0BA01-0BB0**

FDE conventions

The following generic terms are used in this documentation:

Generic term	Specific designation
Device	SIMATIC FDE Gateway

Change directory

The following versions of these operating instructions have been published:

Edition	Comment
05/2024	Physical identification of the installed module by an LED display that is activated from the home page. Remote check of the physical connection of the Ethernet cable to the FDE Gateway on the configuration page. USS and MQTT diagnostics, Modbus data snapshot and measuring tools for inputs and outputs. Function for remote system update. Wi-Fi scan function. Updated user interface.
10/2023	Modbus RTU functionality added
04/2023	First edition

Siemens Industry Online Support

2

You can find current information on the following topics quickly and easily here:

- **Product support**

  All the information and extensive know-how on your product, technical specifications, FAQs, certificates, downloads, and manuals.

- **Application examples**

  Tools and examples to solve your automation tasks – as well as function blocks, performance information and videos.

- **Services**

  Information about Industry Services, Field Services, Technical Support, spare parts and training offers.

- **Forums**

  For answers and solutions concerning automation technology.

- **mySupport**

  Your personal working area in Industry Online Support for messages, support queries, and configurable documents.

This information is provided by the Siemens Industry Online Support in the Internet (https://support.industry.siemens.com).

Introduction 3

3.1 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

3.2 Physical protection

The device is designed to provide security features that keep the installation secure and protected from various types of cybersecurity threats However, all these security features require assistance from the user of the device, who is assumed to physically protect the device hardware from unauthorized access, modification or even replacement.

Protection of the wiring

Not only the device itself but also the wiring can become the target of an attack and must be protected. Failure to secure communication or power lines may result in communication interruptions or unauthorized disclosure/alteration of critical data.

Although the FDE Gateway itself is not intended to change the configuration of connected devices (PLCs, actuators, HMIs, etc.), unauthorized access to the line can allow for detrimental configuration changes in inadequately protected devices.

This applies to all serial ports that do not support secure communication as well as to Ethernet cabling.

Internal protection of the device

The device should always be installed in an area or cabinet that protects the device from unauthorized access. This includes access by unauthorized and untrained personnel who may cause unwanted damage or misconfiguration as well as access by third parties with intent on causing damage.

Wireless interface

The wireless interface poses an additional risk to the customer's system if the Wi-Fi password is not properly configured or if the wireless security configuration uses an outdated security standard (e.g. WEP). Disable the wireless interface when it is not needed.

Supply chain

Purchase all devices in the system from an authorized dealer. Make sure to buy an original device from a trusted source.

Equipment disposal

If a device is decommissioned and should no longer be used, follow these steps:

- Reset the device to factory settings to erase all sensitive data (private keys, Wi-Fi passwords, user accounts).
- If a certificate authority is used for one of the certificates used, add device certificates to a certificate revocation list.
- Ensure that any remaining cables are removed or secured so that they cannot be misused to gain access to the rest of the infrastructure.

3.3 IT security on the northbound side

Ensure sufficient IT security on the northbound side. "Control activities" have a special risk.

We urgently recommend not making the web interface available at any location other than at the production network.

Note

Proper user administration required

Select one dedicated access token/login information per device.

3.4 IT security on the southbound side

The FDE Gateway provides field data in IT environments.

Ensure that the outputs of the device are not used to control automation processes, but solely for signaling purposes.

Make sure to protect the southbound connection in accordance with currently recognized security guidelines. This prevents spying on the field data. More information and application notes can be found here: (https://www.siemens.com/industrialsecurity)

3.5 Personal data

During the configuration of the FDE gateway, it is possible to store user-specific data such as certificates, usernames, and access passwords. These data are stored on the device and, if appropriate, used service-specifically during operation. The device must be reset to the factory settings to erase these data. See section: Resetting to factory settings (Page 75).

3.6 Incident reporting

All security incidents or concerns can be reported directly to Siemens. The following link contains all the necessary instructions to report a problem correctly:

Incident reporting
(https://www.siemens.com/global/en/products/services/cert.html#GetInTouchwithSiemensProductCERTorSiemensCERT)

Overview of the technical documentation 4

The documents listed below are a selection to support you with the planning, installation, and commissioning, up to the analysis of your application. For more documents on other hardware or specific information, please visit SIEMENS SiePortal. (https://sieportal.siemens.com/)

4.1 SIMATIC products

You can find an overview of the SIMATIC documentation available in Siemens Industry Online Support here:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

4.2 SINAMICS products

SIMATIC FDE Gateway enables connection to the following drives:

- SINAMICS V20
- SINAMICS G120 series (except G120D)
- MICROMASTER 420/430/440

The connection is established via USS/RS232.

SINAMICS G120C low voltage converter

Operating instructions

The operating instructions (https://support.industry.siemens.com/cs/ww/en/view/109782995) also contain information for special applications. Since sound prior knowledge of the configuration and parameter assignment of these applications can be assumed, the information is given in a concise form. This applies, for example, to operation with fieldbus systems.

List Manual

The List Manual (https://support.industry.siemens.com/cs/ww/en/view/109817922) contains a detailed description of all parameters and a series of function charts as well as error and alarm messages.

MICROMASTER 440 frequency converter

Operating instructions

The operating instructions (https://support.industry.siemens.com/cs/ww/en/view/24294529) provide information about characteristics of the MICROMASTER 440 as well as the installation, commissioning, control modes, system parameter structure, troubleshooting, technical specifications, and options.

Parameter list

The parameter list (https://support.industry.siemens.com/cs/ww/en/view/23708204) contains a detailed description of all parameters, ordered by function. It also contains a series of function charts as well as error and alarm messages.

MICROMASTER 430 frequency converter

Operating instructions

The operating instructions (https://support.industry.siemens.com/cs/ww/en/view/24479264) provide information about characteristics of the MICROMASTER 430 as well as the installation, commissioning, control modes, system parameter structure, troubleshooting, technical specifications, and options.

Parameter list

The parameter list (https://support.industry.siemens.com/cs/ww/en/view/24479411) contains a detailed description of all parameters, ordered by function. In addition, the parameter list contains function charts with graphical representations of the converter functions.

MICROMASTER 420 frequency converter

Operating instructions

The operating instructions (https://support.industry.siemens.com/cs/ww/en/view/24523400) provide information about characteristics of the MICROMASTER 420 as well as the installation, commissioning, control modes, system parameter structure, troubleshooting, technical specifications, and options.

Parameter list

The parameter list (https://support.industry.siemens.com/cs/ww/en/view/24525275) contains a detailed description of all parameters, ordered by function. In addition, the parameter list contains function charts with graphical representations of the converter functions.

SINAMICS V20 frequency converter

Operating instructions

The operating instructions (https://support.industry.siemens.com/cs/ww/en/view/109811111) contain information on the installation, commissioning, operation, and maintenance of the SINAMICS V20 frequency converter.

4.3 SENTRON products

SIMATIC FDE Gateway enables connection to the following measuring instruments:

- SENTRON 7KM PAC1020
- SENTRON 7KT PAC1200
- SENTRON 7KT PAC165x
- SENTRON 7KT PAC166x
- SENTRON 7KT PAC1682
- SENTRON 7KM PAC2200
- SENTRON 7KM PAC2200 (CLP)
- SENTRON 7KM PAC3120
- SENTRON 7KM PAC3200
- SENTRON 7KM PAC3200T
- SENTRON 7KM PAC3220
- SENTRON 7KM PAC4200
- SENTRON 7KM PAC5100
- SENTRON 7KM PAC5200

SENTRON 7KM PAC1020 Measuring device

Equipment Manual

The 7KM PAC1020 Measuring Device Manual (https://support.industry.siemens.com/cs/ww/en/view/109776608) is a condensed compilation of all required information for normal and safe operation of the PAC1020 measuring device.

SENTRON 7KT PAC1200 Multi-channel current measuring system

System Manual

The System Manual Multi-channel current measuring system 7KT PAC1200 (https://support.industry.siemens.com/cs/ww/en/view/109483442) is a comprehensive compilation of all required information for normal and safe operation of the PAC1200 Power Monitoring Device.

SENTRON 7KT PAC1600 Measuring devices

Equipment Manual

The 7KT PAC1600 Energy Meter Manual (https://support.industry.siemens.com/cs/ww/en/view/109759827) is a condensed compilation of all required information for normal and safe operation of the PAC1600 series measuring devices.

SENTRON 7KM PAC2200 Measuring device

Equipment Manual

The 7KM PAC2200 Measuring Device Manual (https://support.industry.siemens.com/cs/ww/en/view/109746835) is a comprehensive compilation of all required information for normal and safe operation of the PAC2200 measuring device.

SENTRON 7KM PAC3200T Measuring device

Equipment Manual

The 7KM PAC3200T Measuring Device Manual (https://support.industry.siemens.com/cs/ww/en/view/109746833) is a comprehensive compilation of all required information for normal and safe operation of the PAC3200T measuring device.

SENTRON 7KM PAC3120 und PAC3220 Measuring device

Equipment Manual

The 7KM PAC3120 and PAC3220 Measuring Devices Manual (https://support.industry.siemens.com/cs/ww/en/view/109767307) is a condensed compilation of all required information for normal and safe operation of the PAC3120 and PAC3220 measuring devices.

SENTRON 7KM PAC4200 Power Monitoring Device

System Manual

The 7KM PAC4200 Power Monitoring Device System Manual (https://support.industry.siemens.com/cs/ww/en/view/34261595) is a comprehensive compilation of all required information for normal and safe operation of the PAC4200 Power Monitoring Device.

Power Monitoring Device and Power Quality Recorder SENTRON 7KM PAC5100/5200

Equipment Manual

The 7KM PAC5100/5200 Measuring Devices Equipment Manual (https://support.industry.siemens.com/cs/ww/en/view/109477872) is a condensed compilation of all required information for normal and safe operation of the PAC5100/ PAC5200 measuring devices.

Installing and connecting a device

5

5.1 Scope of supply

Supplied components

The following components are included in the scope of supply of the SIMATIC FDE Gateway with article number 6ES7617-0BA01-0AB0:

- 1 x complete unit SIMATIC FDE Gateway
- 1 x 14-pin connection terminal X4

Note

The antenna is not included in the scope of supply.

If you require an external Wi-Fi antenna, please order it separately.
Recommended type: ANT795-4MX
(https://mall.industry.siemens.com/mall/en/ww/Catalog/Product/6GK5795-4MX00-0AA0)
Antenna with omnidirectional characteristics. Article number: 6GK5795-4MX00-0AA0.

Use the cable 6XV1875-5LH50 and the cabinet feedthrough 6GK5798-2PP00-2AA6.

5.2 Information on the software license

Third-party software

SIMATIC FDE Gateway contains Open Source software and/or other third-party software. Copyright © SIEMENS, 2024, and licensor. All rights reserved. For more information, see the web user interface for configuring the device.

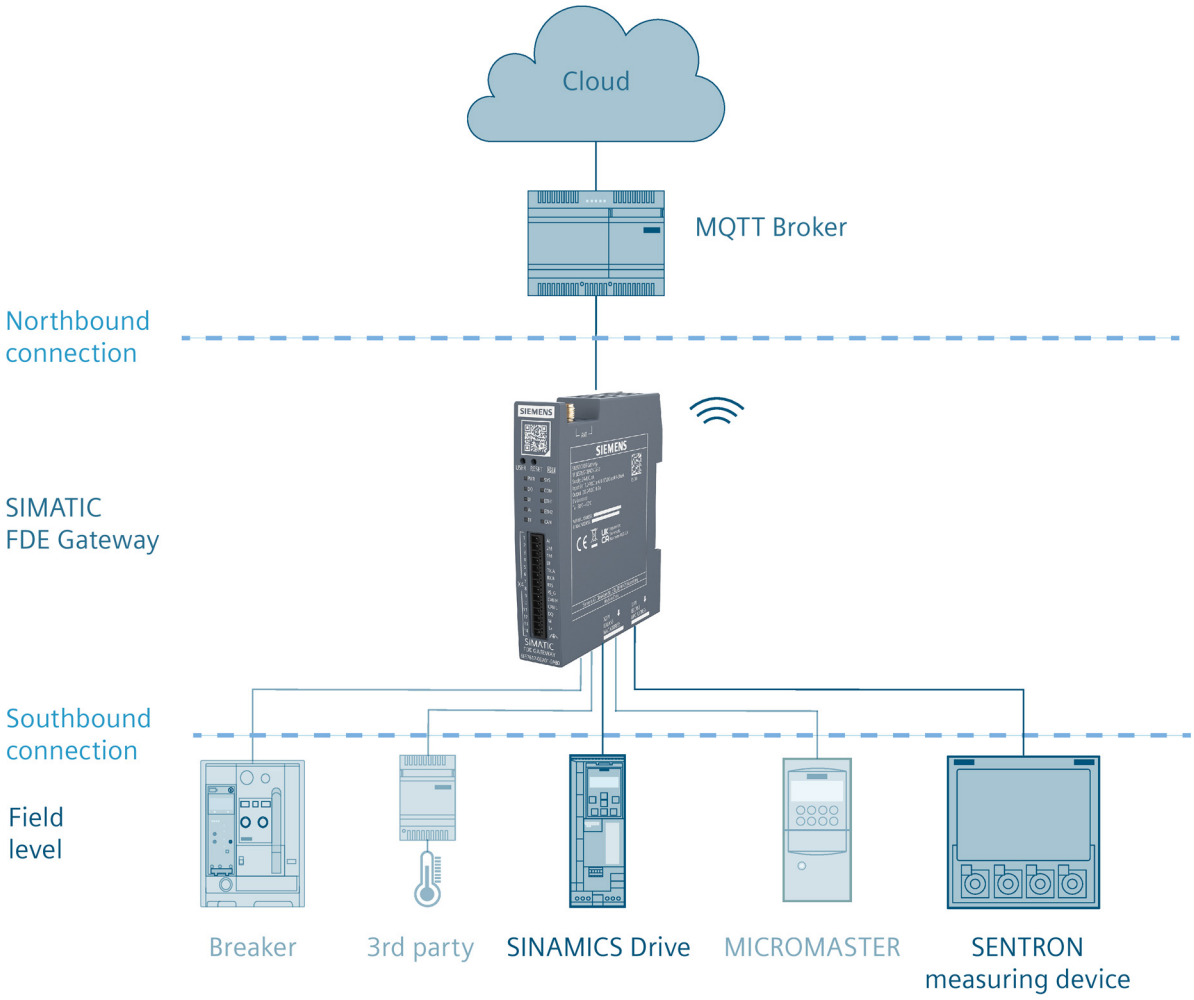
5.3 Description

The SIMATIC FDE Gateway is a flexible IT/OT interface for establishing connectivity for brownfield and greenfield applications. The device allows the transfer of data from the field level to an edge device or to the cloud (Northbound connection).

Via the Southbound connection, the FDE Gateway connects the following inputs and outputs and devices to the cloud systems via MQTT:

- 1 analog input
- 1 digital input

- 1 digital output
- 1 RS232/USS device or 1 RS485/Modbus RTU device
- 1 Modbus TCP device via Ethernet



SINAMICS Drive:	SINAMICS V20, SINAMICS G120 Series (except G120D)
MICROMASTER:	Micromaster 420, 430, 440
SENTRON Modbus measuring device:	e.g. SENTRON 7KM PAC 1020, 7KT PAC 1200, 7KT PAC 165x, 7KT PAC 166x, 7KT PAC 1682, 7KM PAC 2200, 7KM PAC 2200 (CLP), 7KM PAC 3120, 7KM PAC 3200, 7KM PAC 3200T, 7KM PAC 3220, 7KM PAC 4200, 7KM PAC 5100, 7KM PAC 5200

Functionality

The device offers the following functionality:

- Browser-based user interface for configuration and for viewing the device configuration, basic diagnostics
- Forwarding of "Southbound signals" via MQTT to Northbound connectivity.

Note

The SIMATIC FDE Gateway cannot check the data integrity of southbound interfaces.

Properties

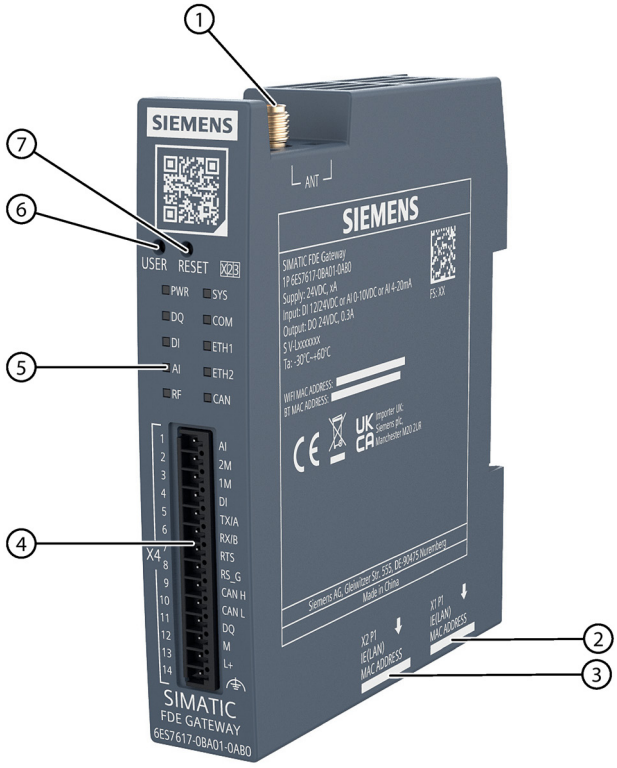
- 2 x Industrial Ethernet interface 100 Mbps:
  - X1 is used for northbound connection
  - X2 can be used either for a northbound connection or for a Modbus TCP connection (southbound)
- 1 x digital input 12/24 V DC
- 1 x analog input 0-10 V DC, 0-20 mA or 4-20 mA
- 1 x digital input 24 V DC / 0.3 A
- 1 x RS232 interface: The product can be connected to the following SINAMICS devices via RS232 interface:
  - SINAMICS V20; over BOP interface module, see the section Connecting a device to the RS232 interface (Page 31)
  - SINAMICS G110M
  - SINAMICS G120 series (except G120D)
  - MICROMASTER 420/430/440
- 1 x RS485 interface: The product can be connected to the following SINAMICS devices via RS485 interface:
  - SENTRONIC Modbus RTU Series
- Wi-Fi: Northbound connection or for configuration via a local access point

Main characteristics

- Comprehensive interface set
- CE conformity
- Easy installation and configuration
- Cloud/IoT interface (MQTT 3.1.1)
  - Secure MQTT via TLS
  - Open data format (JSON payload)
- ISO degree of protection IP20 according to IEC 60529

5.4 Device design

The following figure shows the design of the SIMATIC FDE Gateway, with interfaces:



① Socket for connecting a Wi-Fi or BLE antenna
② Ethernet interface X1 P1: TCP/IP interface
③ Ethernet interface X2 P1: TCP/IP interface
④ 14-pin X4 connection terminal
⑤ LED display
⑥ "USER" button
⑦ "RESET" button

Pin overview of X4 connection terminal ④

The pin designations are also printed on the device.

Pin	Short description	Meaning
1	AI	Analog Input
2	2M	Ground analog input
3	1M	Ground digital input
4	DI	Digital input
5	TX/A	Transmission data TxD for RS232 -/A for RS485
6	RX/B	Receive data RxD for RS232 +/B for RS485
7	RTS	RTS for RS485 (not used in current version)
8	RS-G	Signal ground for RS232 and RS485
9	CAN H	CAN (not used in the current version)
10	CAN L	CAN (not used in the current version)
11	DQ	Digital output
12	M	FDE ground (0 V)
13	L+	24V connection for FDE
14		Shield

Note

It is not possible to use RS232 and RS485 at the same time.

5.5 Analog input and digital input/output

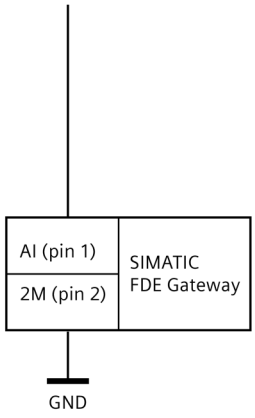
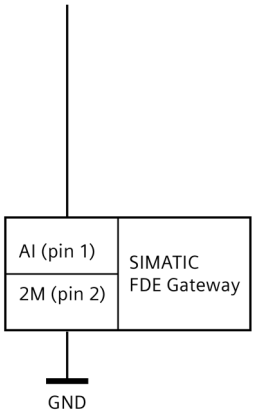
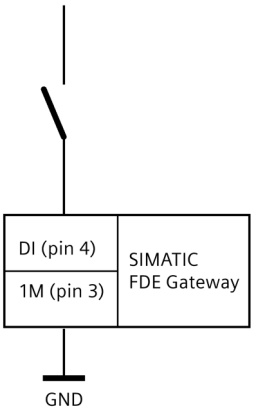
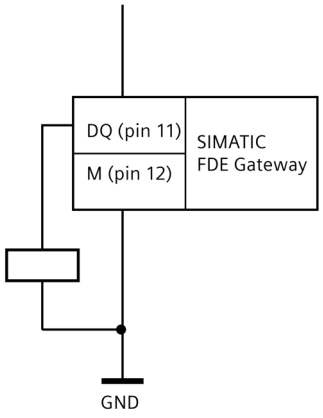
The device supports the following I/O functions:

- Analog input (pins 1-2 of X4 plug)
  - 0 - 10 V DC
  - 0 - 20 mA or 4 - 20 mA
- Digital input 0 - 28.8 V DC, Type III input (pins 4-3 of the X4 plug)
- Digital output 24 V DC, 300 mA (pins 11-12 of the X4 plug)

The functionality depends on the configuration in the web server.

Correct wiring of inputs/outputs

The I/O connection must be connected with circuitry that is intended for the configured behavior. Incorrect wiring can result in a defect of the device.

Analog input	**Analog input**	**Digital input**	**Digital output**
0 - 10 V DC	0 - 20 mA	24 V DC	24 V DC 300 mA
			
		For signal "0" 0 V - 5 V For signal "1" 12 V - 24 V	

For connection to I/O, see section "Connecting interfaces to connecting terminal X4 (Page 29)".

5.6 Operating modes and LED display

LED overview

The SIMATIC FDE Gateway features 10 signal LEDs visible to the user:

LED name	**Driven by**	**Parameter name of the driving application to be watched via MQTT**
PWR	System	N/A
SYS	System	N/A
DQ	DIGITAL_OUTPUT	VALUE
COM	MODBUS_RTU / USS	STATUS
DI	DIGITAL_INPUT	VALUE
ETH1	Networking service of the X1 port TCP/IP and Link layer	N/A
AI	ANALOG_INPUT	IS_VALID
ETH2	Networking service of the X2 port TCP/IP and Link layer	N/A
RF	Networking service of the Wi-Fi TCP/IP and Link layer	N/A
CAN	System	N/A

System LEDs

LED name	Off	Flashes orange	On - green
PWR	Device powered off	Not possible	Device powered on
SYS	After power-on: Booting	• 1 Hz: Configuration mode • 5 Hz: Confirmation after pressing the USER button 5 times (Factory Reset) • One long flash: directly after power-on	RUN mode successfully activated

Connection LEDs

LED name	Off	Flashes orange	On - green
ETH1, ETH2	• Ethernet cable not plugged-in in the corresponding port	• IP address not assigned (the static IP address has not been specified or it could not be obtained from DHCP) • Random internal system error	• None of the conditions for the OFF state or FLASHING state are fulfilled
RF (Wi-Fi)	• Wi-Fi disabled via the configuration page • Wi-Fi enabled, but SSID is empty	• No connection to the selected SSID • IP address not assigned (the static IP address has not been specified or it could not be obtained from DHCP) • Random internal system error	• None of the conditions for the OFF state or FLASHING state are fulfilled

LEDs for specific inputs/outputs

LED name	Off	Flashing	On - green
DQ	• DIGITAL_OUTPUT disabled • VALUE parameter of DIGITAL_OUTPUT app is not set to '1'	Not possible	• VALUE parameter is set to '1'
DI	• DIGITAL_INPUT disabled • VALUE parameter of DIGITAL_INPUT is not set to '1'	Not possible	• VALUE parameter is set to '1'
AI	• ANALOG_INPUT disabled	See the following table	• IS_VALID parameter is set to '1'
COM	• Neither USS nor MODBUS_RTU is enabled	See the following table	• [USS] STATUS parameter is set to '0' or '1' • [MODBUS_RTU] STATUS parameter is set to '1' or '2' or '8'
CAN	• Always OFF (CAN bus not implemented)	Not possible	Not possible

LED name	Flashes orange	Flashes green
AI	Not possible	• IS_VALID parameter is set to '1'
COM	• [USS] STATUS parameter is set neither to '0' nor '1' • [MODBUS_RTU] STATUS parameter is set neither to '1' nor '2' nor '8'	Not possible

Values of driving parameters are accessible via MQTT.

Meaning of parameter values

LED name	Driving function + parameter	Values
COM	USS / MODBUS_RTU / MODBUS_TCP[1]-> STATUS	**USS**: • '-2' (AddressNotAvailable) -> if no target address was specified [LED FLASHING] • '-1' (Invalid) -> function is not running or is frozen [LED FLASHING] • '0' (AllGood) -> reading of all values was successful [LED ON] • '1' (SomeFailed) -> reading of at least one register was successful [LED ON] • '2' (AllFailed) -> reading of all values failed [LED FLASHING] • Other values -> not possible (if present, handled as '2' – [LED FLASHING]) **MODBUS RTU**: • '-8' (UnconfiguredApp) -> one of the following: server ID, baud rate, parity mode, was not specified [LED FLASHING] • '-4' (ModbusClientInitFailed) -> Modbus client could not be initialized [LED FLASHING] • '-2' (SerialBusError) -> serial bus configuration failed [LED FLASHING] • '-1' (Invalid) -> function is not running or is frozen [LED FLASHING] • '0' (InitSuccessful) -> initialization of the corresponding app was successful [LED ON] • '1' (AllGood) -> reading all registers was successful [LED ON] • '2' (SomeFailed) -> reading at least one whole group[2] was successful [LED ON] • '4' (AllFailed) -> reading all registers failed [LED FLASHING] • '8' (NothingToUpdate) -> no register was set for reading [LED ON] • Other values -> not possible (if present, handled as '4' – [LED FLASHING])
DQ	DIGITAL_OUTPUT -> VALUE	• '-1' -> function is not running (handled as '0' – [LED OFF]) • '0' -> logical '0' is written [LED OFF] • '1' -> logical '1' is written [LED ON] • Other values -> not possible (if present, handled as '0' – [LED OFF])

LED name	Driving function + parameter	Values
DI	DIGITAL_INPUT -> VALUE	• '-1' -> function is not running or is frozen (handled as '0' – [LED OFF]) • '1' -> logical '1' is read [LED ON] • '0' -> logical '0' is read [LED OFF] • Other values -> not possible (if present, handled as '0' – [LED OFF])
AI	ANALOG_INPUT -> IS_VALID	• '1' -> read value is valid [LED ON] • '0' -> read value is invalid [LED FLASHING] • Other values -> not possible (if present, handled as '0' – [LED FLASHING])

1) The values for MODBUS_RTU are also applicable for MODBUS_TCP (except '-2').

2) Group means either coils, discrete inputs, holding registers or input registers.

Device identification

The FDE device provides the option of identifying a specific device by LED flashing. This can be enabled on the home page:



If the Flash LED switch is set to "on", the behavior of all LEDs except the SYS and PWR LEDs is overridden by flashing at a frequency of 2 Hz.

5.7 Changing the operating mode

Use the two buttons "USER" and "RESET" or the web user interface to switch between the operating modes:

Target operating mode	Action
RUN	From the web user interface
CONFIGURATION	Press and hold the USER button until the SYS LED starts to flash orange

Note

Pressing the RESET button may result in any unsaved configuration being lost.

5.8 Preparing for installation

1. When accepting a delivery, check the packaging for visible transport damage.
   If there is any transport damage at the time of delivery, make a complaint to the responsible forwarding company.
2. Unpack the device at its installation location.
3. Keep the original packaging in case you need to transport the device again.

   Note

   Damage to the device during transport and storage

   If a device is transported or stored without packaging, then shocks, vibrations, pressure, and moisture may affect the unprotected device. Damaged packaging is an indication that ambient conditions have already had a significant impact on the device.

   The device may be damaged.

   Do not dispose of the original packaging. Be sure to pack the device during transport and storage.

4. Check the contents of the packaging and the accessories for completeness and damage.
   Scope of delivery:

   – Device

   – DC connection terminal (plugged into the device).

5. If the package contents are incomplete or damaged, or do not correspond to your order, please immediately inform the responsible delivery company.

⚠ WARNING

Risk of electric shock and fire due to device damage

A damaged device can carry dangerous voltage and trigger a fire in the machine or plant. A damaged device has unpredictable properties and states.

Death or serious injury can be the result.

Ensure that the damaged device is not installed and commissioned unintentionally. Label the damaged device correspondingly and keep it locked up. Send in the device so that it can be repaired as soon as possible.

NOTICE

Damage caused by condensation

If the device is exposed to low temperatures or extreme fluctuations in temperature (such as during cold weather) during transport, this may cause moisture to build up on or in the device (condensation).

Moisture may cause a short-circuit and damage the device.

To prevent damage to the device, do the following:

Store the device in a dry location.

Let the device warm up to room temperature before commissioning.

Do not expose the device to direct heat radiation from a heater.

If condensation occurs, wait about 12 hours or until the device is completely dry before switching it on.

6. Make a note of the device's identification data.

5.9 Installing the device

5.9.1 Professional installation guide

The device must be installed professionally. The installation must be controlled and requires special training.
The intended use is generally not for the general public. It is generally intended for industrial/commercial use.
The connector is located inside the transmitter enclosure and can only be accessed by disassembling the transmitter that is normally required. The user does not have access to the connector.
The same type of antenna with lower or equal gain as the listed antenna must be used as follows:

External antenna	Frequency (MHz)	Antenna type	MAX. antenna gain (dBi)	Cable loss	Final gain (dBi)
1	2400-2480	vertical monopole omni-antenna	2	-0.53	1.47
	5150-5850	vertical monopole omni-antenna	2	-0.83	1.17

For more details, please visit SIEMENS SiePortal (https://sieportal.siemens.com)

5.9.2 Mounting instructions

- The device is only approved for operation indoors.
- When installing in a control cabinet, observe the SIMATIC installation guidelines (https://support.industry.siemens.com/cs/ww/en/view/1064706) as well as the relevant DIN/VDE regulations or the respective country-specific regulations.

Secure mounting

Open device must be installed in a cabinet or appropriate enclosure. The device is mounted on horizontal or vertical DIN rails with 35 mm DIN.

Distances

Position the device so that it can be easily separated and removed.

Ensure that the following clearances to other components or enclosure walls are complied with:

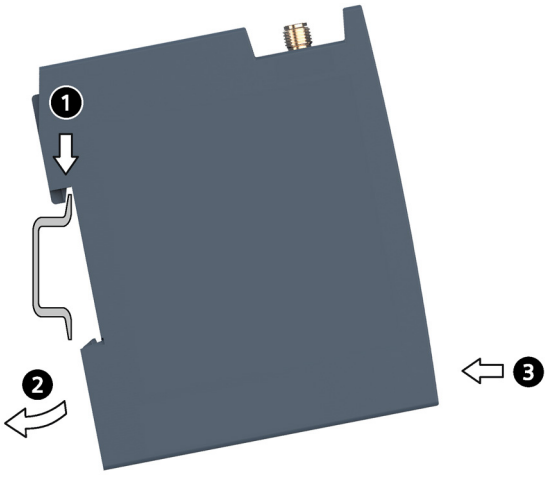
- Below the device: ≥ 50 mm
- Above the device: ≥ 50 mm

5.9.3 DIN-rail mounting

Mounting

Requirement

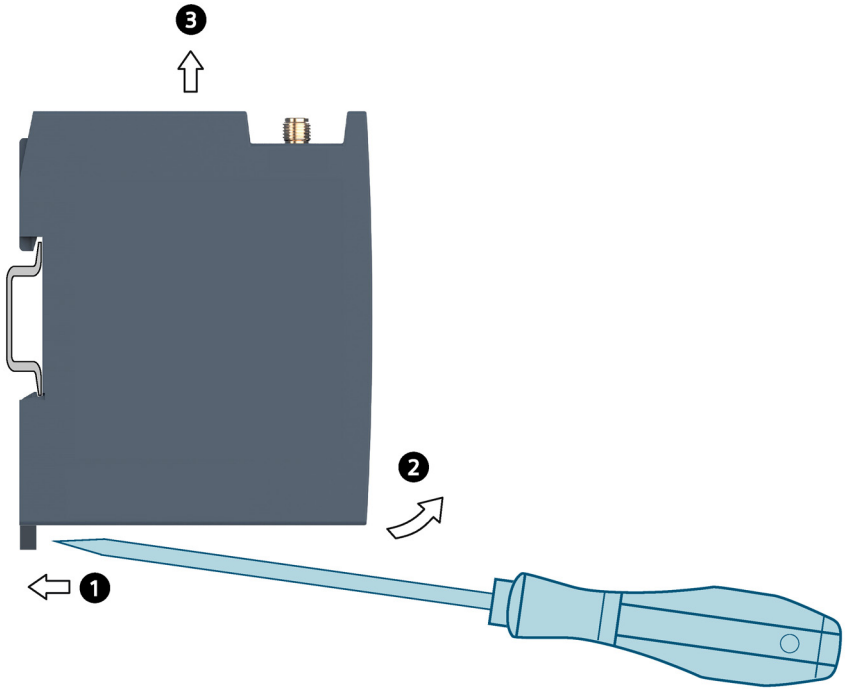
One 35 mm standard profile DIN rail is mounted at the installation location.



Process

1. Place the device with the rail clamp at the marked position on the upper edge of the DIN rail. Press the device downwards.
2. Swivel the rail clamp of the device from below over the DIN rail.
3. Press the device towards the DIN rail. Press the DIN rail clamp in so that the device is firmly seated on the rail.

Removal



Process

1. Use a slotted screwdriver to pull the lower DIN rail clamp on the back of the device down to the extended position. This will release the unit from the rail.
2. Swivel the device away from the DIN rail.
3. Move the device upward and remove it.

5.10 Connecting the device

5.10.1 Notes for connecting

⚠ WARNING

Danger caused by lightning

Lightning can enter power and data transmission cables and jump over to a person.

Lightning can cause death, serious physical injury, and burns.

Take the following precautionary measures:

- If a thunderstorm is approaching, disconnect the device from the electricity supply network in good time.
- Do not touch power or transmission cables during a storm.
- Maintain sufficient distance from electrical cables, distributors, systems, etc.

NOTICE

Malfunctions caused by I/O devices

The connection of I/O devices can lead to devices malfunctioning.

Injury to persons and damage to the machine or plant may result.

Take the following into account when connecting I/O devices:

- Read the documentation related to the I/O devices. Follow all instructions given in the documentation.
- Only connect peripheral devices which are suitable for use in industrial environments according to EN 61000-6-2 and IEC 61000-6-2.
- Non-hot-pluggable I/O devices may only be connected when the device power supply is switched off.

NOTICE

Damage caused by feedback

Regenerative feedback of voltage to ground by a connected or installed component can damage the device.

Connected or installed peripherals must not introduce any voltage into the device. Regenerative feedback is generally not permitted.

5.10.2 Connecting interfaces to connecting terminal X4

Connection capacity

Various types of interfaces can be connected to the device via the X4 terminal. The pin overview is described in the section "Design of the device (Page 17)".

The following aspects must be taken into account:

Conductor type	Minimum cross-section	Maximum cross-section
Solid conductor	0.14 mm² (AWG26)	0.5 mm² (AWG20)
Flexible conductor without end sleeve	0.14 mm²	0.5 mm²
Flexible conductor with ferrules, without plastic sleeve	0.14 mm²	0.5 mm²
Flexible conductor with ferrules, with plastic sleeve	0.14 mm²	0.5 mm²

The maximum length of cables to be connected to X4 is 8 m.

Note

Shielded cables

If cables with a shield are used, the shields must be connected to a ground connection in the system in which the device is used. This is in order to ensure EMC and EMI compatibility.

Connecting an interface

Requirement

- Use the supplied plug connector.
- Use cables which have the supported connection capacity.
- Use slotted screwdrivers with a 3-mm blade.

Process

1. Switch off the power supply.
2. Identify the connections of the interface to be connected.
3. Connect all cables to the correct terminal sockets
4. Plug the connector in.
5. Switch on the power supply unit.

5.10.3 Connecting the power supply

The SITOP device 24 V/0.6 A (6EP3330-6SB00-0AY0) is intended for the power supply. Connect the power supply to the 14-pin X4 terminal on the front of the device.

Note

The device may only be connected to a 24 V DC power supply that meets the requirements for safety extra-low voltage (SELV) according to IEC/EN/DIN EN/UL 61010-1.

Note

The power supply must be adjusted to match the connected loads of the device, see "Technical specifications".

In case of voltage peaks on the power supply lines, protective devices in the form of a varistor (MOV) UMOV = U-nom. x 1.2 (BLITZDUCTOR BVT AVD 24 (918 422) or equivalent) must be used.

Requirement

- Use the connection terminal included in the scope of delivery.
- Use a two-wire cable with a cross-section of 0.75 mm^2 to 2.5 mm^2.
- Use slotted screwdrivers with a 3-mm blade.

Process

1. Switch off the power supply.
2. Connect the wires from the SITOP device to pins 12 and 13 of the 14-pin X4 terminal block.
3. Connect the wires to the SITOP power supply connection.

5.10.4 Securing cables

To ensure strain relief, use cable ties or cable clamps to secure the connected cables to suitable fixing elements.

Make sure that the cables are not pinched by cable ties or cable clamps.

5.10.5 Connecting a device to the RS232 interface

Connect the device to pins 5-6 and 8 of the X4 terminal.

You can connect a SIMATIC FDE Gateway to one of the following converters via the RS232 interface on the converter-specific module or control device:

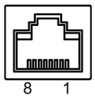
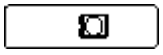
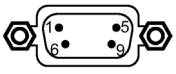
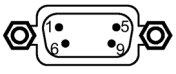
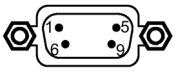
- SINAMICS V20
- SINAMICS G110M
- SINAMICS G120 series (except G120D)
- MICROMASTER 420/430/440

The data transmission takes place via the signals "RS232 TXD" and "RS232 RXD". The third "GND" insulated conductor is used as a shared ground potential.

Interface assignment (converter side)

The RXD signal must be connected to the TXD socket on the X4 terminal.

The TXD signal must be connected to the RXD socket on the X4 terminal.

Converter	RS232 interface	Pin number	Signal name	Pin number FDE Gateway page	Description
BOP interface module for SINAMICS V20 [1]		1	RXD	TX/A (pin 5)	Receive data
		2	TXD	RX/B (pin 6)	Transmit data
		3	GND	RS_G (pin 8)	Signal ground
Power unit for SINAMICS G110M	Optical I/O port interface [2]  RS232 interface of the fiber-optic cable [2] 	2	RXD	TX/A (pin 5)	Receive data
		3	TXD	RX/B (pin 6)	Transmit data
		5	GND	RS_G (pin 8)	Signal ground
Control device for SINAMICS G120 series (except G120D)		2	RXD	TX/A (pin 5)	Receive data
		3	TXD	RX/B (pin 6)	Transmit data
		5	GND	RS_G (pin 8)	Signal ground
PC converter connection module for MICROMASTER 420/430/440		2	RXD	TX/A (pin 5)	Receive data
		3	TXD	RX/B (pin 6)	Transmit data
		5	GND	RS_G (pin 8)	Signal ground

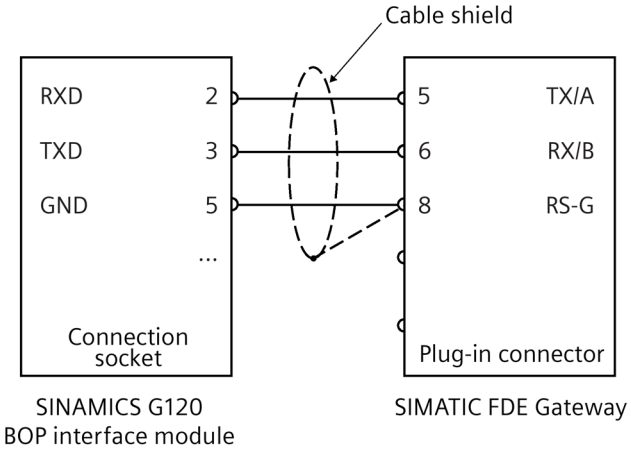
1) MLFB: 6SL3255-0VA00-2AA1

2) Connect the optical cable (article number: 3RK1922-2BP00) with the optical I/O port interface on the power unit for the RS232 communication.

More information on the BOP Interface Module can be found in the Catalog (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6SL3255-0VA00-2AA1) and in the Product information (https://support.industry.siemens.com/cs/ww/de/view/109773863/en).

Wiring example

The following example from the SINAMICS G120 series shows the wiring between the converter and the SIMATIC FDE Gateway.



Cable shield grounding:
RS232 serial cable should be shielded. The shield should be connected to functional grounding at one end of the cable at least.
GND cable grounding:
Many masters do not have a shared connection. If this is the case, the RS232 ground should reference the same functional grounding as the master (at a single point). If the master has a shared connection, then the shared connection is connected with it and not connected to the functional grounding.

Note

When connecting the converter consider the following in order to achieve better EMC behavior:

- Use a shielded cable for RS232 communication between the converter and the device.
- Route the signal cable and the electric power cable separately in different cable ducts.

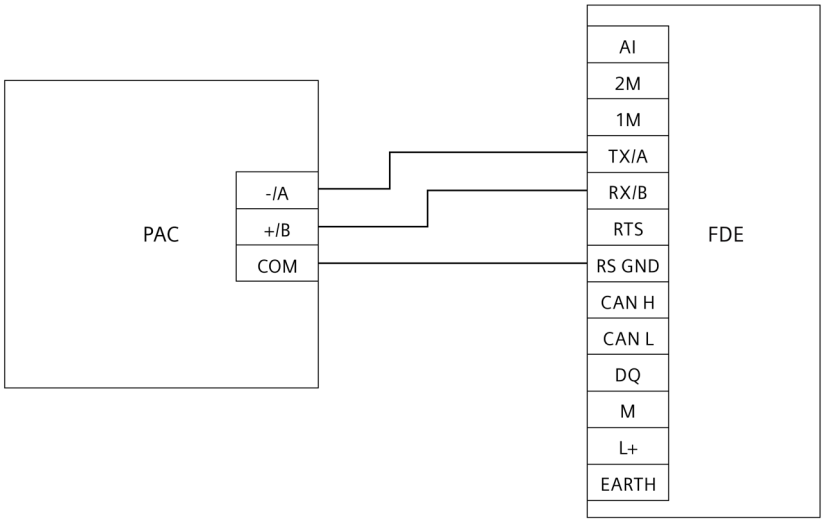
Note

It is not possible to use RS232 and RS485 at the same time.

5.10.6 Connecting a device to the RS485 interface

Connect the device to pins 5-7 of the X4 terminal.

A typical PAC connection to the FDE Gateway looks like this:



Note

The labelling of the RS 485 device connections is not fully standardized.

The "A on A and B on B" rule only applies as long as the same device types are present in a communications line. If there is a mixture of device types, this must be considered individually for each type.

Terminating resistor

The FDE Gateway terminates the RS485 with an internal 120 ohm resistor. This termination cannot be deactivated.

Note

It is not possible to use RS232 and RS485 at the same time.

Software and commissioning

6

6.1 Establishing a connection to the device

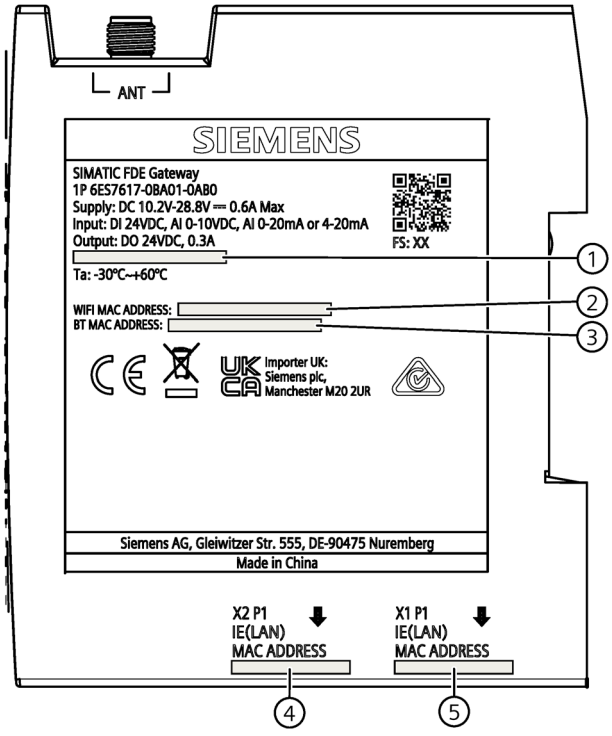
The device starts automatically as soon as power is supplied.

The device configuration is carried out via the device web interface.

Connect to the access point fde_gateway_xxxxxx using Wi-Fi and open the page https://192.168.4.1.

Obtaining the login information from the nameplate of the device

Refer to the data on the nameplate for the login information:



① Serial number
② Wi-Fi MAC address
③ BT MAC address
④ X2 P1 MAC address
⑤ X1 P1 MAC address

The serial number ①, Wi-Fi MAC address ②, BT MAC address ③ and the two IE MAC addresses ④, ⑤ are specific to each device.

Use the last 6 digits of the Wi-Fi MAC address ② for the SSID:

SSID = fde_gateway_[last 6 digits of the Wi-Fi MAC address]

Use the SSID with the underscores replaced by hyphens as the host name.

Use the serial number ① as the password.

Note

In the serial number field of the housing, the number begins with an identification mark "S". The serial number starts with the next character after "S".

Example:

Serial number V-R5A11111

Wi-Fi MAC address: 10:df:fc:10:c8:b2

SSID: fde_gateway_10c8b2

Host name: fde-gateway-10c8b2

Password: V-R5A11111

TLS certificates

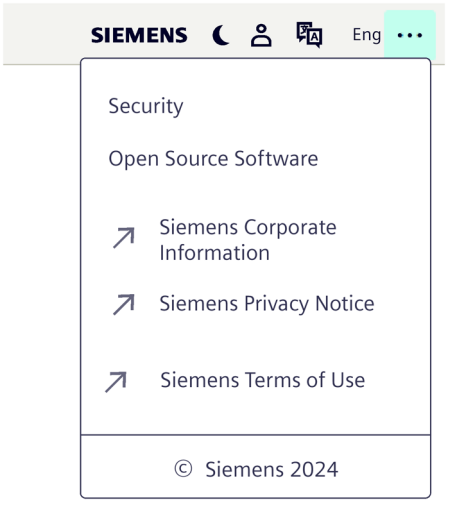
By default, the device comes with a preinstalled certificate from Siemens. This certificate provides a basic level of security, primarily for initial installation. For long-term usage and the best level of security, it is recommended that you replace the certificate with your own certificate signed by your own certificate authority.

If a user-defined trusted certificate authority is used, it is possible to import it as a trusted root certificate authority into the client system. However, this action is only considered secure if you are absolutely sure that your private key is kept securely and there is no suspicion that it has been compromised.

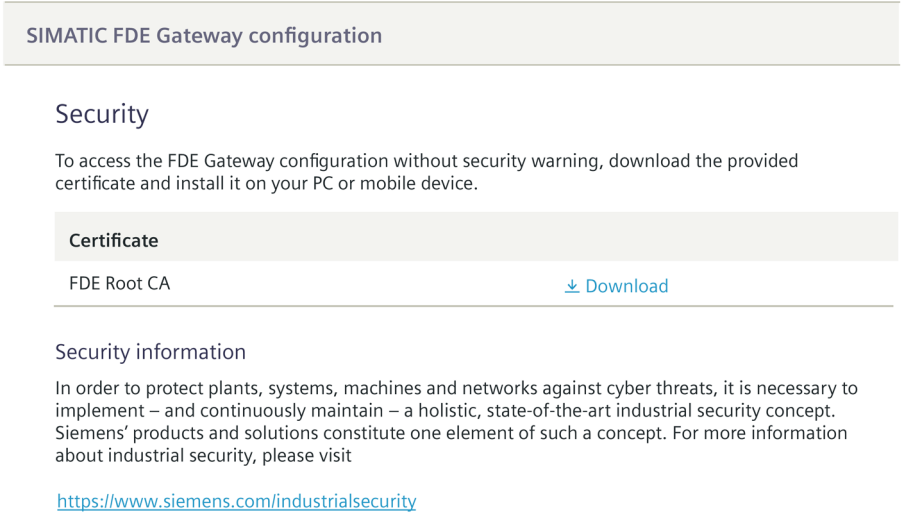
If the certificate authority is compromised, it must be immediately removed from the trust of the client computer, otherwise it could later be used to deliver harmful code to the computer/mobile device or steal personal user data.

Downloading the certificate of the configuration page

1. Click "..." in the upper bar.
   A popup window is displayed:



2. Select "Security".
   Information about the option to download the FDE-Root-CA security certificate is displayed:



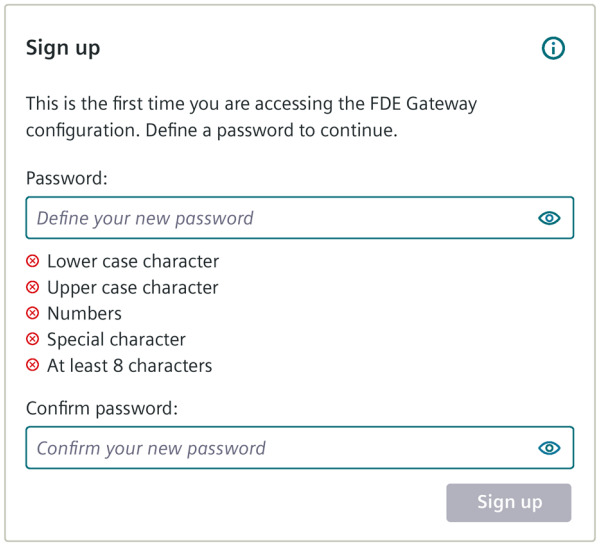
3. Download the FDE Root CA certificate.

First logon

The first time you log in, a registration window is displayed, prompting you to define a password:

Passwords used for all user accounts of the device should always be treated like any other business-related passwords. Observe the following rules:

- The AC password should be long enough and difficult to guess. Recommended minimum password length is at least 8 - 10 characters. It should contain upper and lower case letters, numbers and special characters.
- Always follow the need-to-know principle. Only share the user password with people who need to modify the configuration of the device.
- Avoid using password stickers to remember the password. If a password needs to be recorded, use a Password Manager tool to keep it safe.

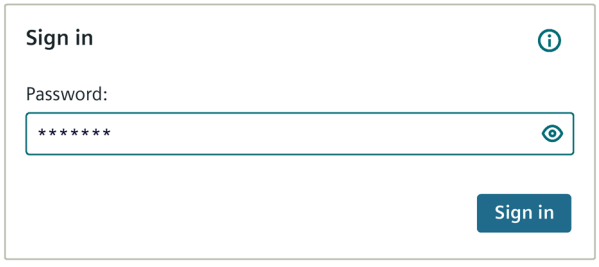


Choose a password and enter it twice in the form. Keep your password safe.

Click "Sign in". After successful registration, you can connect to the device using your password. If the password is lost, the device has to be reset and reconfigured.

6.2 Device configuration

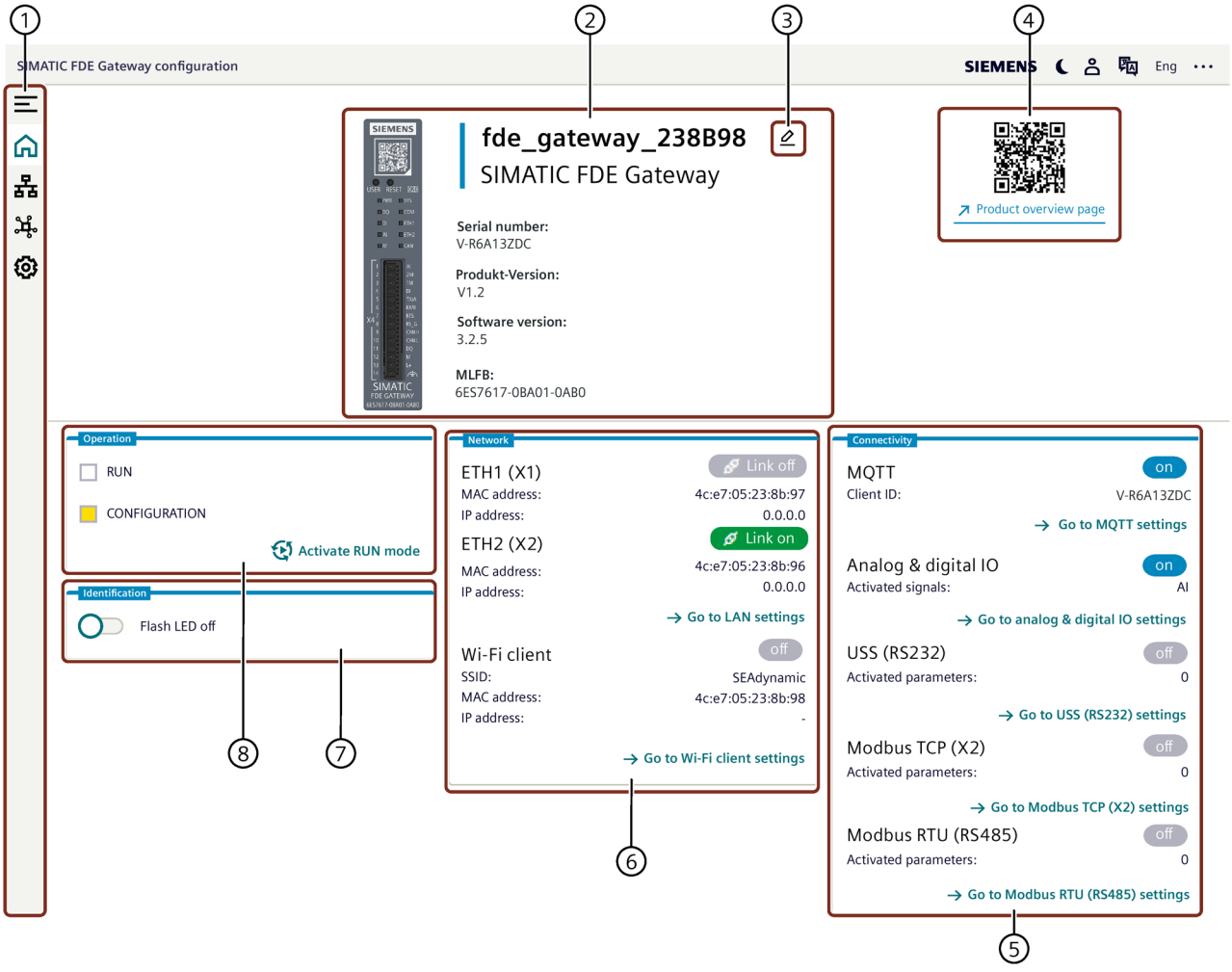
Log on to the device by entering your password:



The start page appears.

Start page

The start page provides information on the device and its current settings.



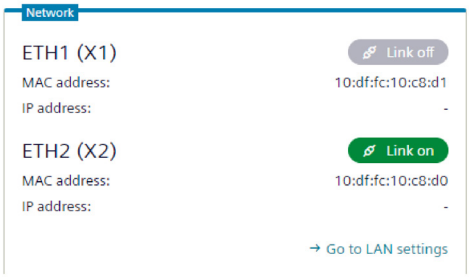
① Menu
② Information about the device
③ Change of device name
④ QR Code + Link to product overview page
⑤ Connectivity settings
⑥ Network settings with LAN diagnostics
⑦ Device identification - Flash LED off/on
⑧ Operating mode setting

LAN diagnostics

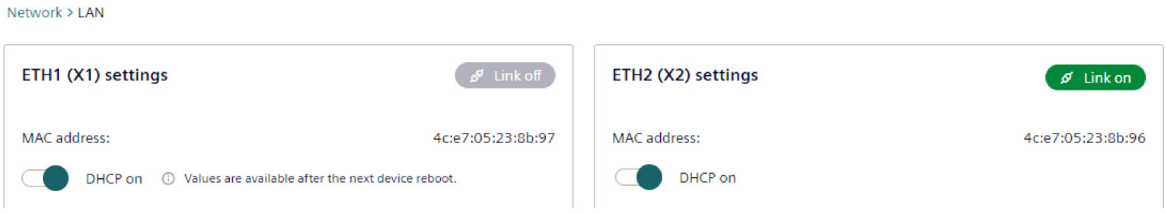
LAN diagnostics is used to monitor the physical Ethernet connection (connected cable) and verify the ability to establish a TCP connection to the desired target socket.

The component that displays the status of the physical connection for each specific Ethernet interface (ETH1 and ETH2) is located in the following places:

- In the Network group box on the home page



- On the LAN settings page



The component that displays the status of the physical connection of the Ethernet cable responds to changes within a few seconds.

Selecting the color theme and language

There are three icons in the top bar of the application:



Use the icon to activate dark mode.

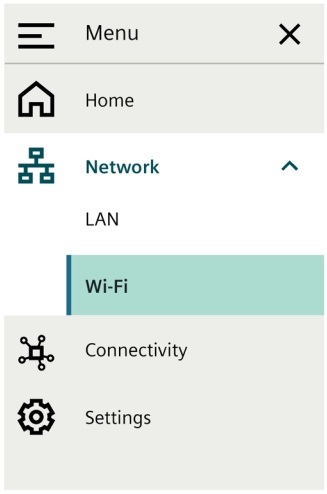
The icon takes you to the user information. Here you can change the password or log out.

Switch the language of the user interface with the icon.

6.3 Network settings

The data from the brownfield level is acquired via digital or analog input, USS (RS232), Modbus TCP (X2) or Modbus RTU (RS485). This data is then transferred to Northbound via LAN or Wi-Fi.

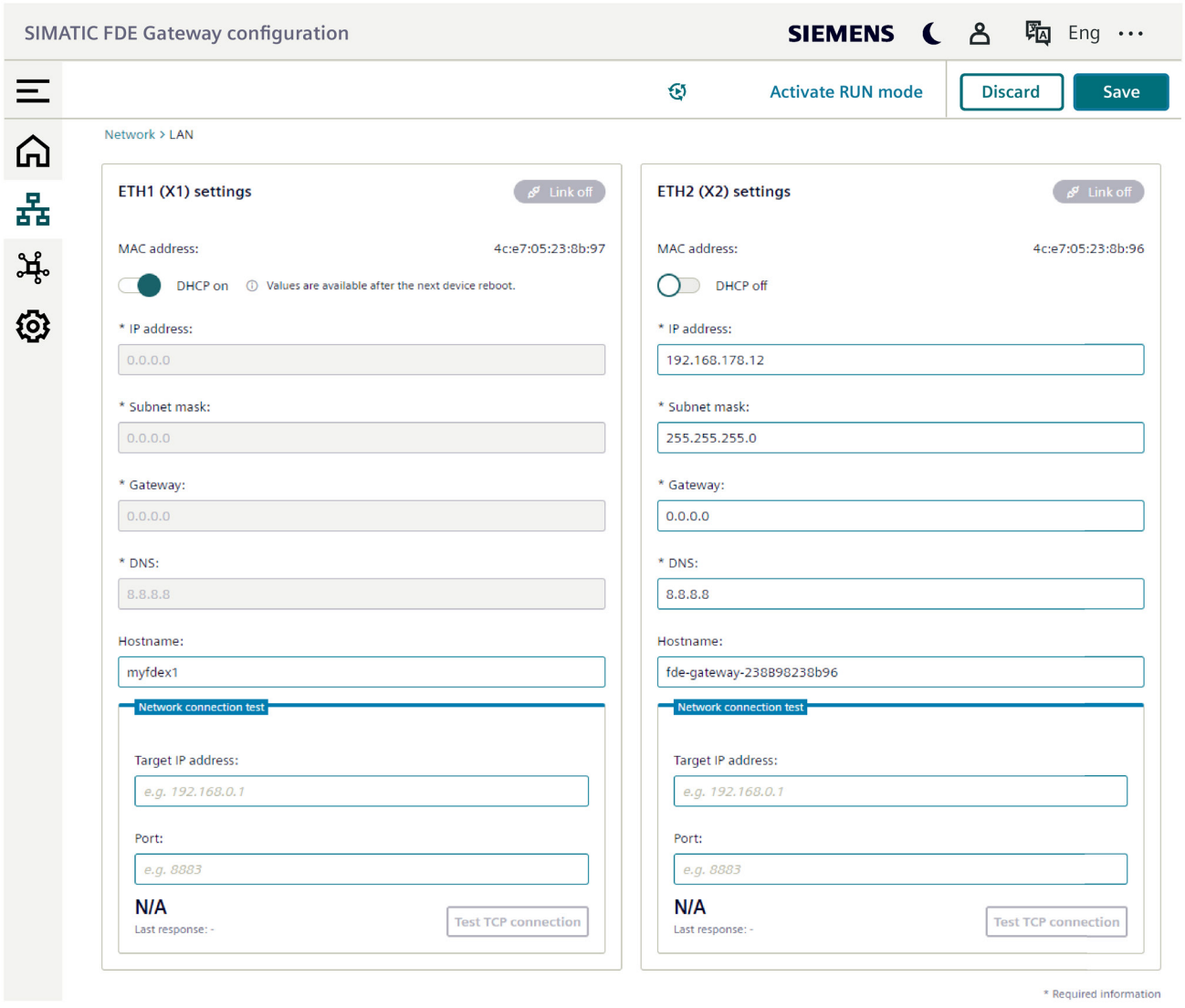
Under Network settings, set the parameters for the two Industrial Ethernet ports and for the Wi-Fi connection.



LAN settings

Open the LAN tab. There are two ways to provide the IP address:

- **Manually:** The parameters are entered manually and, if necessary, coordinated with the network administrator. The lines with asterisks must be completed.
  - The toggle button for enabling the automatic setting is set to off.
  - Fill in the "**IP address**" field with the address for ETH1 (X1).
  - Complete the fields "**Subnet mask**", "**Gateway**" and "**DNS**".
  - Save the configuration by clicking the "Save" button in the upper right corner.



- **Automatically** - DHCP on: The addresses are assigned to the gateway via DHCP (Dynamic Host Configuration Protocol).
  - Move the switch to the "on" position.
  - Save the configuration by clicking the "Save" button in the upper right corner.

Note

The settings are only applied after a restart.

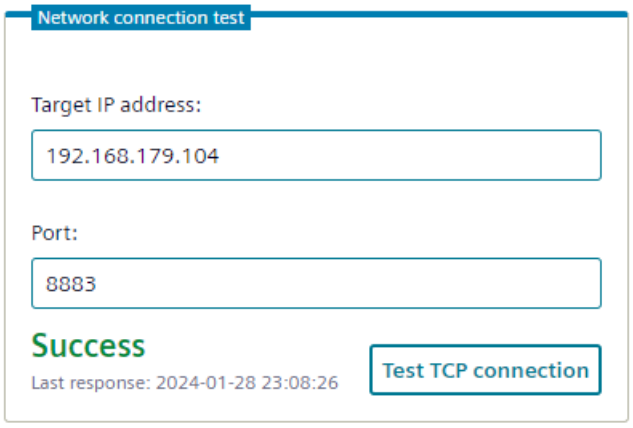
Network connection test

Note

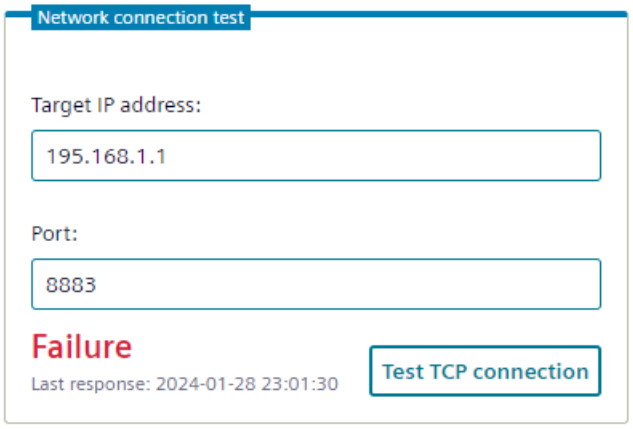
The connection test is designed to test the ability to create a TCP connection, so it is not a ping-like test.

Enter the target IP address and port and click "Test TCP connection".

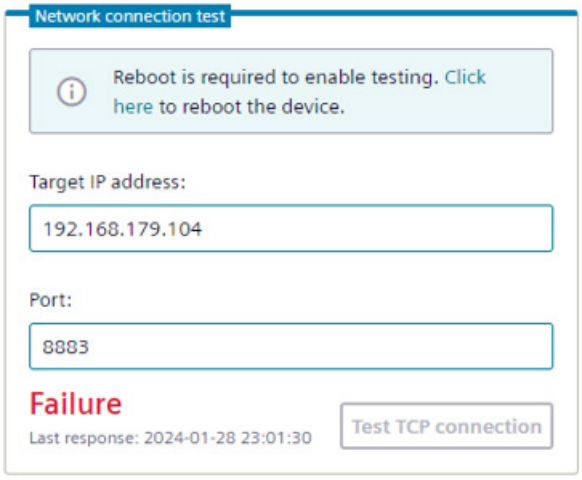
If the connection was successfully established, the label "Success" is displayed, and the label "Last response" is updated:



If the connection is not established, the label "Failure" is displayed, and the label "Last response" is updated:



If there is a change in the ETH interface settings, a contextual help with the link for rebooting within the configuration mode is displayed:

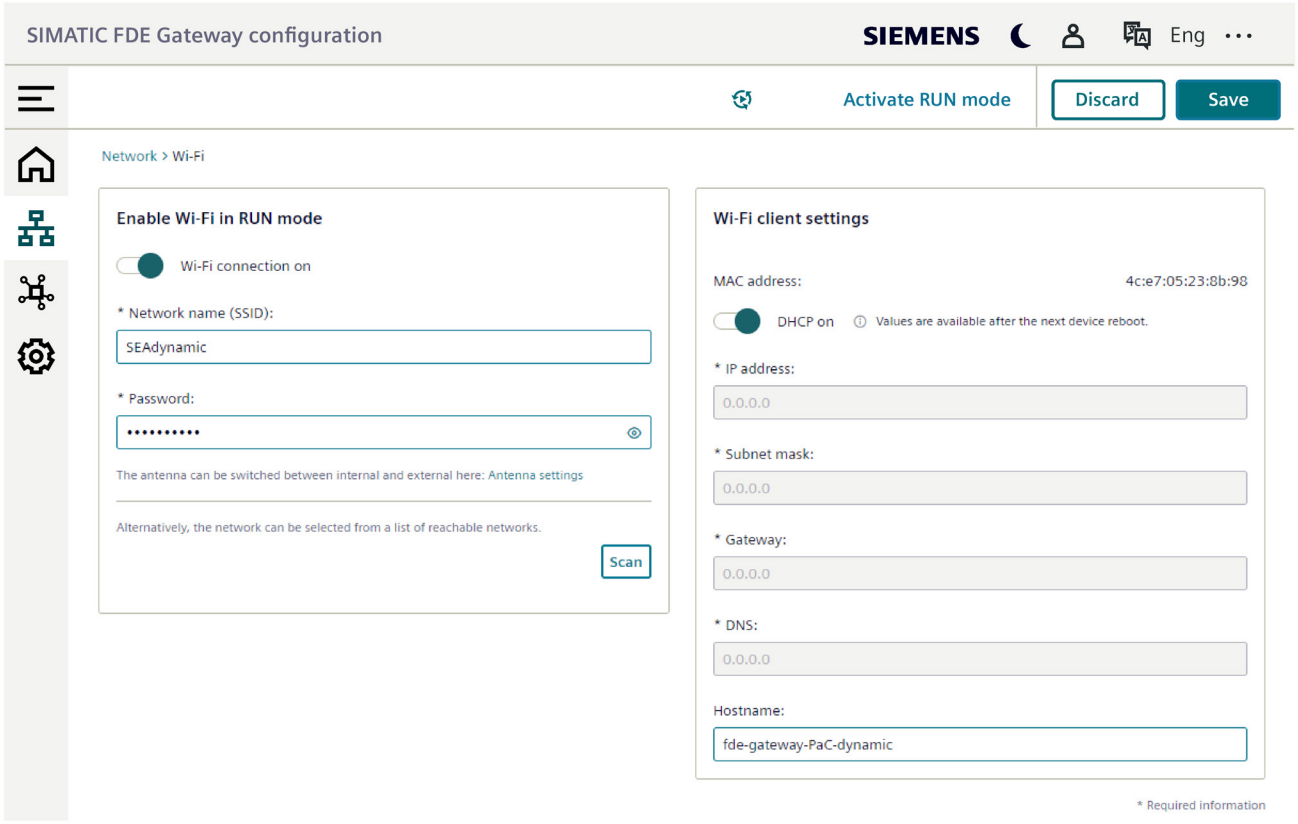


Wi-Fi settings

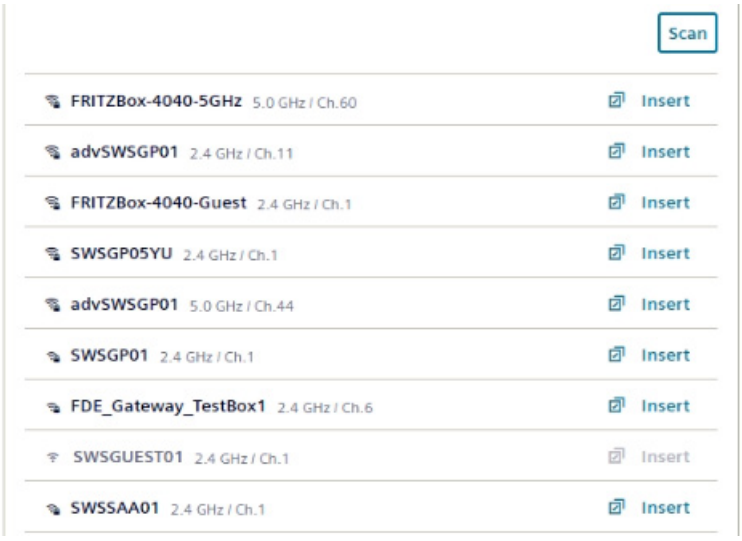
You can configure the Northbound interface under Wi-Fi.

If you want to use an external Wi-Fi antenna, first adjust the basic settings as described in section "Antenna settings (Page 78)".

Switch on the Wi-Fi connection.



Fill in the parameters "Network name (SSID)" and "Password" or use the "Scan" button and select a network from the available options. The detected networks are sorted in descending order by signal strength:



Next to the SSID of the found network is information about the frequency and the specific channel on which the network operates.

In the right column, there is an icon that indicates network security. The "Insert" button to copy the SSID to the "Network name" field is disabled when the network is unsecured.

Once you have selected the network, complete the settings for the **Wi-Fi client**.

There are two ways to provide the IP address:

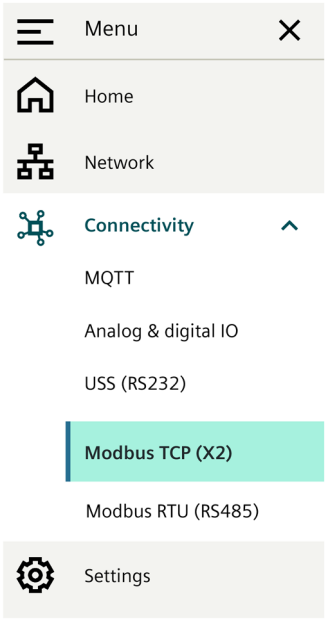
- **Manually:** The parameters are entered manually and, if necessary, coordinated with the network administrator. The lines with asterisks must be completed.
  - The toggle button for enabling the automatic setting is set to off.
  - Fill in the "**IP address**" field.
  - Complete the fields "**Subnet mask**", "**Gateway**" and "**DNS**".
  - Save the configuration by clicking the "Save" button in the upper right corner.
- **Automatically** - DHCP on: The addresses are assigned to the gateway via DHCP (Dynamic Host Configuration Protocol).
  - Move the switch to the "on" position.
  - Save the configuration by clicking the "Save" button in the upper right corner.

The connection to a cloud/Internet connection can be set.

6.4 Connectivity settings

You can set the following functionalities under Connectivity:

- MQTT configuration
- Analog or digital input and digital output
- USS (RS232)
- Modbus TCP (X2)
- Modbus RTU (RS485)



6.4.1 MQTT settings

MQTT broker configuration

The configuration of the MQTT broker service goes beyond the intended content of this document. The user system can implement the service in many ways. However, an improper (insecure) configuration of the broker or a compromise of the broker can cause all collected data to become false and unusable.

To minimize the risk of this happening, the following rules must be followed to make the system stable and secure:

- The broker's operating system and all applications used to access the devices on the network should be kept up-to-date and configured according to the provider's recommendations (e.g. Microsoft in the case of a Windows operating system). Always use a manufacturer-supported version of the operating system to receive security updates. Do not use an outdated operating system or outdated applications, especially if the computer is connected to the network.
- Only a minimum set of necessary applications should be installed on the broker system.
- The broker configuration should only enable features that are necessary for the use case.

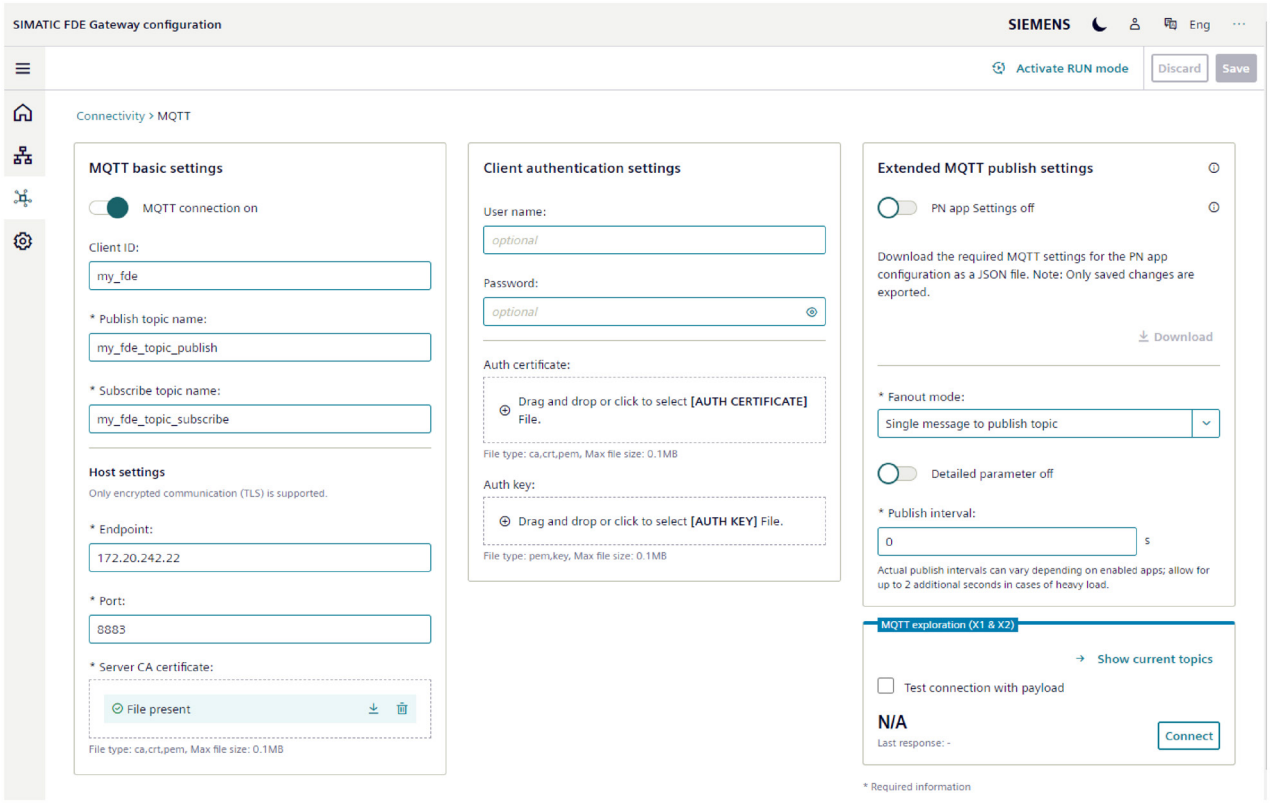
Proven methods

The following tips can improve a broker's security:

1. Install the broker on a trusted hardware or virtual machine. Otherwise, there is a significant risk of a backdoor being introduced into the system.
2. Make sure the broker is not reachable over the internet. Otherwise, the broker will be exposed to potential attackers from anywhere.
3. Disable anonymous access to the broker. Otherwise, any device on the network that can communicate via MQTT can send arbitrary data to the broker and overwrite valid data stored in topics.
4. Allow only TLS connections and disable insecure connections. Otherwise, an attacker can change data during the transition between client and broker.
5. Configure the Access Control List (ACL) so that clients can only publish to their own topics and have no influence on others. Otherwise, any device will be able to access a topic dedicated to another device.
6. Make sure that each client has a different certificate. Otherwise, the broker will not be able to differentiate between clients and to apply the ACL correctly.
7. Revoke access for removed devices. Otherwise, the attacker could use the discarded device to corrupt data on the broker with data at will.

MQTT basic settings

Open the MQTT tab.



Switch on the "MQTT connection on".

Fill in the parameters for the MQTT basic setting:

- **Client ID:** MQTT client identifier at MQTT broker
- **Publish topic name:** The main topic through which data is published
- **Subscribe topic name:** Payloads in JSON format can be sent to the FDE Gateway via this topic
- **Endpoint:** The IP address or the host name of the MQTT broker
- **Port:** The TCP port of the MQTT broker application
- **Server CA certificate:** Public certificate from the Certificate Authority (e.g. ca.crt)

For optional authentication of the client, you can use user name and password and/or certificates.

Note

FDE Gateway only supports secured communication with the MQTT broker over TLS (Transport Layer Security) and requires a server certificate.

Extended MQTT publish settings

The FDE Gateway allows the export of MQTT settings to configure the "Field Data Enabler PN for Linux" application. This app enables data mapping at the operator's network layer using an OPC UA server for IT connectivity.

To enable the "Download" link, save a valid MQTT configuration and set the "PN app Settings" switch to "on". Clicking the enabled "Download" link downloads the configuration as a JSON file.

You can set **Fanout mode** and the publish interval to suit your requirements:

Setting of the topic subdivision in the MQTT payload. Choose one of the three options from the drop-down menu:

- **Single message to publish topic**
  Current values are sent in a single message via the publish topic.
- **One message for each interface as subtopic**
  Current values are sent in different topics. These are subordinate to the publish topic.
- **One message for each parameter as subtopic**
  Current values are sent in different topics. The parameters are also divided into different topics. These are subordinate to the publish topic.

Detailed parameter: Sets whether the data type is also displayed for each parameter.

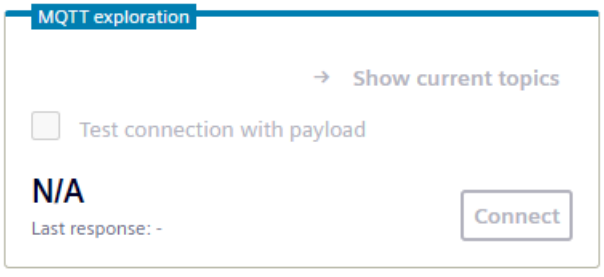
Publish interval: Setting for the time period in which the MQTT payloads are published to the MQTT broker via the publish topics. With a value of 0, the data is sent as fast as possible. Other times can be set, e.g. 5 s, 10 s, etc. The maximum publish interval is 86400 seconds.

For all these cases, the observed times can vary depending on apps enabled / data volume - for example, with a publish interval of 0, the actual publish interval can be up to 2 seconds in cases of heavy device load.

You can find more examples of payloads with parameters in the section "MQTT payload examples (Page 70)".

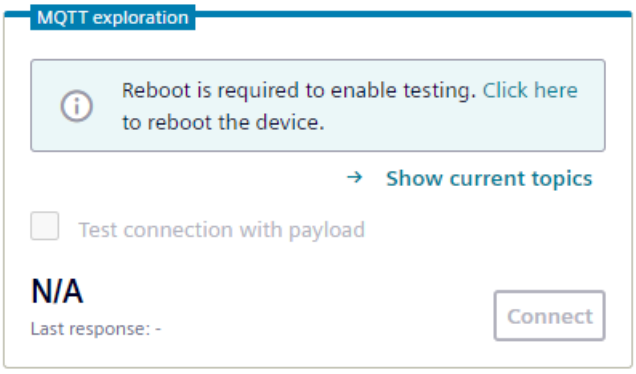
MQTT diagnostics

If the MQTT is "off" or in an unsaved state, the "MQTT exploration" is in a disabled state:



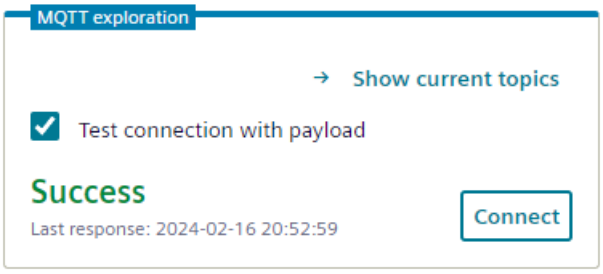
If valid MQTT settings have been saved, MQTT is "on" and there is a change in the ETH configuration, the "Show current topics" link is enabled.

If there is a saved change in the ETH configuration, a contextual help with a prompt to reboot is displayed:

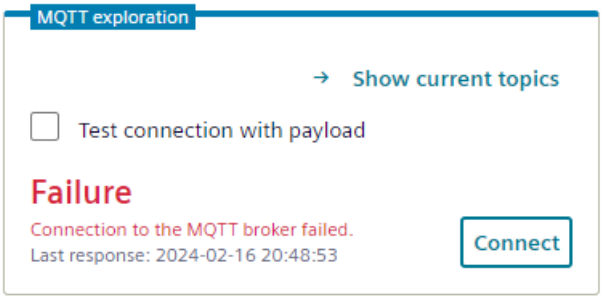


All diagnostic controls are enabled if the MQTT setting is saved, MQTT is "on" and there is no change in the ETH configuration.

After clicking the "Connect" button, a "Success" result is displayed if a successful connection to the MQTT broker is established according to the current settings.



An error message "Failure" is displayed if an error occurs during the MQTT broker connection diagnostics.

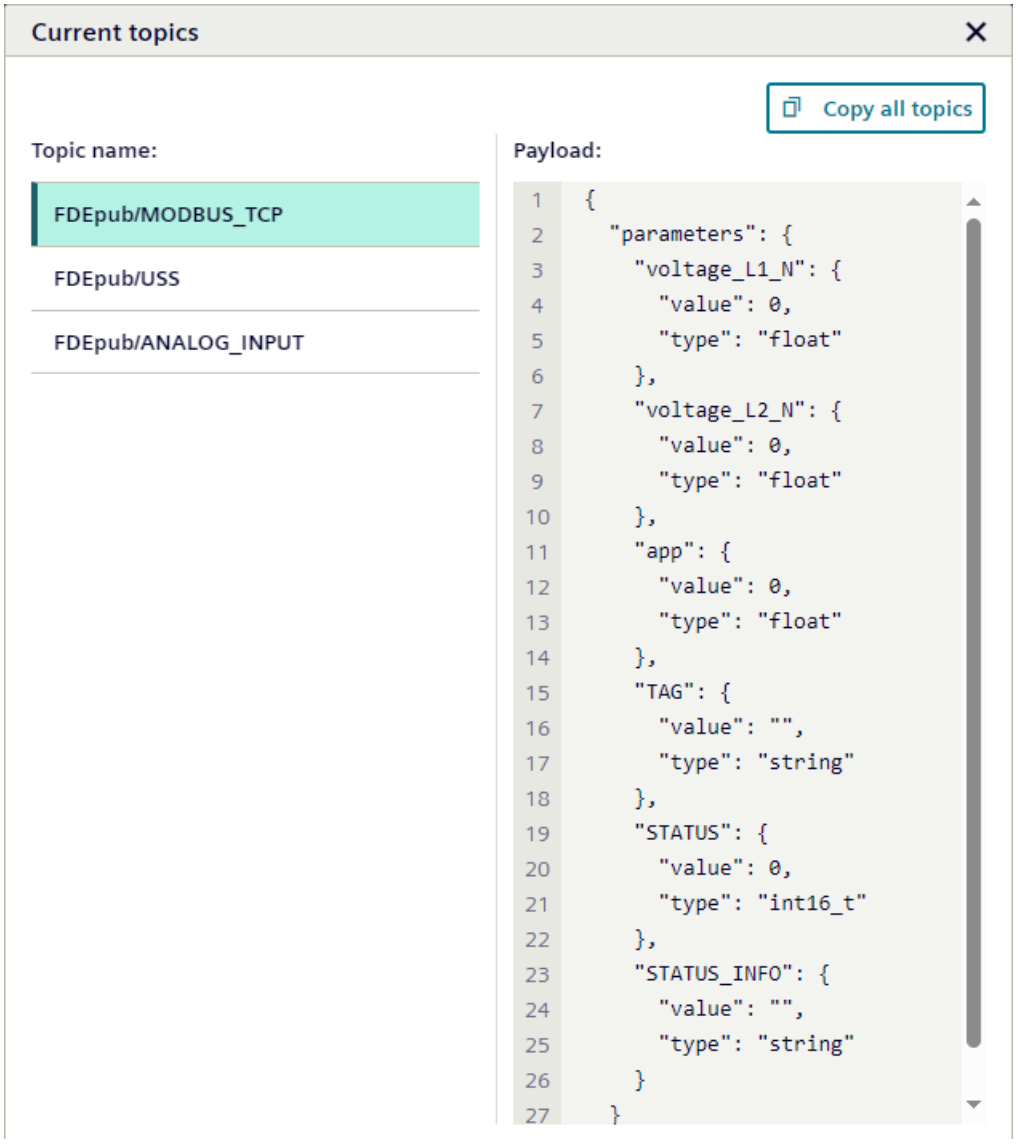


In cases where it is possible to determine the origin of the error based on the current MQTT configuration, additional information regarding the failure is displayed. This applies to the following cases:

- No physical connection: No physical ETH connections detected.
- Connection failed: TCP connection test to MQTT broker failed.
- Certificate failed: At least one of the certificates or authentication key is invalid.
- Client authentication failed: The username or password does not match.

If the "Test connection with payload" checkbox is selected, the test will be performed with the current payload corresponding to the currently active applications.

Clicking the "Show current topics" button displays a dialog box containing a list of all active topics and a preview of the payload for the selected topic (topic names and payload format correspond to the currently enabled applications and the fanout mode configuration, as well as the status of the configuration of detailed parameters).



All parameter values in the topic payload preview are set to their default values, even if diagnostics for the respective topic have been performed previously, namely:

- Value of type string = ""
- Value of type number = 0
- Value of type boolean = false

Clicking the "Copy all topics" button in the "Current topics" dialog window copies all active topics with payloads to the clipboard in JSON format.

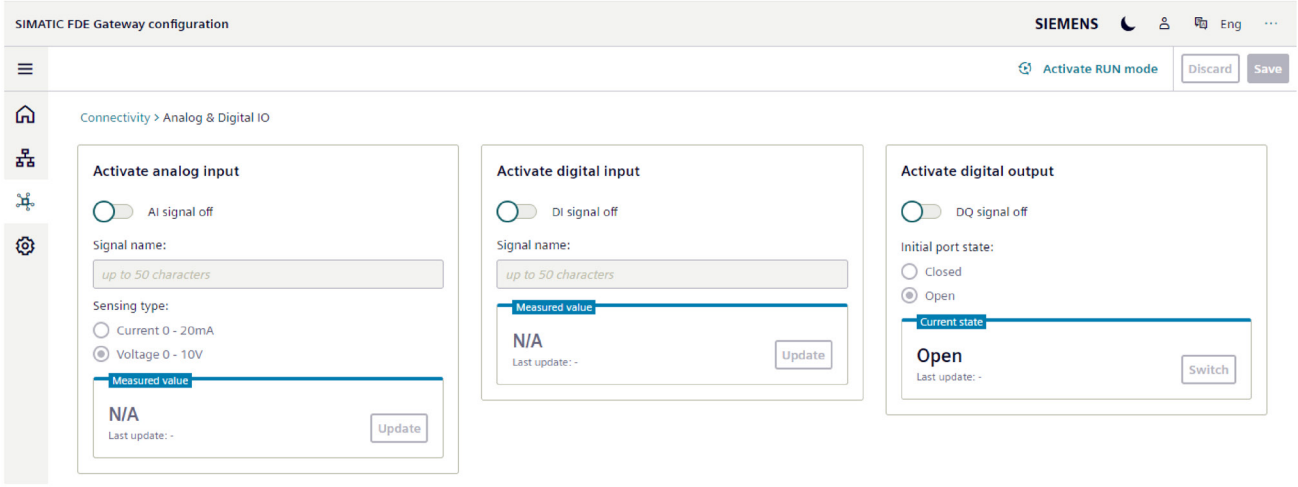
Example content for the "Single message to publish" topic and "Detailed parameter off":


```
[
  {
    "topic": "FDEpub",
    "payload": [
      {
        "app": "MODBUS_TCP",
        "parameters": {
          "voltage_L1_N": 0,
          "voltage_L2_N": 0,
          "app": 0,
          "TAG": "",
          "STATUS": 0,
          "STATUS_INFO": ""
        }
      },
      {
        "app": "ANALOG_INPUT",
        "parameters": {
          "TAG": "",
          "RAW_VALUE": 0,
          "MA_VALUE": 0,
          "MV_VALUE": 0,
          "IS_VALID": 0
        }
      }
    ]
  }
]
```

6.4.2 Enable analog & digital input and digital output

Parameters of the analog and digital input and the digital output can be set in the "Analog & Digital IO" tab.

Correct wiring of inputs and the output is described in the section "Analog input and digital input/output (Page 18)".



Activate analog input

Set the switch to "on".

Enter the signal name.

Select the desired measurement type (current 0 - 20 mA or voltage 0 - 10 V).

Activate digital input

Set the switch to "on".

Enter the signal name.

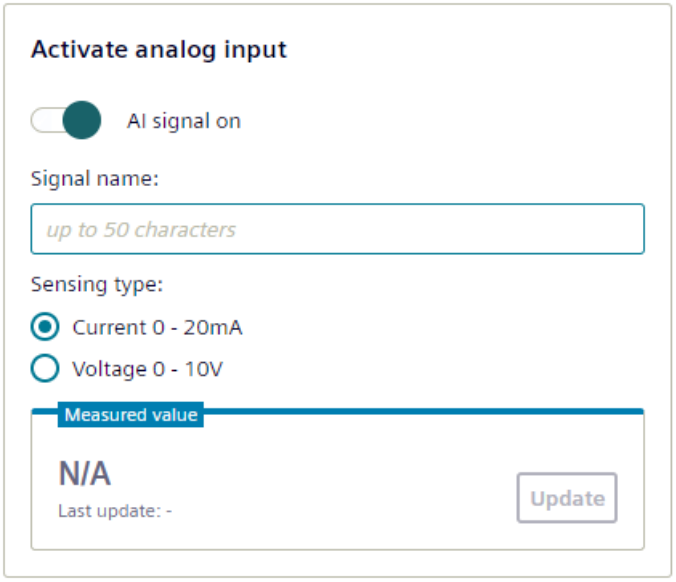
Activate digital output

Set the switch to "on".

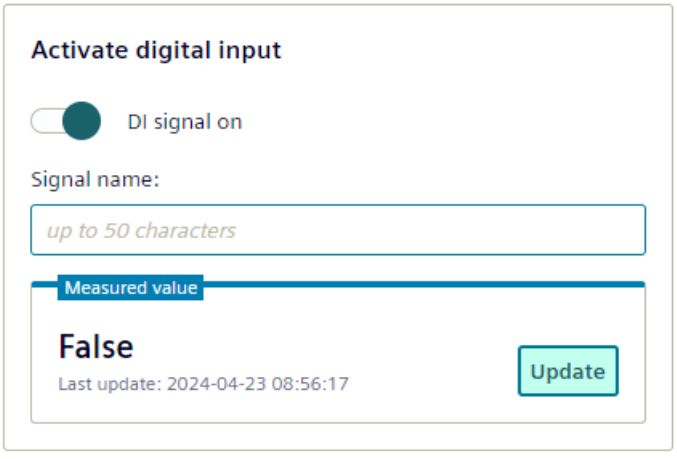
Select the desired initial port state (closed or open).

Input diagnostics

The diagnosis of analog and digital inputs is primarily used to check the correct connection of external signals. This ensures that the input signals are read correctly.



In the analog input field, press the "Update" button. The current value of the physical analog input will be displayed with the corresponding unit in the "Measured value" group box, and the corresponding timestamp in the "Last update" line will be updated.

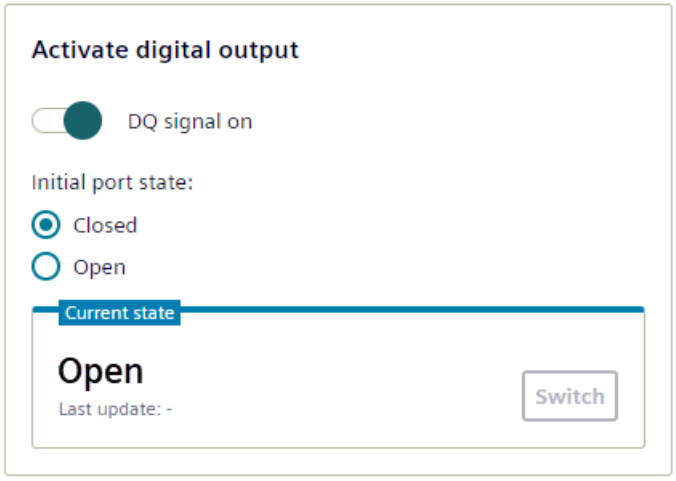


In the digital input field, press the "Update" button. The current status of the physical digital input will be displayed in the "Measured value" group box as "True" or "False" and the corresponding timestamp in the "Last update" line will be updated.

Output diagnostics

Diagnostics of the digital output ensures that the connected device is properly controlled via a digital output.

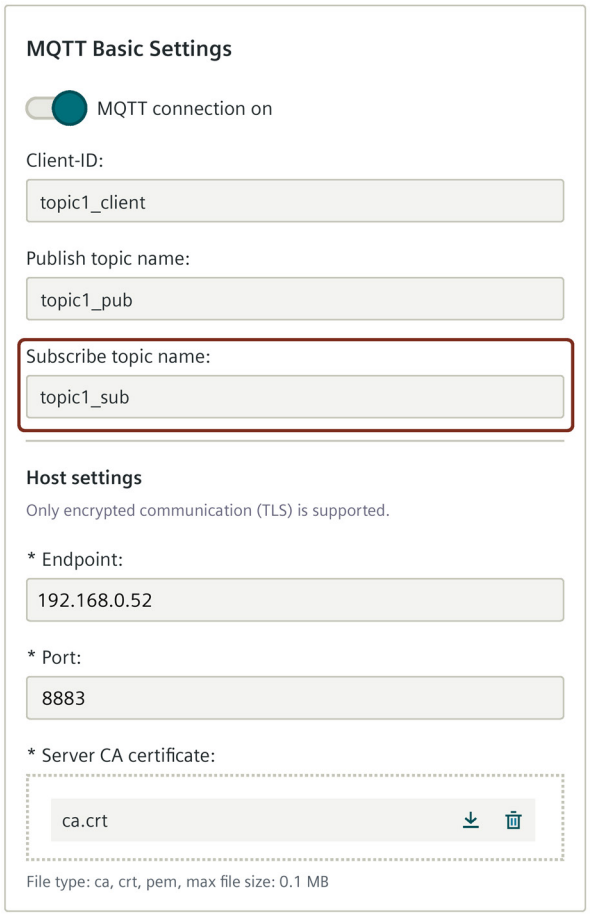
In the digital output field, press the "Switch" button in the "Current state" group box. The current state of the physical digital output will be toggled from "Open" or "Closed" and vice versa, and the corresponding timestamp in the "Last update" line will be updated.



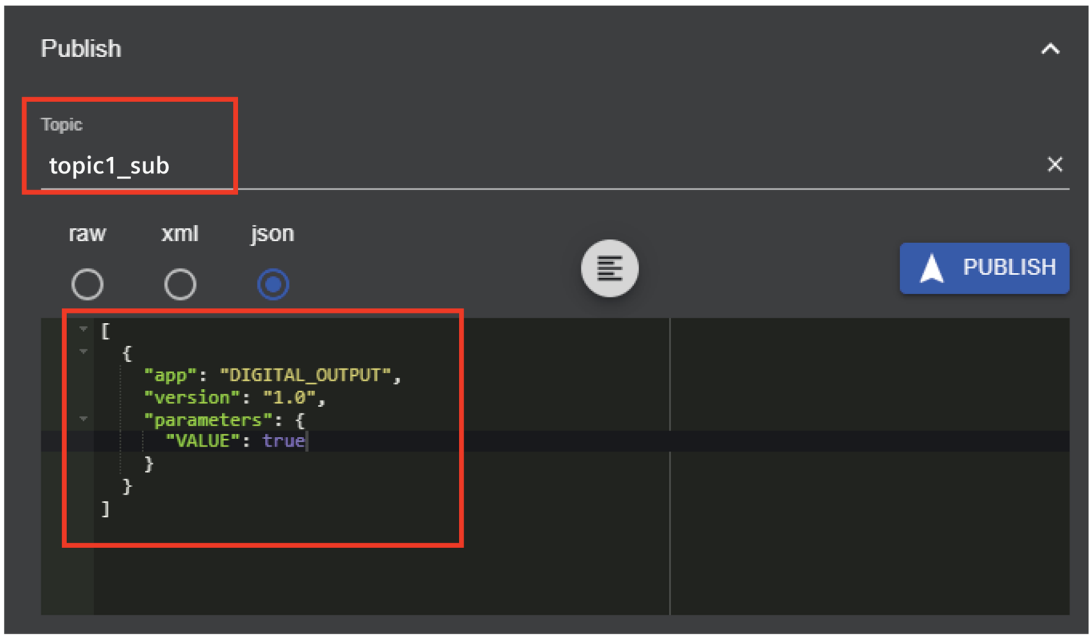
When the "Analog & Digital IO" settings page is exited, the physical digital output automatically changes to the "Open" state.

Settings of the DIGITAL_OUTPUT via MQTT protocol

A Subscribe topic name is assigned under Connectivity/MQTT. Under this topic, you can change the values of the DIGITAL_OUTPUT, e.g.:



Publish desired changes to the DIGITAL_OUTPUT application:



Publish topic must match the previously set Subscribe topic name in the SIMATIC FDE Gateway.

The following payload in the JSON format shows how the settings can be changed:

```
[
  {
    "app": "DIGITAL_OUTPUT",
    "version": "1.0",
    "parameters": {
      "VALUE": true
    }
  }
]
```

The VALUE value can be changed.

6.4.3 USS settings

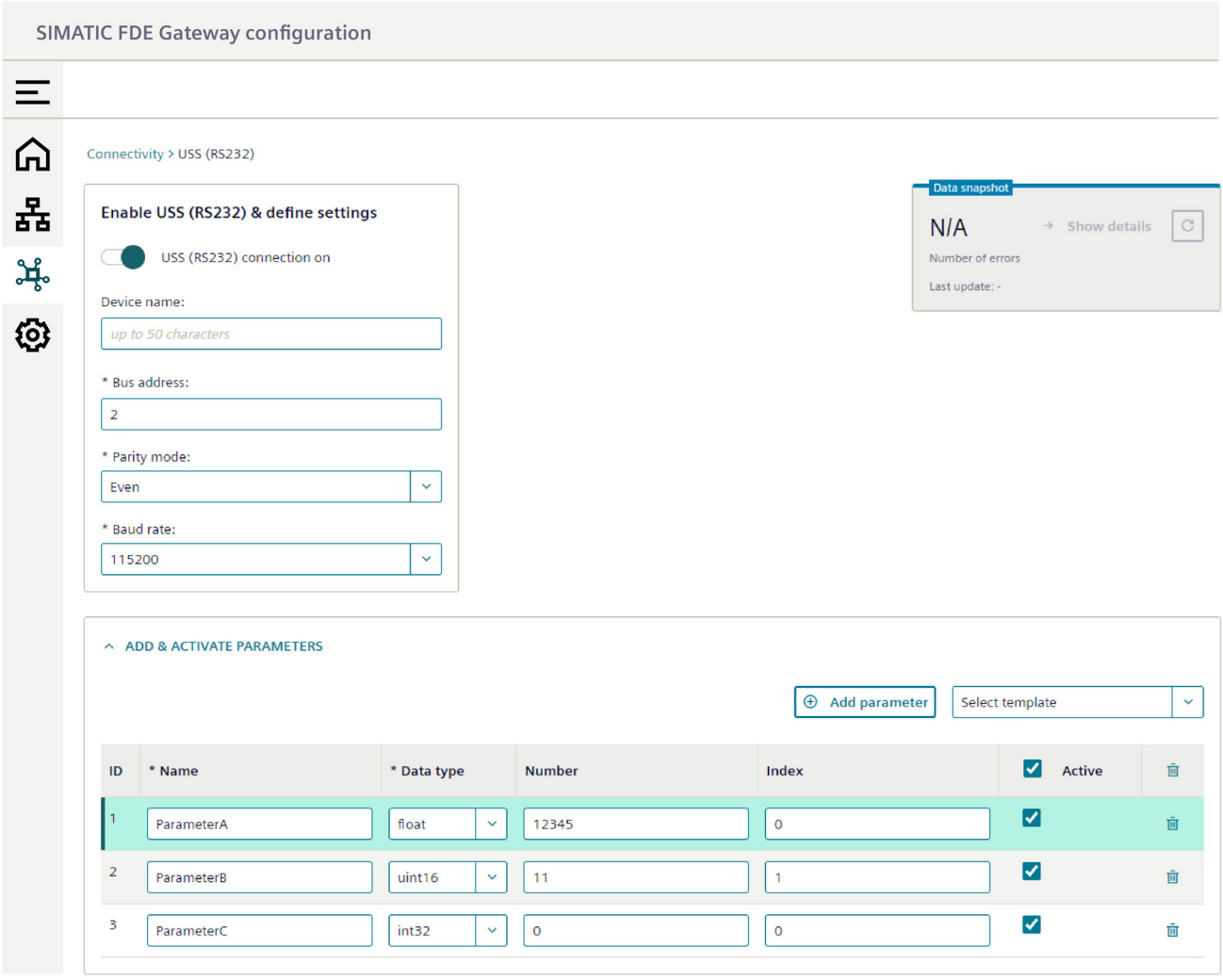
USS basic setting

Enable the USS connectivity and set the parameters in the USS (RS232) tab.

The "Bus address" field accepts values in the range from 0 to 31, representing the address of the slave device.

The "Parity mode" field allows selection of the following values: None; Even; Odd.

The "Baud rate" field allows selection of the following values: 9600; 19200; 38400; 57600; 76800; 93750; 115200.



Adding and activating parameters

To be able to save the configuration, at least one parameter must be "Active" when the interface is active.

Click "Add parameter". A parameter with name, data type, number, and index can then be inserted.

Added and activated parameters are read out via USS. Clear the check box in the corresponding line to disable the parameter.

The FDE Gateway accepts a maximum of 50 parameters.

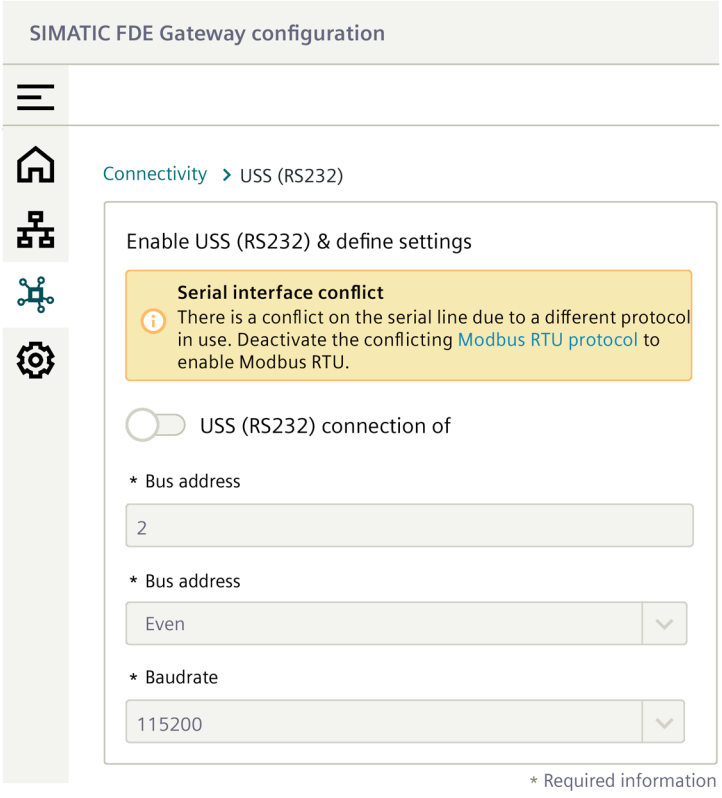
You can find detailed information on the available parameters, data types, numbers and indexes in the product information for your converter.

You can also select a template valid for G120 via "Select template".

Note

It is not possible to use RS232 and RS485 at the same time.

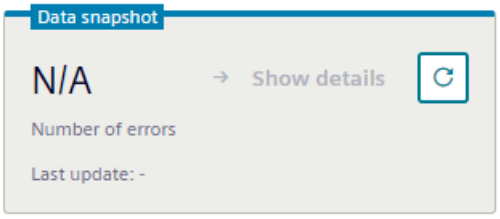
If RS485 is enabled, the following window appears in USS:



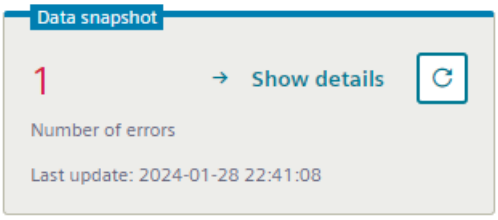
Diagnostics of active parameters

These general diagnostics serve to check the correctness of active parameter settings, verify communication and display current values.

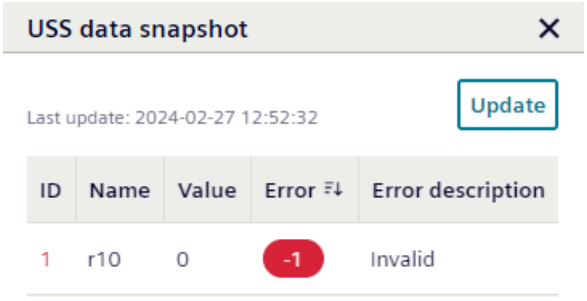
If a valid connectivity configuration has been saved and the connectivity enabled, the "Data snapshot" group box has an active button for performing diagnostics.



When diagnostics are performed by clicking the button, the current number of errors and the time stamp of the last test is displayed. The "Show details" link is activated.



Clicking the "Show details" button displays a table with all active parameters:



The five columns show:

ID: Parameter ID (black if there is no error; red if there is an error)

Name: Parameter name

Value: If no error occurred, the current value received by the app from the connected device is displayed; otherwise, 0 is displayed**.**

Error: 0 and gray background if there is no error; otherwise the error code and red background.

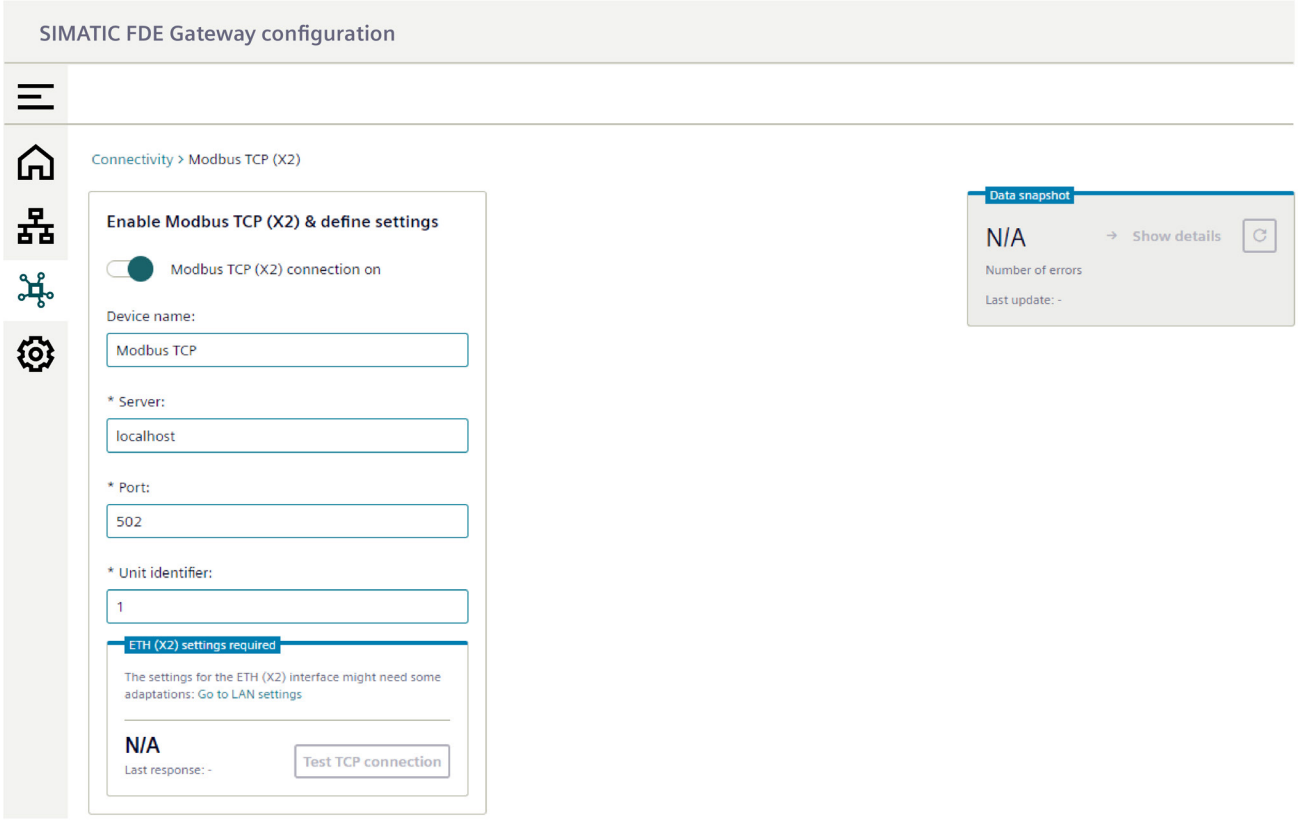
Error description: If there is an error, the error description is shown here; otherwise, the field is empty.

You can find an overview of the USS error codes in the section MQTT parameters (Page 65).

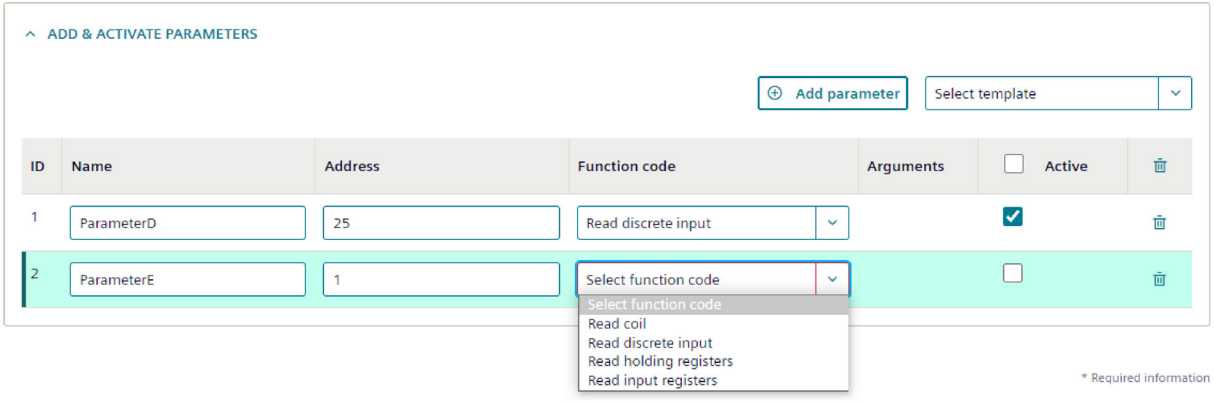
6.4.4 Activate Modbus TCP (X2)

Modbus TCP basic settings

Enable Modbus TCP connectivity and set the parameters in the Modbus TCP (X2) tab. The parameters are read out periodically.



Adding and activating parameters

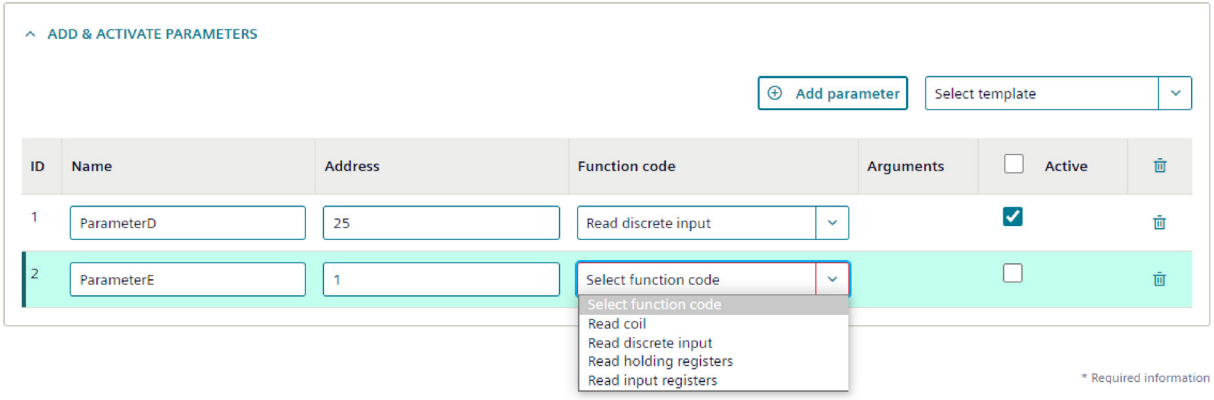


To be able to save the configuration, at least one parameter must be "Active" when the interface is active.

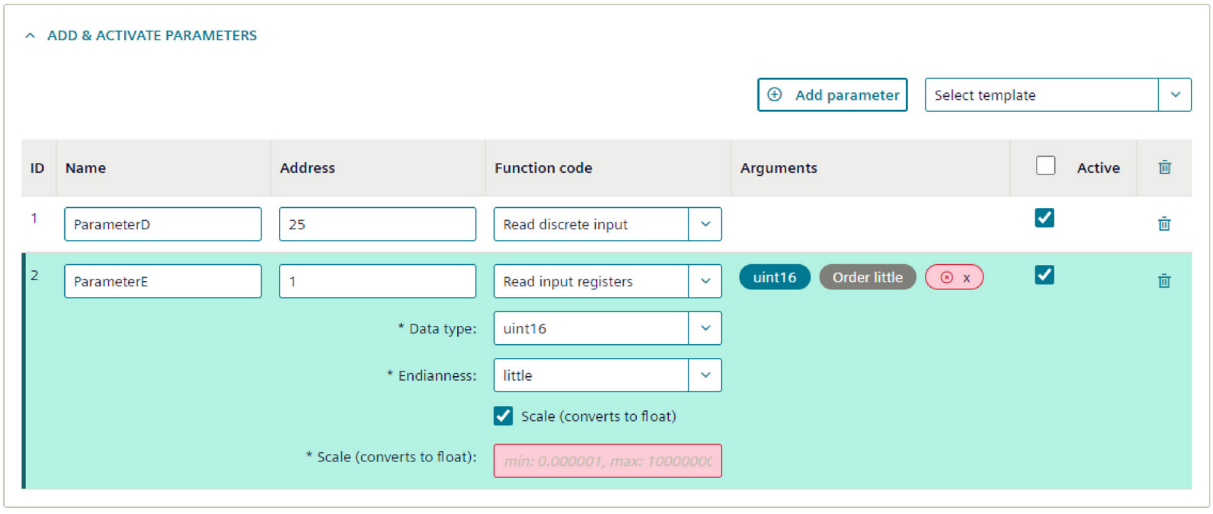
Click "Add parameter". A parameter with name, address, function code and arguments can then be inserted.

Enter the name and address of the parameter. Select the function code from the drop-down menu.

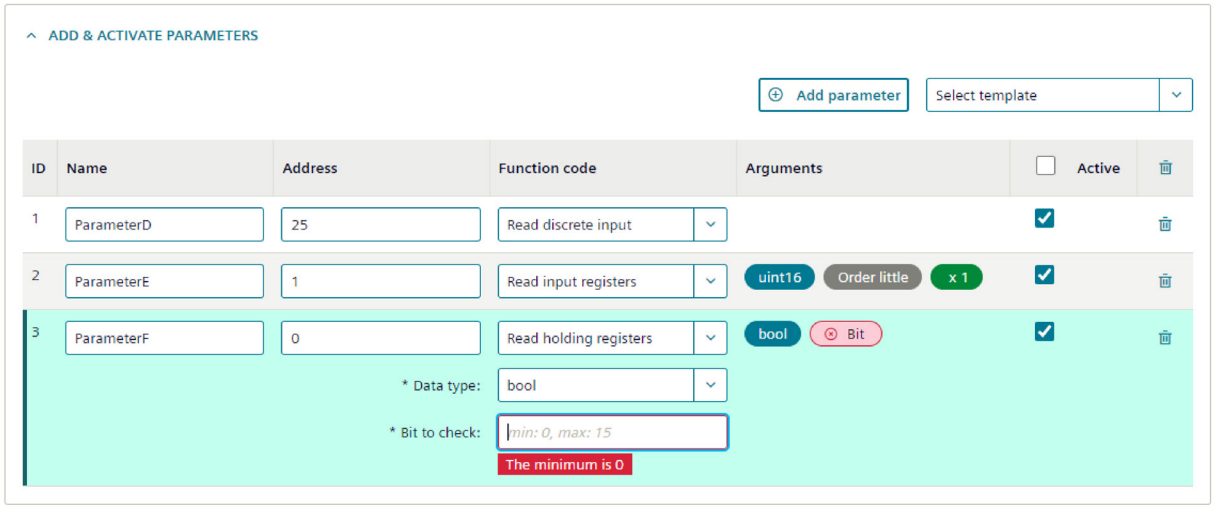
For the "Read holding registers" and "Read input registers" function codes, select the data type from the drop-down menu.



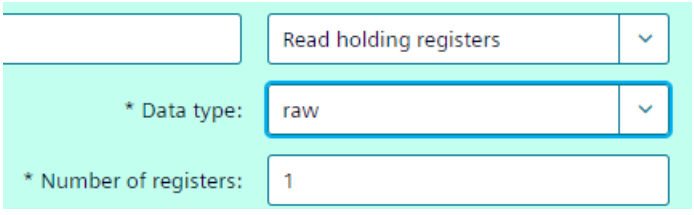
For the "float", "double", "int" and "uint" data types, select "Endianness". You can also convert the "int" and "uint" data types to "float" by selecting the "Scale" check box.



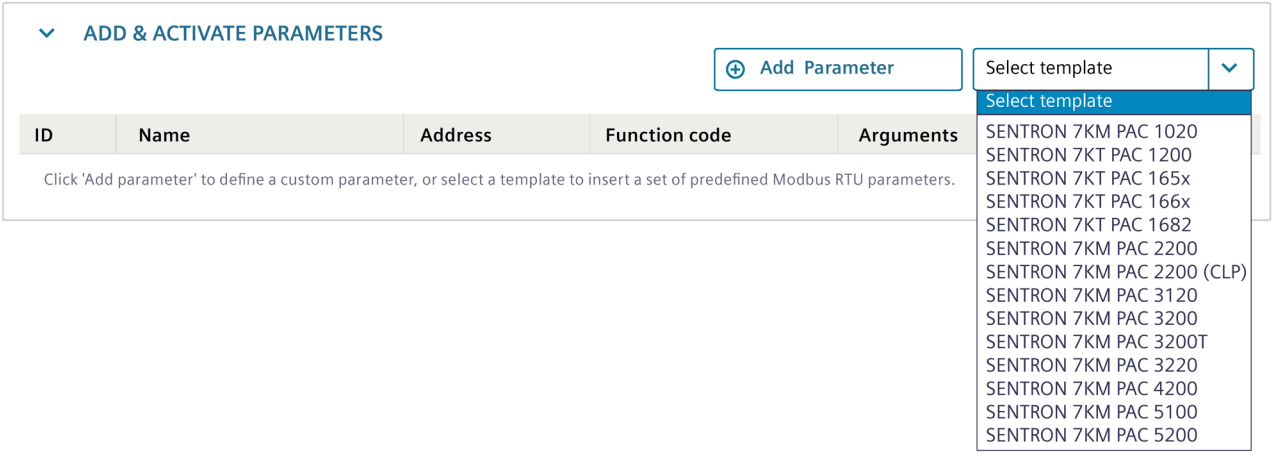
For the "bool" data type, enter the bit number to be checked:



For the "raw" data type, enter the number of registers.



Alternatively, you can insert a template from the template list. Each template corresponds to one PAC device. Some parameters have been specified as "Active" in an added template. These active parameters are generally read from a target PAC.



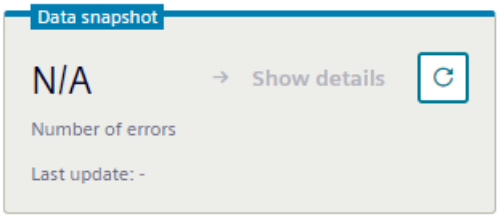
Select the "Active" check box in the corresponding line to activate the parameter.

Clear the "Active" check box in the corresponding line to deactivate the parameter.

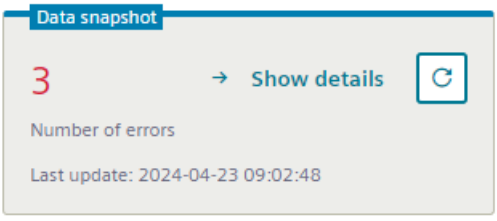
Diagnostics of active parameters

These general diagnostics serve to check the correctness of active parameter settings, verify communication and display current values.

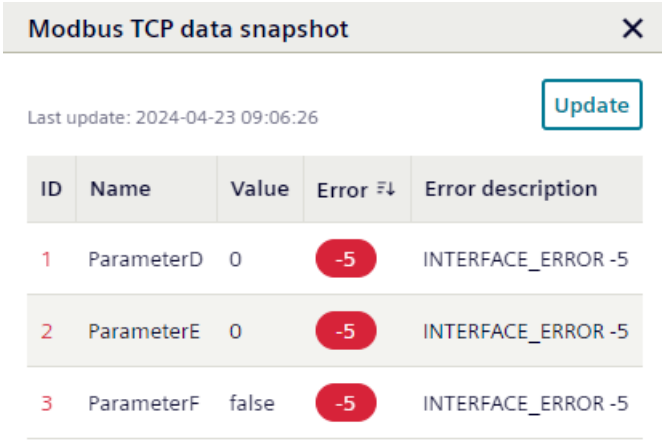
If a valid connectivity configuration has been saved and the connectivity enabled, the "Data snapshot" group box has an active button for performing diagnostics.



When diagnostics are performed by clicking the button, the current number of errors and the time stamp of the last test is displayed. The "Show details" link is activated.



Clicking the "Show details" link displays a table with all active parameters:



The five columns show:

ID: Parameter ID (black if there is no error; red if there is an error)

Name: Parameter name

Value: If no error occurred, the current value received by the app from the connected device is displayed; otherwise, 0 is displayed.

Error: 0 and gray background if there is no error; otherwise, the error code and red background.

Error description: If there is an error, the error description is shown here; otherwise, the field is empty.

You can find an overview of the standard Modbus error codes in the section: MQTT parameters (Page 65).

6.4.5 Activating Modbus RTU (RS485)

Modbus RTU basic settings

Enable Modbus RTU connectivity and set the parameters in the Modbus RTU (RS485) tab. Follow the same procedure as for Modbus TCP.

Adding and activating parameters

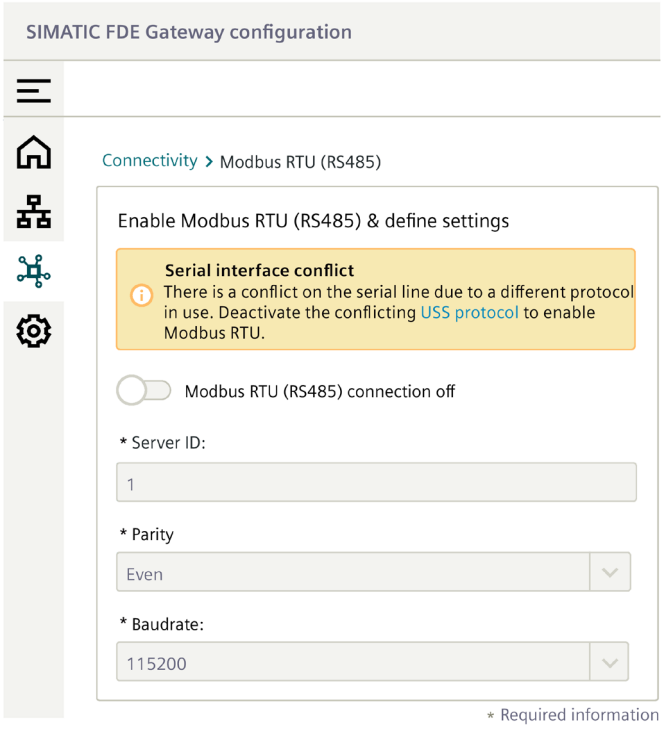
To be able to save the configuration, at least one parameter must be "Active" when the interface is active. Follow the same procedure as for Modbus TCP.

Note

It is not possible to use RS232 and RS485 at the same time.

It is not possible to use USS and Modbus RTU at the same time.

If RS232 (USS connectivity) is enabled, the following window appears in Modbus RTU:



Diagnostics of active parameters

Use the same diagnostics tools as for Modbus TCP.

6.5 MQTT parameters

Here you can see parameters that are defined in the connectivity configuration and published via MQTT.

Device attributes

The FDE Gateway provides the following device attributes in its MQTT payload:

- DEVICE_NAME: Device name; the default value is fde_gateway_[last 6 characters of the Wi-Fi MAC]
- MLFB
- WIFI_MAC: Wi-Fi MAC address as identifier of the device that is publishing to the MQTT broker
- DEVICE_TIME: Device time for adding the timestamp on the data points on the OPC UA Server
- MQTT_PNAPP_SETTINGS_ACTIVE: Flag indicating whether the required configuration for the "PN for Linux" app connection is fulfilled

Note

These attributes are always provided when MQTT is activated, even if nothing else is activated.

Analog input

Parameter	Description	Value
TAG	User-defined name displayed in an MQTT payload	Text (String) -> settable via WebUI
RAW_VALUE	Read raw value	unit32
MA_VALUE	Read value in mA	float
MV_VALUE	Read value in mV	float
IS_VALID	Indication if read value is valid	bool • Any value except '1': Read value is invalid • '1': Read value is valid

Digital input

Parameter	Description	Value
TAG	User-defined name displayed in an MQTT payload	Text (String) -> settable via WebUI
VALUE	Read digital value	bool • '0': false • '1': true

Digital output

The digital output does not provide any output via MQTT.

USS

Parameter	Description	Value
TAG	User-defined name displayed in an MQTT payload	Text (String) -> settable via WebUI
Read registers	Register values actually read	Depends on the register
STATUS	General status code that indicates the status of the last transfer	• '-2' (AddressNotAvailable) -> if no target address was specified • '-1' (Invalid) -> the functionality is not running or is frozen • '0' (AllGood) -> reading of all values was successful • '1' (SomeFailed) -> at least one of many registers was read successfully • '2' (AllFailed) -> reading of all values has failed

Parameter	Description	Value

STATUS_INFO	Detailed information on which registers could not be read and why. The data is supplied in JSON format.	The data is provided as text (String).
		`{`
		`  "last_update_failed":[`
		`    {`
		`      "name":"register_A",`
		`      "number":123,`
		`      "read_error":1`
		`    },`
		`    {`
		`      "name":"register_B",`
		`      "number":321,`
		`      "index":1,`
		`      "read_error":2`
		`    }`
		`  ]`
		`}`
		The values of `read_error`:
		• '1' (SerialBusTimeout)
		• '2' (StxLgeTimeout)
		• '3' (StxLgeInvalidRead)
		• '4' (InsufficientBuffer)
		• '5' (AdrDataBccTimeout)
		• '6' (AdrDataBccInvalidRead)
		• '7' (InternalError)
		• '8' (InvalidPacketType)
		• '9' (InvalidIndexes)

TIMESTAMP_MS	Timestamp when reading of all parameters ended	Text -> time since the Unix epoch in milliseconds
READOUT_MS	Time consumed of the last reading of all selected parameters	uint32 -> time in milliseconds

Modbus TCP/RTU

Parameter	Description	Value
TAG	User-defined name displayed in an MQTT payload	Text (String) -> settable via WebUI
Read registers	Register values actually read	Depends on the register
STATUS	General status code that indicates the status of the last transfer	• '-8' (UnconfiguredApp) -> one of the following: server ID, baud rate, parity mode, was not specified • '-4' (ModbusClientInitFailed): -> Modbus client could not be initialized • '-2' (SerialBusError) -> serial bus configuration failed • '-1' (Invalid) -> the functionality is not running or is frozen • '0' (InitSuccessful) -> initialization of the corresponding app was successful • '1' (AllGood) -> reading all registers was successful • '2' (SomeFailed) -> at least one group[1)] of several groups was read successfully • '4' (AllFailed) -> reading all registers failed • '8' (NothingToUpdate) -> no register was set for reading

Parameter	Description	Value

STATUS_INFO	Detailed information on which registers were not read and why. The data is supplied in JSON format.	The data is provided as text (String).
		`{`
		`  "last_update_failed":[`
		`  {`
		`  "name":"register_A",`
		`  "address":123,`
		`  "exception_code":1`
		`  },`
		`  {`
		`  "name":"register_B",`
		`  "address":321,`
		`  "exception_code":-1`
		`  }`
		`  ]`
		`}`
		• `exception_code` > 0: Modbus protocol error; the value corresponds to the exception codes according to the Modbus standard:
		– 0x01: Illegal function
		– 0x02: Illegal data address
		– 0x03: Illegal data value
		– 0x04: Slave device failure
		– 0x05: Acknowledge
		– 0x06: Slave device busy
		– 0x07: Negative acknowledge
		– 0x08: Memory parity error
		– 0x10: Gateway path not available
		– 0x11: The target device has failed to respond
		• `exception_code` < 0: Bus error

1) Group means either coils, discrete inputs, holding registers or input registers

6.6 MQTT payload examples

This section contains MQTT payload examples.

Fanout mode: Single message to publish topic

Example: Setting of detailed parameters "On"

```
[
  {
    "app": "USS",
    "parameters": {
      "Parameter1": {
        "value": 315.854,
        "type": "float"
      },
...
      "STATUS": {
        "value": 0,
        "type": "int32_t"
      },
      "STATUS_INFO": {
        "value": "{}",
        "type": "string"
      },
      "TIMESTAMP_MS": {
        "value": "1663312002231",
        "type": "string"
      },
      "READOUT_MS": {
        "value": 35,
        "type": "uint32_t"
      }
    }
  }
]
```

Example: Setting of detailed parameters "Off"

```
[
  {
    "app": "USS",
    "parameters": {
      "Parameter1": 315.254,
...
      "STATUS": 0,
      "STATUS_INFO": "{}",
      "TIMESTAMP_MS": "1663313457709",
      "READOUT_MS": 35
      }
  }
]
```

Example: Setting - only digital input

```
[
  {
    "app": "DIGITAL_INPUT",
    "parameters": {
      "TAG": {
        "value": "digital_input_signal",
        "type": "string"
      },
      "VALUE": {
        "value": 1,
        "type": "int8_t"
      }
    }
  },
]
```

Explanation

The value under "VALUE" corresponds to the state of the digital input:

- Value: 1: Input voltage.
- Value: 0: No input voltage.

Example: Setting - only digital output

If only the digital output is activated, the state corresponds to the value of the DIGITAL_OUTPUT application to be published.

Example: Setting - only of analog input current (0 - 20 mA): active

```
[
  {
    "app": "ANALOG_INPUT",
    "parameters": {
      "TAG": {
        "value": "analog_input_voltage",
        "type": "string"
      },
      "RAW_VALUE": {
        "value": 4057,
        "type": "uint32_t"
      },
      "MA_VALUE": {
        "value": 20,
        "type": "float"
      },
      "MV_VALUE": {
        "value": 0,
        "type": "float"
      }
    }
  }
```

Explanation

The value under "MA_VALUE" is output directly in mA.

Example: Analog input voltage active

```
[
  {
    "app": "ANALOG_INPUT",
    "parameters": {
      "TAG": {
        "value": "analog_input_voltage",
        "type": "string"
      },
      "RAW_VALUE": {
        "value": 451,
        "type": "uint32_t"
      },
      "MA_VALUE": {
        "value": 0,
        "type": "float"
      },
      "MV_VALUE": {
        "value": 8185.19,
        "type": "float"
      }
    }
  },
  {
    "app": "USS",
    "parameters": {
...
```

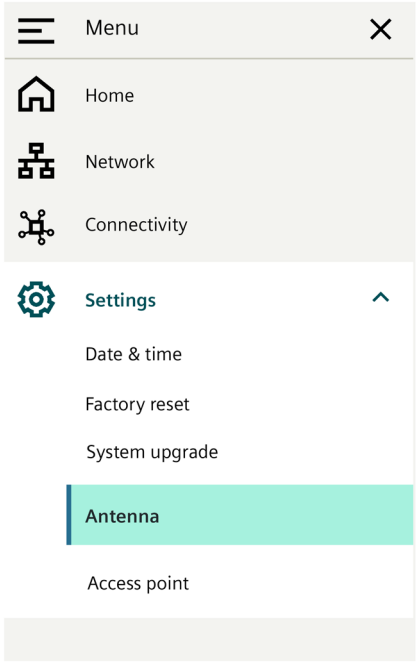
Explanation

The value under "MV_VALUE" is entered directly in mV.

6.7 Basic settings

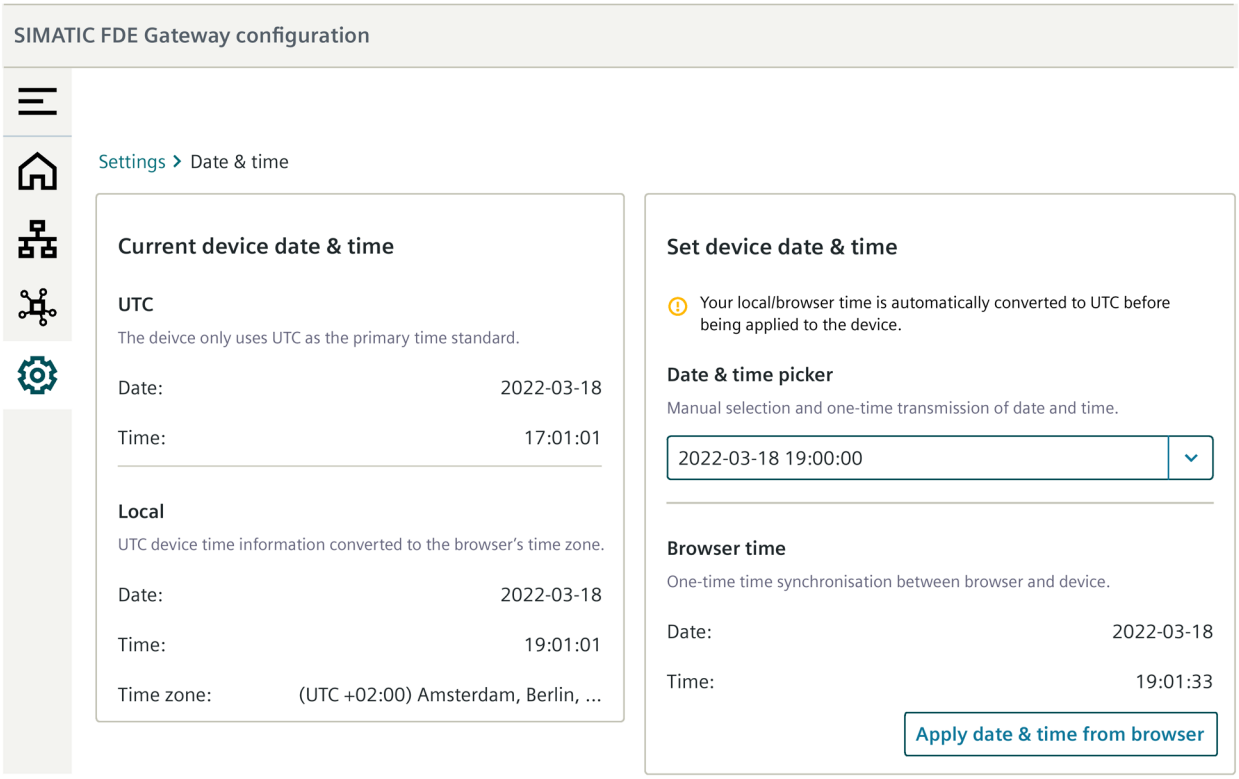
The "Settings" tab contains the following:

- Date and time
- Reset to factory settings
- System upgrade
- Antenna (external or internal)
- Access point



6.7.1 Date & time

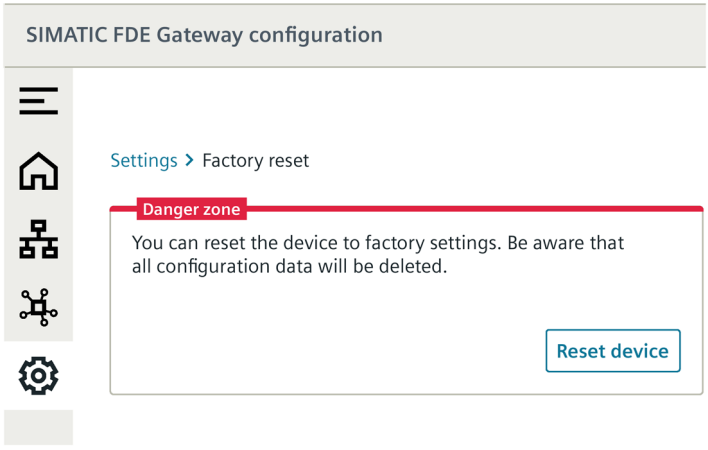
The time configured on the device always corresponds to UTC as the primary format. This time can be set manually or applied from the web browser:



6.7.2 Resetting to factory settings

It is possible to reset the device to the factory settings. Note that all configuration data is deleted in the process. Press and release the "USER" button 5 times within 10 seconds to restore the factory settings of the gateway.

You can also restore the factory settings via the web user interface:



If you forget the password, it can be reset by restoring the factory settings. To do this, use the "USER" button as described above.

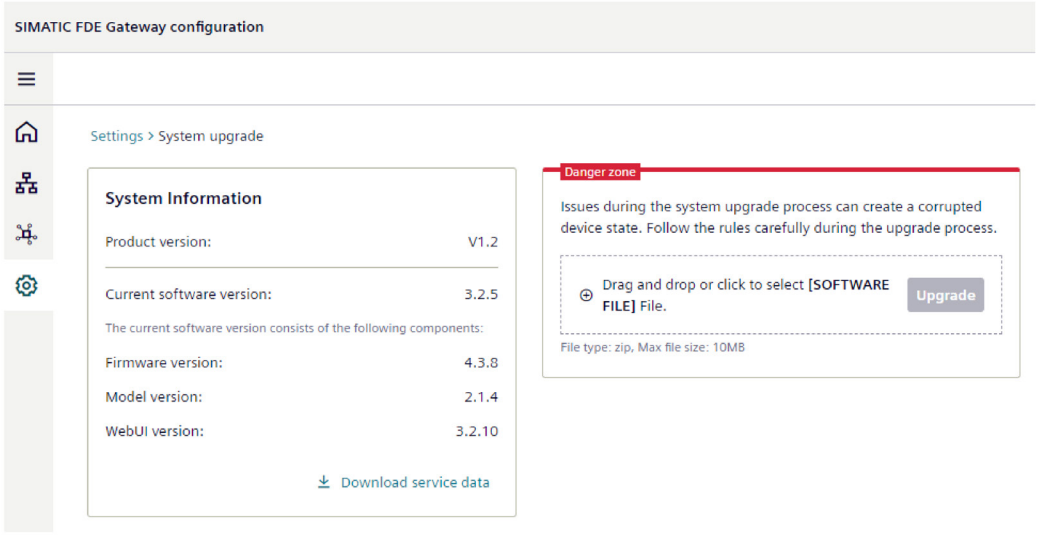
6.7.3 System upgrade

The firmware update is a feature that should always be used with caution. Always read the release notes included with the package and follow Siemens' recommendations. In general, firmware updates should be installed in the following cases:

- The update package contains security-related fixes.
- The update package solves an issue in a feature that is causing problems or provides a new feature that is needed.

You can find updated software versions in the SiePortal (https://sieportal.siemens.com/).

You can update the firmware via the system upgrade interface:



The link at the bottom allows you to download the current service data.

Read the notes which appear during the process.

Note

Follow these rules to avoid damage to the device during the system upgrade:

- Ensure that the device is connected to a stable 24 V power supply.
- Do not close or refresh the website.
- Ensure that your client is always connected to the SIMATIC FDE Gateway hotspot. Do not leave the area.

Remote firmware update in RUN mode

Requirements

The FDE_BUNDLE_UPDATE has made available the parameters "url" and "ca_crt", where:

- The "url" parameter corresponds to the network location of the unzipped bundle file hosted on an SSL-secured server
- The "ca_crt" parameter corresponds to the text of the SSL certificate needed to access the server

Note

For the remote update, the line breaks in the SSL certificate must be replaced with "\n" placeholders.

Start of the remote firmware update

```
[{
    "app": "FDE_BUNDLE_UPDATE",
    "version": "1.0",
    "parameters": {"url": "https://<server IP>:<server port>/<bundle file location,
    "ca_crt": "<text of the SSL certificate, with linebreaks replaced with '\n' placehold-
ers>"}
}]
```

When the right "url" and "ca_crt" parameters are provided via the MQTT payload, the FDE Gateway initiates the following:

- Connection to the server whose address is specified by the "url" parameter
- Output to the serial log "using interface [current device IP]"

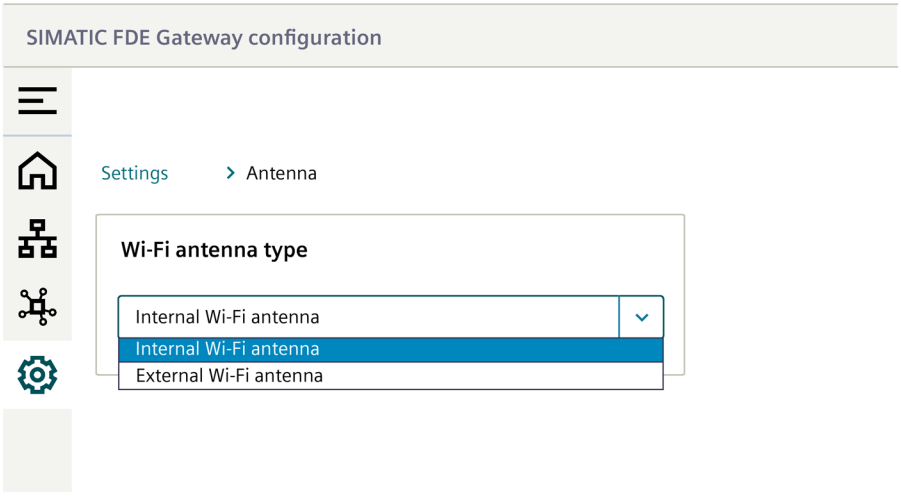
After streaming and applying all assets in BUNDLE_UPDATE mode, the FDE Gateway restarts in RUN mode with the new firmware version without losing any configuration data.

If the provided "url" and "ca_crt" parameters are invalid or a connection to the file server cannot be established for any other reason, the FDE Gateway restarts in RUN mode on the previous, unchanged firmware without losing any configuration data.

6.7.4 Antenna settings

An FDE-Wi-Fi can work either in internal or in external antenna mode. By default, the internal antenna for Wi-Fi is activated.

Select the internal or external antenna in Settings:

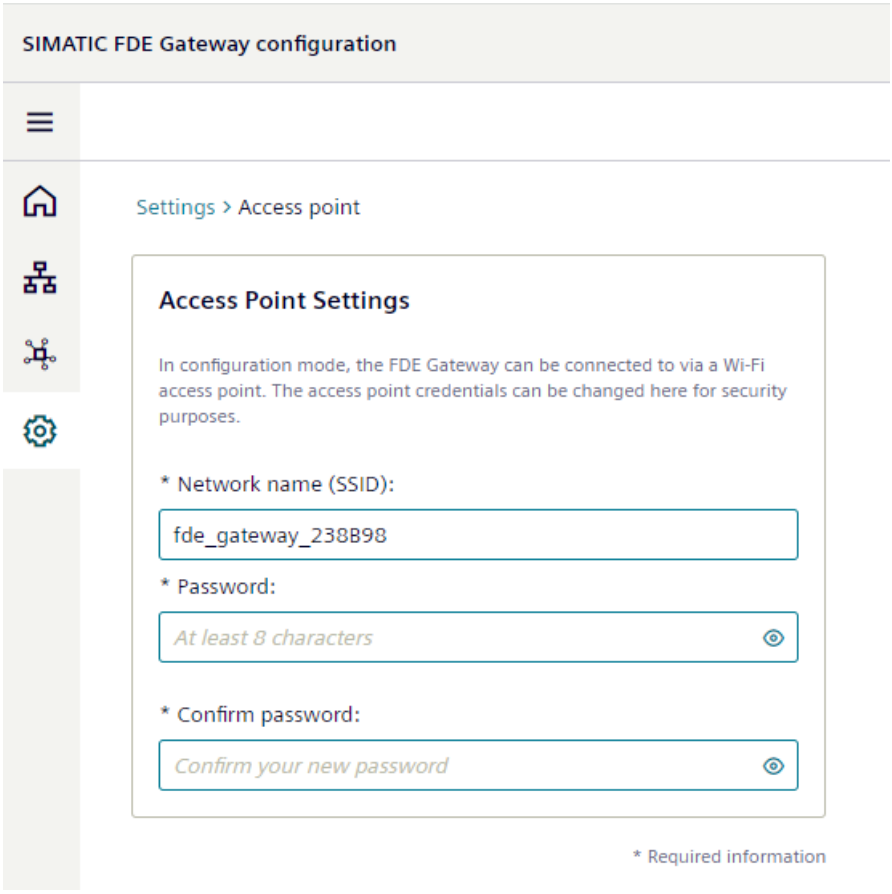


Note

Changes only become effective after saving and restarting.

6.7.5 Access point

In configuration mode, you can connect to the FDE Gateway via a Wi-Fi access point. The login data for the access point can be changed for security reasons. Enter and confirm the password:



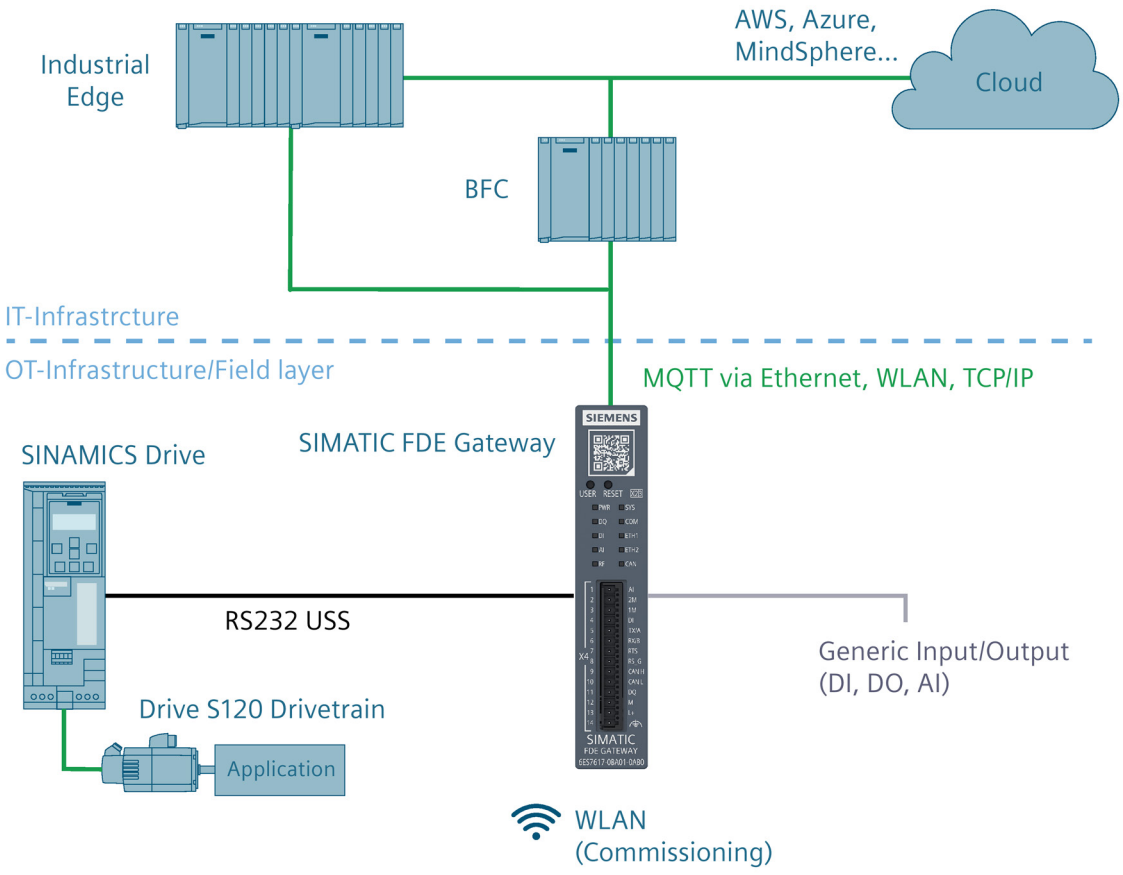
The network name (SSID) must be between 2 and 32 characters long.

The password must be between 8 and 63 characters long. It should contain upper and lower case letters, numbers and special characters.

6.8 Settings for operation on the BFC Gateway

The Brownfield Connectivity Gateway enables the installation of applications such as BFC Analytics. This app offers a solution for visualizing data and machine tool-related KPIs which provide information about the production and machine states.

The following figure shows a use case for connecting an FDE Gateway to a BFC Gateway when using G120/RS232.



Settings

The BFC Gateway is in "Connect via UI" commissioning mode. Make all necessary configurations for the MQTT connection to the BFC on both sides:

- MQTT settings must be made on the FDE side.
- Insert the certificate and/or user name and password.
- The USS communication must be configured according to the converter and parameters must be specified manually or via a template (only valid for G120).
- The BFC Gateway settings and installation are described in the BFCG Function Manual (https://support.industry.siemens.com/cs/us/en/view/109801700).
- Middleware script must be inserted (internal mapping of the parameter values).

Overview of system limits

By default, a BFC Gateway supports up to 60 connected clients (BFC devices).

Up to 50 data points are supported per BFC device, divided into "datasets".

The shortest interval for reading datasets is 200 ms.

Open BFC Gateway ports for incoming communication

Port	Type	Protocol	Use	Encrypted	Description
22	TCP	SSH	Commissioning/ Updates	Yes	SSH access for commissioning and system updates
1883	TCP	MQTT	Commissioning	No	Standard MQTT port for commissioning BFC clients
4840	TCP	OPC UA	Data forwarding	Yes	Standard OPC UA server port, used to present collected data.
8883	TCP	MQTT	Data acquisition	Yes	Standard MQTTS port for data acquisition from BFC clients
9876	TCP	HTTP	Commissioning	No	HTTP WebUI for commissioning the BFC Gateway
9877	TCP	HTTPS	Configuration & HTTP REST Client	Yes	HTTPS WebUI for configuring the BFC Gateway

Further setting options are described in the BFCG Function Manual (https://support.industry.siemens.com/cs/us/en/view/109801700).

6.9 Settings for operation on the Industrial Edge device

The Industrial Edge device enables you to install applications including IE Databus, IE Flow Creator, and IE MQTT Connector.

These apps offer solutions for visualizing data and machine tool-related KPIs which provide information about the production and machine states.

The Siemens Industrial Edge Hub platform also offers many pre-built apps. For example, the apps "Analyze MyDrives /Edge" or "Predictive Service Analyzer - Converter" were developed for monitoring the drive train.

Settings

Make all necessary configurations for the MQTT connection to Industrial Edge on both sides:

- MQTT settings must be made on the FDE side.
- Insert the certificate and/or username and password.
- The USS communication must be configured according to the converter and parameters must be specified manually or via a template (only valid for G120).

The settings and installation of Edge applications are described in the Industrial Edge Management Operating Manual.

Perform the following steps:

- Install the required apps (IE Databus, IE Flow Creator, IE MQTT Connector).
- Define the required network settings on the Edge device side.
- Generate the keys for the safe MQTT connection.

6.10 Settings for operation in MindSphere

The Siemens IoT-as-a-service solution MindSphere saves operating data and makes them accessible through digital applications so that you can make decisions on the basis of valuable factual information. One of these apps is the Predictive Service Assistance app, which offers access via your tenant to all relevant service and asset data of the drive systems, such as pumps and fans.

Settings

Make all necessary configurations for the MQTT connection to the BFC and MindSphere on both sides:

- MQTT settings must be made on the FDE side.
- Insert the certificate and/or username and password.
- Select a USS example template to obtain valid data.
- BFC Gateway and MindSphere settings and installation are described in the BFCG Function Manual.

Certificates and approvals

7

7.1 CE (Industry)

The device complies with the guidelines listed in the following sections.

EU Declaration of Conformity

The associated Declaration of Conformity is available on the Internet: EU Conformity Declaration (https://support.industry.siemens.com/cs/ww/en/view/109820713).

Radio Equipment Regulations (RED) Standards

ETSI EN 301489-1 (Common technical requirements)

ETSI EN 301489-17 (Specific conditions for Broadband Data Transmission Systems)

ETSI EN 300 328 (Wideband transmission systems)

ETSI EN 301 893 (5 GHz RLAN)

EN IEC 62311 (Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz – 300 GHz))

EN 55032 (Electromagnetic compatibility of multimedia equipment - Emission requirements)

EN 55035 (Electromagnetic compatibility of multimedia equipment - Emission requirements)

EN 62368-1 (Audio/video, information and communication technology equipment - Part 1: Safety requirements)

7.2 UKCA

The device complies with the British Standards (BS) applicable to the IPC as published in the Official Consolidated List of the British Government. The device fulfills the requirements and protection objectives of the following regulations and related supplements:

- Radio Equipment Regulations 2017 (RED)
- Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (RoHS).

UK Declarations of Conformity for the respective authorities are available from:

Siemens AG
Digital Industries

Factory Automation
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg

The UK Declaration of Conformity is also available for download from the Siemens Industry Online Support website under the keyword "Declaration of Conformity".

7.3 RCM Declaration of Conformity for Australia/New Zealand



FDE Gateway fulfills the requirements of the standard IEC 61000-6-4.

7.4 FCC and Canada (USA)

USA	
Federal Communications Commission Radio Frequency Interference Statement	This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a resential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: • Reorient or relocate the receiving antenna. • Increase the separation between the equipment and receiver. • Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. • Consult the dealer or an experienced radio/TV technician for help.
Shielded Cables	Shielded cables must be used with this equipment to maintain compliance with FCC regulations.
Modifications	Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

CANADA	
Canadian notice	This Class B digital apparatus complies with Canadian ICES-003. This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) This device may not cause interference. (2) This device must accept any interference, including interference that may cause undesired operation of the device.
Avis Canadian	Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada. L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : 1) L'appareil ne doit pas produire de brouillage; 2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

les dispositifs fonctionnant dans la bande 5 150-5 250 MHz sont réservés uniquement pour uneutilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit;

le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5 250-5 350 MHz et 5 470-5 725 MHz doit se conformer à la limite de p.i.r.e.

For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate;

le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5 725-5 825 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.

This radio transmitter [enter the device's ISED certification number] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

The concrete contents to check are the following three points:

1) Must use antenna such as vertical monopole omni-Antenna with gain not exceeding 2 dBi;

2) Should be installed so that the end user cannot modify the antenna;

3) Feed line should be designed in 50ohm

Fine tuning of return loss etc. can be performed using a matching network.

Le présent émetteur radio [enter the device's ISED certification number] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Le contenu concret à vérifier sont les trois points suivants :

1) Doit utiliser une antenne telle que l'omni-antenne monopôle verticale avec un gain ne dépassant pas 2 dBi;

2) doivent être installés de façon que l'utilisateur final ne peut pas modifier l'antenne

3) La ligne d'alimentation doit être conçue en 50ohm

Le réglage précis de la perte de rendement, etc. peut être effectué en utilisant un réseau correspondant.

RF exposure warning	
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body. Cet émetteur ne doit pas être Co-placé ou ne fonctionnant en même temps qu'aucune autre antenne ouémetteur. Cet équipement devrait être installé et actionné avec une distance minimum de 20 centimètres entre leradiateur et votre corps.	

Supplier's Declaration of Conformity	
Unique Identifier	SIEMENS, SIMATIC FDE Gateway
Responsible party	Siemens Industry, Inc. Digital Factory - Factory Automation 5300 Triangle Parkway, Suite 100 Norcross, GA 30092 USA Mail to: (amps.automation@siemens.com)
FCC Compliance 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.

Directives and declarations

8

8.1 Overvoltage category

Overvoltage category II: For devices that are to be supplied via the building wiring. This applies to both pluggable and permanently connected devices.

8.2 Pollution degree for electrical equipment

Pollution degree 2: Usually, only non-conductive pollution occurs. Temporary conductivity due to condensation is to be expected.

8.3 Electromagnetic Compatibility industrial area +A1:2011

Electromagnetic compatibility

This product meets the requirements of the EU Electromagnetic Compatibility Directive 2014/30/EU.

The device is designed in accordance with the CE marking for the following areas of application:

Area of application	Requirement for	
	Interference emission	Immunity to interference
Industrial area	EN 61000-6-4:2007 +A1:2011	EN 61000-6-2:2005

8.4 ESD guideline

What does ESD mean?

An electronic module is equipped with highly integrated components. Due to their design, electronic components are highly sensitive to overvoltage and thus to electrostatic discharging. Such electronic components or modules are marked as "electrostatic sensitive devices".

The following abbreviations are commonly used for "electrostatic sensitive devices":

- ESD - Electrostatic-sensitive device
- ESD – Electrostatic Sensitive Device is the common international designation

Electrostatic-sensitive devices can be labelled with the corresponding icon.



NOTICE

Damage of ESD through contact

Electrostatic-sensitive devices (ESDs) can be destroyed by voltages well below the threshold of human perception. If you don't discharge yourself electrostatically beforehand, just touching a component or electrical connector is sufficient to cause such voltages.

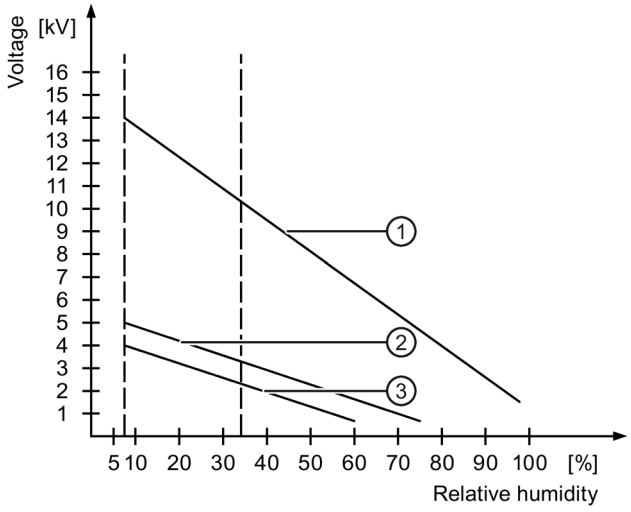
The damage that occurs to a component due to overvoltage is often not immediately detectable, but may only be noticed after a longer operating time. The consequences are unpredictable, and range from unforeseeable malfunctions to total failure of the machine or plant.

It is essential to avoid touching components directly. Make sure that personnel, workstations, and packaging are properly grounded.

Charging

Any person who is not conductively connected to the electrical potential of their surroundings can accumulate an electrostatic charge.

Of particular importance is the material with which the person comes into contact. The figure below shows the maximum values of the electrostatic voltages with which a person can be charged, depending on air humidity and material. These values correspond to the specifications of IEC 61000-4-2.



① Synthetic material

② Wool

③ Antistatic material such as wood or concrete

NOTICE
Observe grounding If no grounding is available, then no equipotentiality can be achieved. Electrostatic charges are not discharged and damage to the ESD may occur. Protect yourself against electrostatic discharging. When handling ESDs, make sure that personnel and workstations are properly grounded.

Protection against electrostatic discharging.

- Always disconnect the power supply before installing or removing modules which contain ESDs.
- Ensure sufficient grounding:
  - When handling electrostatic sensitive devices, make sure that personnel, workstations, devices, tools, and packaging are properly grounded. This prevents static charging.
- Avoid direct contact:
  - As a general rule, do not touch electrostatic sensitive devices, except in the case of unavoidable maintenance work.
  - Handle the assemblies at the edge so that you do not touch any connection pins or conductor paths. In this way, the discharge energy does not reach and damage any sensitive components.
  - Discharge your body electrostatically before taking module measurements by touching grounded metallic objects. Only use grounded measuring devices.

Technical specifications

9

9.1 General technical specifications

Article number	6ES7617-0BA01-0AB0
Dimensions	
• Width	18 mm
• Altitude	90 mm
• Depth	76.6 mm
Weight	83.1 g
Supply voltage[1]	
• Rated value (DC)	12/24 V
• Valid range low limit (DC)	10.2 V
• Valid range high limit (DC)	28.8 V
• Power failure buffering time	typ. 1 ms
• Power loss	Max. 11.5 W including digital output
Degree of protection	IP20 according to IEC 60529
Quality assurance	According to ISO 9001

1 The device may only be connected to a power supply in accordance with the requirements of safety extra low voltage (SELV) as specified in IEC/EN/DIN EN/UL 60950-1. The power supply must meet NEC Class 2 or LPS requirements according to IEC/EN/DINEN/UL 60950-1. Lower supply voltage reduces buffer times.

Digital inputs

Number of inputs	1
Cable length (unshielded)	Max. 600 m
Input voltage	
• Type of input voltage	DC
• "0" signal	< 5 V
• "1" signal	> 12 V

Digital output

Number of inputs	1
Type of digital output	Open Collector
Short-circuit protection	Yes

Cable length (unshielded)	Max. 300 m
Output voltage	
• Type of output voltage	DC
• Permitted voltage at output, max.	9.2 V
• Permitted voltage at output, min.	28.0 V
Output current	
• For signal "1" rated value	0.3 A

Analog inputs

Number of inputs	1
Type	Unipolar
Electrical isolation	Yes
Resolution	12 bits
Cable length (shielded)	Max. 200 m
Error limit	± 0.5 % FS
Input ranges	
• Voltage	0 - 10 V
• Current [1]	0 - 20 mA or 4 - 20 mA

[1] Input impedance typ. 124 Ohms

Interfaces

LAN interface X1 P1, RJ45 [1]	10/100 Mbps
LAN interface X2 P2, RJ45 [1]	10/100 Mbps
Protocols (Ethernet)	TCP/IP, DHCP, MQTT, Modbus TCP (X2)
RS232	USS protocol
Wi-Fi	2.4 GHz for configuration 2.4/5 GHz for northbound connection

[1] For unambiguous labeling, the LAN interfaces are numbered on the enclosure. The operating system numbering may differ.

Electromagnetic compatibility - immunity to interference

Immunity with regard to conducted disturbance variables on the power supply cables	± 2 kV 5 kHz and 100 kHz according to IEC 61000-4-4; burst ± 0.5 kV cable to cable according to IEC 61000-4-5; overvoltage ± 1 kV cable to ground according to IEC 61000-4-5; overvoltage
Immunity on signal cables	± 1 kV 5 kHz and 100 kHz according to IEC 61000-4-4; burst; length < 30 m ± 2 kV 5 kHz and 100 kHz according to IEC 61000-4-4; burst; length > 30 m ± 1 kV cable to ground according to IEC 61000-4-5; overvoltage; length > 30 m
Immunity against static electric discharge	±6 kV contact discharge according to IEC 61000-4-2 ±2 kV, ±4 kV, ±8 kV air discharge according to IEC 61000-4-2
Immunity against radiofrequency radiation	10 V/m, 80 MHz...1 GHz, 80% AM according to IEC 61000-4-3 10 V/m, 1 GHz ... 2 GHz, 80% AM according to IEC 61000-4-3 3 V/m, 2 GHz ... 6 GHz, 80% AM according to IEC 61000-4-3 10 V, 150 kHz ... 80 MHz, 80% AM according to IEC 61000-4-6

If there are voltage peaks on the power supply lines, use a protective device in the form of a varistor (MOV) UMOV = Urated x 1.2 (BLITZDUCTOR BVT AVD 24 (918 422) or compatible).

Electromagnetic compatibility - emitted interference

Conducted interference emission (DC): IEC 61000-6-4 + A1, IEC 61131-2	• 0.15 to 0.5 MHz 79 dB (µV) QP, 66 dB (µV) A • 0.5 to 30 MHz 73 dB (µV) QP, 60 dB (µV) A
Conducted emission (telecommunication/network): IEC 61000-6-4 + A1	• 0.15 to 0.5 MHz 84 dB (µV) - 74 dB (µV) QP, 74 dB(µV) – 64 dB(µV) A • 0.5 to 30 MHz 74 dB (µV) QP, 64 dB (µV) A
Radiated emission: IEC 61000-6-4, CISPR 32:17 1	• 30 to 230 MHz: 40 dB(µV/m) QP (3 m distance) • 230 to 1000 MHz: 47 dB (µV/m) QP (3 m distance) • 1 to 3 GHz: 70 dB (µV/m) P; 50 dB (µV/m) A (3 m distance) • 3 to 6 GHz: 74 dB (µV/m) P; 54 dB (µV/m) A (3 m distance)

9.2 Ambient conditions

Climatic ambient conditions

Temperature values have been tested according to IEC 60068-2-1, IEC 60068-2-2, and IEC 60068-2-14.

Ambient air temperature	
• Operation	-30 ... 60 °C
• Transport/storage	-40 ... 70 °C
Gradient	
• Operation	Max. 10 °C/h
• Storage	20 °C/h, no condensation
Relative humidity, tested according to IEC 60068-2-78, IEC 60068-2-30	
• Operation	5 ... 95% at 30 °C, no condensation
• Transport/storage	5 ... 95% at 25/55 °C, no condensation
Elevation in operation in relation to sea level	
• Installation altitude above MSL, max.	5000 m According to IEC 61131-2, the temperature specification must be linearly reduced if the installation altitude above sea level is above 2000 m. You need to add the different derating ratio for the temperature under different altitudes.

Mechanical environmental conditions

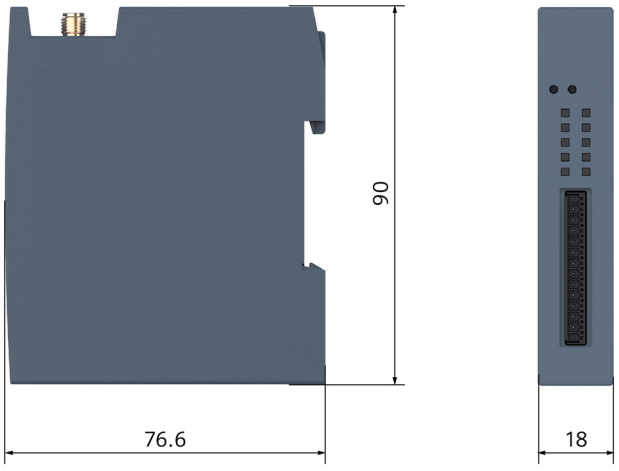
Vibration resistance, tested according to IEC 60068-2-6	
• Operation	Vibration load 1 g, 10 cycles per axis: • 5 ... 8.4 Hz, deflection 3.5 mm • 8.4 ... 200 Hz, acceleration 9.8 m/s^2
• Transport/storage	• 5 ... 8.4 Hz: Deflection 3.5 mm • 8.4 ... 500 Hz: Acceleration 9.8 m/s^2
Shock resistance, tested according to IEC 60068-2-27	
• Operation	150 m/s^2, 11 ms
• Transport/storage	250 m/s^2, 6 ms

Dimension drawings

A

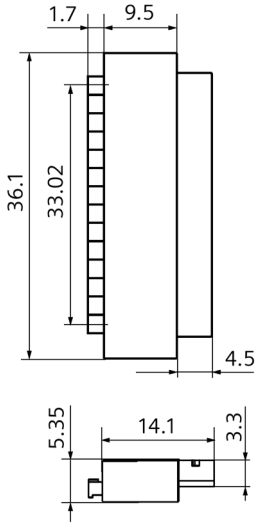
A.1 Dimension drawings

Dimensional drawing of the device



All dimensions are in mm.

Dimension drawing of the 14-pin X4 terminal



The grid dimension is 2.54 mm. All dimensions are in mm.