Communication Modules

Modbus TCP Communication Module

2789-9052

Product manual | Version 1.0.0

WAGO GmbH & Co. KG
Hansastraße 27
D - 32423 Minden
Phone: +49 571/887 – 0
Fax: +49 571/887 – 844169
E-Mail: ✉ **info@wago.com**
Internet: **www.wago.com**

Technical Support
Phone: +49 571/887 – 44555
Fax: +49 571/887 – 844555
E-Mail: ✉ **support@wago.com**

Every conceivable measure has been taken to ensure the accuracy and completeness of this documentation. However, as errors can never be fully excluded, we always appreciate any information or suggestions for improving the documentation.

E-Mail: ✉ **documentation@wago.com**

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present manual are generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

Provisions

This document applies to the following product:

2789-9052 (Modbus TCP Communication Module)

Product detail page	www.wago.com/

The product must only be installed and operated in accordance with the operating instructions. Knowledge of the operating instructions is required for proper use. You can find all documents and information on the detailed product page.

Additional document

- Product Manual of the Pro 2 Power Supply used

1.1 Intended Use

The 2789 Series Modbus TCP Communication Module is used for communication with a Modbus TCP fieldbus environment and is plugged into a subordinate WAGO Power Supply Pro 2.

The product is an open system and is designed for installation in a additional enclosure.

- This product is intended for installation in automation technology systems.
- The product is designed for use in dry indoor rooms.
- Operation of the products in industrial area is permitted.
- The product meets the EMC requirements for residential, office and commercial areas as well as small businesses, if the product used complies with the required emissions of interference (emission limits).
- Operation of the product in other application areas is only permitted when corresponding approvals and labeling are present.

Improper Use

Improper use of the product is not permitted. Improper use occurs especially in the following cases:

- Non-observance of the intended use
- Use without protective measures in an environment in which moisture, salt water, salt spray mist, dust, corrosive fumes, gases, direct sunlight or ionizing radiation can occur
- Use of the product in areas with special risk that require continuous fault-free operation and in which failure of or operation of the product can result in an imminent risk to life, limb or health or cause serious damage to property or the environment (such as the operation of nuclear power plants, weapons systems, aircraft and motor vehicles)

Warranty and Liability

The terms set forth in the General Business and Contract Conditions for Delivery and Service of WAGO GmbH & Co. KG and the terms for software products and products with integrated software stated in the WAGO Software License Contract – both available at www.wago.com – shall apply. In particular, the warranty is void if:

- The product is improperly used.
- The deficiency (hardware and software configurations) is due to special instructions.

- Modifications to the hardware or software have been made by the user or third parties that are not described in this documentation and that has contributed to the fault.

Individual agreements always have priority.

Obligations of Installers/Operators

The installers and operators bear responsibility for the safety of an installation or a system assembled with the products. The installer/operator is responsible for proper installation and safety of the system. All laws, standards, guidelines, local regulations and accepted technology standards and practices applicable at the time of installation, and the instructions in the the products' Instructions for Use, must be complied with. In addition, the Installation regulations specified by Approvals must be observed. In the event of non-compliance, the products may not be operated within the scope of the approval.

1.2 Typographical Conventions

Number Notation

100	Decimals: Normal notation
0x64	Hexadecimals: C-notation
'100'	Binary: In single quotation marks
'0110.0100'	Nibbles separated by a period

Text Formatting

italic	Names of paths or files
bold	Menu items, entry or selection fields, emphasis
`Code`	Sections of program code
>	Selection of a menu point from a menu
"Value"	Value entries
[F5]	Identification of buttons or keys

Cross References / Links

	Cross references/links to a topic in a document
	Cross references / links to a separate document
	Cross references / links to a website
	Cross references / links to an email address

Action Instructions

✓ This symbol identifies a precondition.

1. Action step
2. Action step

   ⇨ This symbol identifies an intermediate result.

⇨ This symbol identifies the result of an action.

- Individual action step

Lists

- Lists, first level
  - Lists, second level

Figures

Figures in this documentation are for better understanding and may differ from the actual product design.

Notes

⚠ DANGER

Type and source of hazard

Possible consequences of hazard that also include death or irreversible injury

- Action step to reduce risk

⚠ WARNING

Type and source of hazard

Possible consequences of hazard that also include severe injury

- Action step to reduce risk

⚠ CAUTION

Type and source of hazard

Possible consequences of hazard that include at least slight injury

- Action step to reduce risk

NOTICE

Type and source of malfunction (property damage only)

Possible malfunctions that may restrict the product's scope of functions or ergonomics, but do not lead to foreseeable risks to persons

- Action step to reduce risk

Note

Notes and information

Indicates information, clarifications, recommendations, referrals, etc.

1.3 Legal Information

Intellectual property

The intellectual property of this document belongs to WAGO GmbH & Co. KG. The reproduction and distribution of its content (in whole or in part) is prohibited, unless otherwise provided by statutory provisions, written agreements or this document. In case of doubt, the written consent of WAGO GmbH & Co. KG must be obtained in advance.

Third-party products are always mentioned without any reference to patent rights. WAGO GmbH & Co. KG, or the manufacturer of third-party products, retains all rights regarding patent, utility model or design registration.

Third-party trademarks are referred to in the product documentation. The "®" and "™" symbols are omitted hereinafter. The trademarks are listed in the Appendix: **Protected Rights [▶ 64]**.

Subject to Change

The instructions, guidelines, standards, etc., in this manual correspond to state of the art at the time the documentation was created and are not subject to updating service. The installer and operator bear sole responsibility to ensure they are complied with in their currently applicable form. WAGO GmbH & Co. KG retains the right to carry out technical changes and improvements of the products and the data, specifications and illustrations of this manual. All claims for change or improvement of products that have already been delivered – excepting change or improvement performed under guarantee agreement – are excluded.

Licenses

The products may contain open-source software. The requisite license information is saved in the products. This information is also available under: **www.wago.com**.

Safety

2.1 General Safety Rules

- This documentation is part of the product. Therefore, retain the documentation during the entire service life of the product. Pass on the documentation to any subsequent user of the product. In addition, ensure that any supplement to this documentation is included, if necessary.
- The product must only be installed and put into operation by qualified electrical specialists per EN 50110-1/-2 and IEC 60364.
- Comply with the laws, standards, guidelines, local regulations and accepted technology standards and practices applicable at the time of installation.

2.2 Electrical Safety

- Make sure the product does not carry any voltage before starting work.

Grounding/Protection/Fuses

- When handling the product, please ensure that environmental factors (personnel, work space and packaging) are properly equalized. Do not touch any conducting parts.

Cables

- Use shielded cables with copper braiding or tinned copper braiding. This reduces electromagnetic interference and increases signal quality. Measurement errors, data transmission errors and interference due to excessive voltage can be prevented.
- Maintain spacing between control, signal and data lines and the power supply lines.
- Observe permissible temperature range of connecting cables.
- Use appropriate strain relief.

2.3 Mechanical Safety

- As the installer of the system, you are responsible for ensuring the necessary touch-proof protection. Follow the installation guidelines for the specific application.
- Before startup, please check the product for any damage that may have occurred during shipping. Do not put the product into operation in the event of mechanical damage.
- Replace any defective or damaged devices.
- Do not open the product housing.
- The product is an open-type device and is designed for installation in an additional enclosure, which supplies the following safety aspects:
  - Restrict access to authorized personnel and may only be opened with tools.
  - Ensure the required pollution degree in the vicinity of the system.
  - Offer adequate protection against direct or indirect contact.
  - Offer adequate protection against UV irradiation.
  - Prevent fire from spreading outside of the enclosure.
  - Guarantee mechanical stability.

2.4 Thermal Safety

- The surface of the housing heats up during operation. Under special conditions (e.g., in the event of a fault or increased surrounding air temperature), touching the product may cause burns. Allow the product to cool down before touching it.
- The temperature inside the additional enclosure must not exceed the surrounding air temperature permitted for the mounted product.
- Cooling of the product must not be impaired. Ensure air can flow freely and that the minimum clearances from adjacent products/areas are maintained.

2.5 Indirect Safety

- Only use a dry or cloth or a clothed dampened with water to clean the product. Do not use cleaning agents, e.g., abrasive cleaners, alcohols or acetone.
- Clean tools and materials are imperative for handling the product.
- Before installation and operation, please read the product documentation thoroughly and carefully. In addition, note the information on the product housing and further information, e.g. at **www.wago.com**/<item number>.
- The product contains no parts that can be serviced by the user. Always have all service, maintenance and repair work performed by specialists authorized by WAGO.

Properties

3.1 Overview

The 2789-9052 Modbus TCP Communication Module supports ETHERNET-based communication with a lower-level product. [1] It functions as a gateway. The following protocols are supported:

- Modbus TCP
- Modbus UDP, firmware version 02.00.00 and higher
- BootP, firmware version 02.00.00 and higher
- DHCP
- SNTP
- HTTP
- HTTPS with TLS 1.3

The integrated switch with two external RJ45 ports makes it possible to set up a line topology without additional infrastructure elements, e.g., switches or hubs.

[1] *For example a WAGO Power Supply Pro 2, firmware version 01.04.xx or higher.*

3.2 View

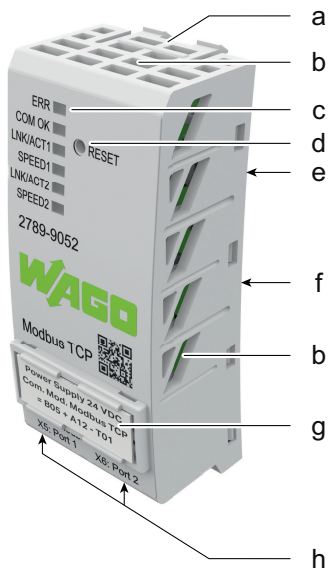


Figure 1: View

Position	Comment	Details
a	Locking tab	–
b	Ventilation openings	–
c	Optical status indication	**Indicators [▶ 14]**
d	Reset button	**Control Elements [▶ 15]**
e	Communication interface	–
f	Type label	**Type label [▶ 12]**
g	Marker carrier	**Accessories – Marking [▶ 63]**
h	ETHERNET port 1 (X5); ETHERNET port 2 (X6)	-

3.3 Type label

The product's type plate contains the following information:

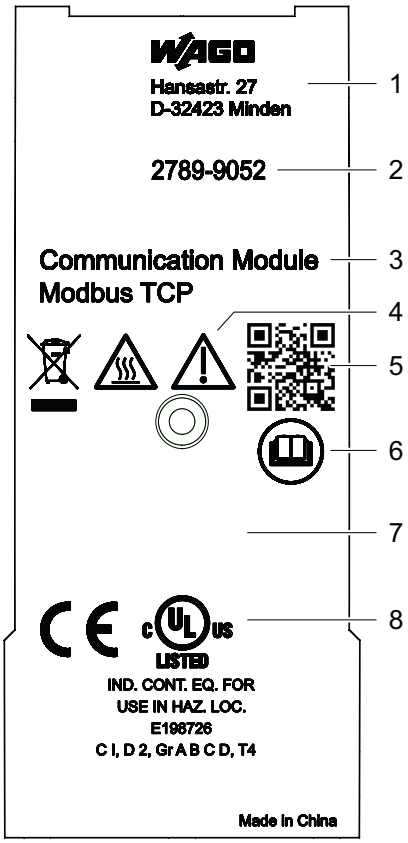


Figure 2: Type label

Position	Comment	Details
1	Company logo and address	–
2	Item number	–
3	Product name	–
4	Warning notice symbols	Safety [▶ 9]
5	QR link with link to website	–
6	Reference to product documentation	–
7	Product-specific information	Product-Specific Information [▶ 12]
8	Box for approvals	Approvals [▶ 16]

3.4 Product-Specific Information

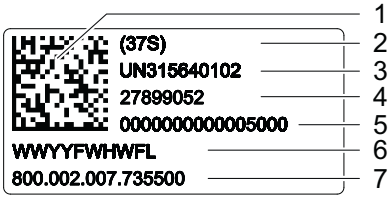


Figure 3: Product-Specific Information

Position	Comment	Details
1	2D data matrix code	Contains the information for positions 2 … 5
2	Key number	Fixed information (37S)
3	ID number per D-U-N-S®	Fixed information (WAGO Minden)
4	WAGO item number or internal SAP number	Product-specific
5	Consecutive number	Product-specific
6	Production date and revision	• Production date • Revision index (xx yy zz)
7	Internal manufacturer product number	Product-specific

Table 1: Revision index structure

Software index	Hardware index	Boot loader index
xx	yy	zz

3.5 Connections

3.5.1 Power Supply

The communication module is powered via the communication interface of the lower-level device.

3.5.2 RJ-45 Interfaces

The connection to ETHERNET-based fieldbuses is established via two RJ45 connectors (see figure “RJ45 Interfaces X5/X6”), also called “Western plugs”, which are connected to the fieldbus controller via an integrated switch.

The integrated switch works in store-and-forward mode and supports 10/100 Mbit/s transmission speeds, as well as full and half-duplex transmission modes, for each port.

The RJ45 sockets are wired in accordance with the specifications for 100BaseTX.

The ETHERNET standard stipulates a twisted pair cable of at least Category 5e as a connecting cable. S/UTP (Screened Unshielded Twisted Pair) and STP (Shielded Twisted Pair) type cables with a maximum segment length of 100 m can be used.

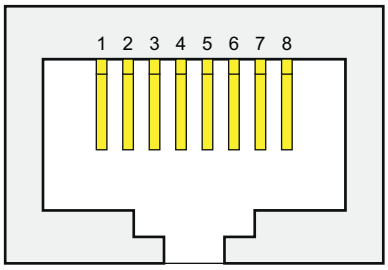


Figure 4: RJ45 Interfaces X5/X6

Pin	Description
1	Transmit data +
2	Transmit data −
3	Receive data +
4	–
5	–

Pin	Description
6	Receive data −
7	–
8	–

3.6 Indicators

The product has a visual status indicator. This indicator consists of six LEDs.

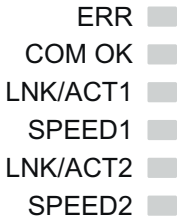


Figure 5: Visual Status Indicator

Table 2: Operating Status Indication

Indicator		LED Description	Status	Description
ERR		Error	Off	Ready for operation; no error present
			On	General error, or reset button pressed
			Flashing (8 Hz)	No communication or connection error to the lower-level device
			Flashing (16 Hz)	Module resets to factory defaults
COM OK		Device status	On	Initialization
			Flashing (2 Hz)	Communication active
			Flashing (16 Hz)	DHCP state machine active (module receives network settings)
LNK/ACT1		Port 1: connection/activity	Off	There is no connection
			On	There is a connection, but no activity
			Flashing	There is a connection and activity
SPEED1		Port 1: speed	Off	Connection rate: 10 Mbit/s
			On	Connection rate: 100 Mbit/s
LNK/ACT2		Port 2: connection/activity	Off	There is no connection
			On	There is a connection, but no activity
			Flashing	There is a connection and activity
SPEED2		Port 2: speed	Off	Connection rate: 10 Mbit/s
			On	Connection rate: 100 Mbit/s

3.7 Control Elements

A reset button is located on the front of the product. This button can be used to reset the product.

See Operation [▶ 36] for a detailed description of how you can use this button to make settings.

3.8 Technical data

3.8.1 Product

Table 3: Technical Data – Product

Property	Value
Width	35 mm
Height	80 mm
Depth	22 mm
Weight	45 g
Degree of protection	IP20

3.8.2 Power Loss

Table 4: Technical Data – Power Loss

Property	Value
Power loss (max.)	1.1 W

3.8.3 Communication

Table 5: Technical Data – Communication

Property	Value
Communication	Modbus TCP, Modbus UDP firmware version 02.00.00 and higher
Interface	RJ-45 interface
Cable length	≤ 100 m
Transmission medium	Twisted pair, shielded
Transmission rate	100 MBd (ETHERNET: 10/100 Mbit/s)
ETHERNET protocols	HTTP(S), BootP firmware version 02.00.00 and higher, DHCP, SNTP
Specifications of the conductors used	≥ +75 °C (ambient air temperature: ≤ +60 °C)

3.8.4 Environmental Conditions

Table 6: Technical Data – Environmental Conditions

Property	Value
Test voltage (fieldbus)	0.775 kVAC, 50 Hz, 1 min.
Type of insulation	Functional insulation
Ambient temperature, operation[1]	−40 … +55 °C
Ambient temperature, storage	−40 … +85 °C
Relative humidity	5 … 95 % (no condensation)
Elevation above sea level, max.	5000 m
Pollution degree according to IEC/EN 60664-1	2
Protection class	III
Protection type[2]	IP20

[1] When the Modbus TCP communication modules is used in combination with a WAGO Power Supply Pro 2 approved for a maximum ambient temperature of +70 °C, a maximum ambient temperature of +55 °C must not be exceeded during operation.
[2] The lower-level WAGO Power Supply Pro 2

3.9 Guidelines, approvals and standards

3.9.1 Guidelines

An EU “Declaration of Conformity” and CE marking exist for the product.

3.9.2 Approvals

The following approvals have been granted for the product:

Table 7: Approvals

Logo	Certification Body	Standard
	Underwriters Laboratories Inc. (Ordinary Locations)	UL 61010-1
	Underwriters Laboratories Inc. (Ordinary Locations)	UL 61010-2-201
	Underwriters Laboratories Inc. (Hazardous Locations)	UL 121201

Note

More information on approvals

You can find detailed information on the approvals online at:
www.wago.com/<item number>

3.9.3 Standards

Table 8: Mechanical and Climatic Environmental Conditions

Standard	Test Value
Mechanical Environmental Conditions	
EN 60068-2-6	f = 5 …150 Hz: 1g, 3.5 m
IEC 60068-2-27, Shock	15g, 11 ms, 6 shocks per axis and direction, half-sine

Standard	Test Value
EN 61131-2, sec. 4.3	Freefall ≤ 300 mm (packaged in the product packaging)
Climatic Environmental Conditions	
EN 60870-2-2	3K3 (except for low air pressure)

Table 9: EMV – Immunity to Interference

Standard	Title
EN 61000-6-2	Part 6-2: Generic standards – Immunity for industrial environments*
EN 61000-4-2	Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test
EN 61000-4-3	Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test
EN 61000-4-4	Part 4-4: Testing and measurement techniques – Electrical fast transient/ burst immunity test
EN 61000-4-5	Part 4-5: Testing and measurement techniques – Surge immunity test
EN 61000-4-6	Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields

** If there is interference, there may be performance deviations.*

Table 10: EMC – Emission of Interference

Standard	Title
EN 61000-6-3	Part 6-3: Generic standards – Emission standard for residential, commercial and light-industrial environments

Fieldbus Description

4.1 Technology

4.1.1 TCP/IP

The Internet Protocol (IP) separates data telegrams into segments and is responsible for transporting them from one network station to the other. During this process, the stations involved can be located either in the same network or in different physical networks that are connected to each other with routers. The routers are able to select various network transmission paths through a network connection, thus avoiding overloads and disruptions of individual networks. However, certain segments may be chosen that are shorter than others, allowing the data telegrams to overtake each other and yielding an incorrect data packet order. For this reason, correct transmission must be guaranteed at higher levels, e.g., through TCP. In addition to the user data to be transported, the IP data packets include a great deal of address information and additional information in the packet header.

4.1.2 HTTP/HTTPS

The HTTP/HTTPS server implemented on the Modbus TCP Communication Module reads HTML pages from the communication module and the lower-level device.

The HTTP server uses port number 80.

The HTTPS server uses port number 443.

4.1.3 Hardware Address (MAC ID)

The Modbus TCP Communication Module carries a globally unique physical address, the MAC ID (Media Access Control Identity). The MAC ID is printed on the bottom of the housing. The MAC ID has a set length of 6 bytes (48 bits) (hexadecimal). The first 3 bytes provide information about the manufacturer (e.g., 00:30:DE for WAGO). The other 3 bytes contribute to a globally unique MAC address.

4.2 Communication Module

4.2.1 Function Codes

The Modbus specification defines various function codes (FCs). The following three function codes are supported by all products in the WAGO Power Supply Pro 2 Series:

Table 11: Function Codes

FC	Name	Description
FC3	Read Holding Register	Reads the parameters from the product
FC4	Read Input Register	Reads the measured values from the product
FC16	Write Multiple Register	Writes the parameters to the product

4.2.2 Exception Codes

Exception codes per the Modbus specification (“frame exceptions”):

Table 12: Exception Codes

Code	Name	Description
0x01	Illegal Function	Function not supported
0x02	Illegal Data Address	Parameter not available at this address
0x03	Illegal Data Value	Parameter length invalid; structure error, CRC error

User-defined exception codes (“parameter exception”):

Table 13: User-Defined Exception Codes

Code	Name	Description
0x9B	PAR_READONLY	Write to parameter “read only”
0xA8	VAL_OUTOF_RNG	Value out of range
0xAD	FUNC_NOTAVAIL	Write invalid value to command parameter
0xAE	FUNC_NOTAVAIL_ TEMP	Command not possible due to current command status (e.g., during block parameterization that is not closed; other commands are rejected)
0xB8	PAR_SETINVALID	Parameter single access: Parameter value inconsistent with other parameter values
0xB9	PAR_SETINCONSIST	Block parameterization: Parameter set inconsistent
0xD0	PASS_PROTECTION_ACTIVE	No parameter access; password protection enabled

4.3 Module Parameters

4.3.1 Internal Module Parameters

Starting with address offset 0xFD00, internal module parameters such as network settings and module information are addressed.

Cross-Device Information for Identification

Table 14: Internal Module Parameters — Cross-Device Information for Identification

Address		Access	Data Type	Description	Value Limits		
Dec.	Hex.				Factory Settings	Min	Max
64770	0xFD02	Read-only	UINT32	Module item number	0x28579052		
64776	0xFD08	Read-only	UINT32	Consecutive number (“high word”)	0		
64778	0xFD0A	Read/write	UINT32	Consecutive number (“low word”)	0		
64780	0xFD0C	Read-only	UINT16	Firmware version (major)	1		
64781	0xFD0D	Read-only	UINT16	Firmware version (minor)	0		
64782	0xFD0E	Read-only	UINT16	Firmware version (bug fix)	0		
64783	0xFD0F	Read-only	UINT16	Hardware version	1		
64788	0xFD14	Read-only	CHAR[34]	Fixed item description of the device	“Modbus TCP Communication Module”		
64805	0xFD25	Read/write	CHAR[34]	Location name	“”		
64822	0xFD36	Read/write	CHAR[34]	Function name	” ”		
64839	0xFD47	Read/write	CHAR[34]	Customer information	” ”		

General ETHERNET Settings

Table 15: Internal Module Parameters – General ETHERNET Settings

Address		Access	Data Type	Description	Value Limits		
Dec.	Hex.				Factory Settings	Min	Max
64874	0xFD6A	Read-only	CHAR[6]	MAC address of the communication module			
64877	0xFD6D	Read/write	CHAR[4]	IP address of the communication module	192.168.1 17		
64879	0xFD6F	Read/write	CHAR[4]	Subnet mask of the communication module	255.255.255.0		
64881	0xFD71	Read/write	CHAR[4]	Gateway address	192.168.1.1		
64884	0xFD74	Read/write	UINT16	Enables fast aging (0 = off, 1 = on)	0		
64886	0xFD76	Read/write	UINT16	Enables WBM via HTTP (0 = off, 1 = on)	1	0	1
64887	0xFD77	Read/write	UINT16	Enables WBM via HTTP	1	0	1
64888	0xFD78	Read/write	UINT16	Enables SNTP (0 = off, 1 = on)	0	0	1
64892	0xFD7C	Read/write	CHAR[4]	IP address of the SNTP server	192.168.1.109		

Switch Settings for Channel 1

Table 16: Internal Module Parameters – Switch Settings for Channel 1

Address		Access	Data Type	Description	Value Limits		
Dec.	Hex.				Factory Settings	Min	Max
65004	0xFDEC	Read/write	UINT16	Enables “Autonegotiation” mode (0 = off, 1 = on)	1	0	1
65005	0xFDED	Read/write	UINT16	Forces 100 MB connection (0 = off, 1 = on)	1	0	1
65006	0xFDEE	Read/write	UINT16	Forces full duplex connection (0 = off, 1 = on)	1	0	1
65008	0xFDF0	Read/write	UINT16	Enables BroadcastStormProtection (0 = off, 1 = on)	0	0	1

Switch Settings for Channel 2

Table 17: Internal Module Parameters – Switch Settings for Channel 2

Address		Access	Data Type	Description	Value Limits		
Dec.	Hex.				Factory Settings	Min	Max
65016	0xFDF8	Read/write	UINT16	Enables “Autonegotiation” mode (0 = off, 1 = on)	1	0	1
65017	0xFDF9	Read/write	UINT16	Forces 100 MB connection (0 = off, 1 = on)	1	0	1
65018	0xFDFA	Read/write	UINT16	Forces full duplex connection (0 = off, 1 = on)	1	0	1
65020	0xFDFC	Read/write	UINT16	Enables BroadcastStormProtection (0 = off, 1 = on)	0	0	1

Date

Table 18: Internal Module Parameters – Date

Address		Access	Data Type	Description	Value Limits		
Dec.	Hex.				Factory Settings	Min	Max
				Date			
65028	0xFE04	Read/write	CHAR	Year	20	0	99
65028.5	0xFE04	Read/write	CHAR	Month	12	1	12
65029	0xFE05	Read/write	CHAR	Day	2	1	31

Time

Table 19: Internal Module Parameters – Time

Address		Access	Data Type	Description	Value Limits		
Dec.	Hex.				Factory Settings	Min	Max
65030	0xFE06	Read/write	CHAR	Hours	4	0	24
65030.5	0xFE06	Read/write	CHAR	Minutes	26	0	59
65031	0xFE07	Read/write	CHAR	Seconds	37	0	59
65032	0xFE08	Read/write	INT16	Time zone	2	−12	12
65033	0xFE09	Read/write	UINT16	Synchronization mode (1 = off; 2 = read time from lower-level device; 4 = write time from module; 8 = update time with SNTP)	1		

4.4 Device Parameters

4.4.1 General Device Parameters of Lower-Level Devices

The Modbus TCP Communication Module uses the following general parameters of a lower-level WAGO Power Supply Pro 2. These parameters can be read and written via function codes FC3 and FC16.

Device Identification

Table 20: General Device Parameters – Device Identification

Address		Access	Data Type	Description
Dec.	Hex.			
2	0x0002	Read-only	UNIT32	Item number
4	0x0004	Read-only	UNIT32	Item number extension
8	0x0008	Read/write	UNIT32	Consecutive number (“high word”)
10	0x000A	Read/write	UNIT32	Consecutive number (“low word”)
12	0x000C	Read-only	UNIT16	Firmware version (major)
13	0x000D	Read-only	UNIT16	Firmware version (minor)
14	0x000E	Read-only	UNIT16	Firmware version (bug fix)
15	0x000F	Read/write	UNIT16	Hardware version
20	0x0014	Read-only	CHAR32	Item description
36	0x0024	Read/write	CHAR32	Device name
52	0x0034	Read/write	CHAR32	Customer information (1)
68	0x0044	Read/write	CHAR32	Customer information (2)
84	0x0054	Read-only	CHAR8	Password
92	0x005C	Read/write	CHAR16	Password level

“Password Level” Parameter

The “Password Level” parameter controls the behavior of the lower-level device in terms of password protection. There are four password levels:

- Password level 0 (value 0): No parameters are password protected
- Password level 1 (value 1): All parameters are read-only
- Password level 2 (value 2): All parameters are read- and write-protected
- Password level 3 (value 3): All parameters are read- and write-protected In addition, process data outputs (e.g., “Switch product on and off” or “Activate digital output”) are write-protected.

Table 21: General Device Parameters – “Password Level” Parameter

Password level	Parameter: Write Protection	Parameter: Read Protection	Process Data: Write Protection	Process Data: Read Protection
0	No	No	No	No
1	Yes	No	No	No
2	Yes	Yes	No	No
3	Yes	Yes	Yes	No

General Module Parameters

Table 22: General Module Parameters: Modbus

<table>
<tr><th colspan="2">Address</th><th rowspan="2">Access</th><th rowspan="2">Data Type</th><th rowspan="2">Description</th></tr>
<tr><th>Dec.</th><th>Hex.</th></tr>
<tr><td>122</td><td>0x007A</td><td>Read/write</td><td>UINT16</td><td>Device address</td></tr>
<tr><td>124</td><td>0x007C</td><td>Read/write</td><td>UINT32</td><td>Baud rate
This parameter can be used to set the baud rate.
The options are as follows:
• 4800 baud
• 9600 baud
• 19200 baud
• 38400 baud
• 57600 baud
• 115200 baud</td></tr>
<tr><td>126</td><td>0x007E</td><td>Read/write</td><td>UINT16</td><td>Data bits</td></tr>
<tr><td rowspan="5">127</td><td rowspan="5">0x007F</td><td rowspan="5">Read/write</td><td rowspan="5">UINT16</td><td>Stop bits
The options are as follows:</td></tr>
<tr><td><table><tr><th>Value</th><th>Stop Bit</th></tr><tr><td>0</td><td>1</td></tr><tr><td>1</td><td>0.5</td></tr><tr><td>2</td><td>2.5</td></tr><tr><td>3</td><td>1.5</td></tr></table></td></tr>
<tr><td>128</td><td>0x0080</td><td>Read/write</td><td>UINT16</td><td>Parity
The following options are available:</td></tr>
<tr><td>129</td><td>0x0081</td><td>Read/write</td><td>UINT16</td><td>Response delay</td></tr>
<tr><td>130</td><td>0x0082</td><td>Read/write</td><td>UINT16</td><td>Data format
The following options are available:
• 0: BigEndian (B0, B1, B2, B3)
• 1: MiddleEndian (B2, B3, B0, B1)
• 2: LittleEndian (B3, B2, B1, B0)</td></tr>
</table>

4.4.2 Device Parameters of the WAGO Pro 2 Power Supply

The following parameters of the Pro 2 Power Supply can be edited via the communication module. These parameters can be read and written via function codes FC3 and FC16.

DC Output

Table 23: Parameter – DC Output

Address		Access	Data Type	Description	
Dec.	Hex.				
136	0x0088	Read/write	UNIT16	Output voltage (unit: mV)	
137	0x0089	Read/write	UNIT16	Warning threshold (unit: mA)	
138	0x008A	Read/write	UNIT16	Bit 0	Switch output on
				Bit 1	“Active droop” parallel switching mode
				Bit 2	Overload threshold enabled
				Bit 3	Enable switching on and off of the DC output via cyclic process data
				Bit 4	Reserved
				Bit 5	Reserved
				Bit 6[1]	Constant current
				Bit 7[1]	Constant current with latching shutdown
				Bit 8[1]	Hiccup mode
				Bit 9[1]	Electronic circuit breaker
				Bit 10	Reserved
				Bit 11	Reserved
				Bit 12	Latching shutdown on thermal overload
				Bit 13	PowerBoost
				Bit 14	TopBoost
				Bit 15	Reserved
139	0x008B	Read/write	UNIT16	Switch-on delay (unit: ms)	

1 These bits are mutually interlocked.

“Electronic Circuit Breaker” Mode

Table 24: Parameter – Electronic Circuit Breaker Mode

Address		Access	Data Type	Description
Dec.	Hex.			
148	0x0094	Read/write	UNIT16	Trip current (unit: mA)
149	0x0095	Read/write	UNIT16	Trip delay (unit: ms)

Signaling – Digital Input

Table 25: Parameter – Signaling – Digital Input

Address		Access	Data Type	Description	
Dec.	Hex.				
168	0x00A8	Read/write	UNIT16	Bit 0	Switch power supply on and off
				Bit 1	Reserved
				Bit 2	Reserved
				Bit 3	Reserved
				Bit 4	Reserved
				Bit 5	Reserved
				Bit 6	Reserved
				Bit 7	Reserved
				Bit 8	Reserved
				Bit 9	Reserved
				Bit 10[1]	Inversion
				Bit 11[1]	Function on edge change (0 to 1)
				Bit 12[1]	Function on edge change (1 to 0)
				Bit 13	Reserved
				Bit 14	Reserved
				Bit 15	Reserved

1 These bits are mutually interlocked.

Signaling ─ Digital Output

Table 26: Parameter – Signaling ─ Digital Output

Address		Access	Data Type	Description	
Dec.	Hex.				
176	0x00B0	Read/write	UNIT16	Bit 0	DC O.K.
				Bit 1	Overload threshold exceeded
				Bit 2	Electronic circuit breaker tripped
				Bit 3	Latching shutdown occurs
				Bit 4	Activation of the readout function of the digital output via the process data
				Bit 5	Switching digital output on and off
				Bit 6	Reserved
				Bit 7	Reserved
				Bit 8	Reserved
				Bit 9	Reserved
				Bit 10	Inversion
				Bit 11	Reserved
				Bit 12	Reserved
				Bit 13	Reserved
				Bit 14	Reserved
				Bit 15	Reserved

System

Table 27: Parameter – System

Address		Access	Data Type	Description	
Dec.	Hex.				
189	0x00BD	Read/write	UNIT16	Bit 0[1]	Behavior when power supplied – previous state restored
				Bit 1[1]	Behavior when power applied – DC output is switched on
				Bit 2[1]	Behavior when power applied – DC output is switched on
				Bit 3	Switch-on delay enabled
				Bit 4	Reserved
				Bit 5	Reserved
				Bit 6	Enable button lock
				Bit 7	Lock resetting to factory settings
				Bit 8	Reserved
				Bit 9	Reserved
				Bit 10	Inversion
				Bit 11	Reserved
				Bit 12	Reserved
				Bit 13	Reserved
				Bit 14	Reserved
				Bit 15	Reserved

1 These bits are mutually interlocked.

4.4.3 Events and Measured Values for WAGO Power Supply Pro 2

The Modbus TCP Communication Module outputs the WAGO-specific events and measured values listed below. These events and measured values can be read via function codes FC3 and FC4.

Process Output Data

Table 28: Events and Measured Values – Process Input Data

Address				Data Type	Description
FC3		FC4			
Dec.	Hex.	Dec.	Hex.		
1280	0x0500	0	0x0000	UNIT16	Output voltage (unit: mV)
1281	0x0501	1	0x0001	UNIT16	Output current (unit: mA)

Status Messages

Table 29: Events and Measured Values – Status Messages

Address				Data Type	Description	
FC3		FC4				
Dec.	Hex.	Dec.	Hex.			
1282	0x0502	2	0x0002	UNIT16	Bit 0	DC status O.K.
					Bit 1	Overtemperature
					Bit 2	No output voltage
					Bit 3	Short circuit at output
					Bit 4	Status at digital input

Warnings

Table 30: Events and Measured Values – Warnings

Address				Data Type	Description	
FC3		FC4				
Dec.	Hex.	Dec.	Hex.			
1283	0x0503	3	0x0003	UNIT16	Bit 0	Undervoltage at output
					Bit 1	Overvoltage at output
					Bit 2	Overload
					Bit 3	Configurable overload threshold exceeded
					Bit 4	Configurable operating hours reached
					Bit 5	Top boost output
					Bit 6	Power boost output
					Bit 7	Higher device temperature
					Bit 8	-

Error

Table 31: Events and Measured Values – Errors

Address				Data Type	Description	
FC3		FC4				
Dec.	Hex.	Dec.	Hex.			
1284	0x0504	4	0x0004	UNIT16	Bit 0	Overtemperature, device switched off
					Bit 1	No output voltage
					Bit 2	Short circuit at output
					Bit 3	Circuit breaker tripped

Power/Energy

Table 32: Events and Measured Values – Power/Energy

Address				Data Type	Description
FC3		FC4			
Dec.	Hex.	Dec.	Hex.		
1286	0x0506	6	0x0006	UNIT32	Output power (unit: W)
1288	0x0508	8	0x0008	UNIT32	Output level of the previous second (unit: Ws)
1290	0x050A	10	0x000A	UNIT32	Output level of the previous minute (unit: Ws)
1292	0x050C	12	0x000C	UNIT32	Output level of the previous hour (unit: Wh)

Transport and Storage

The original packaging offers optimal protection during transport and storage.

- Store the product in suitable packaging, preferably the original packaging.
- Only transport the product in suitable containers/packaging.
- Make sure the product contacts are not contaminated or damaged during packing or unpacking.
- Observe the specified ambient climatic conditions for transport and storage.

Installation and Removal

NOTICE

Avoid electrostatic discharge!

The products are equipped with electronic components that you may destroy by electrostatic discharge when you touch. Please observe the safety precautions against electrostatic discharge in accordance with EN 61340-5-1/-3. Pay attention while handling the products to good grounding of the environment (persons, job and packing).

NOTICE

Do not cover the ventilation openings!

To ensure adequate air circulation, the ventilation openings must be kept clear. Maintain a distance of at least 50 mm from the ventilation openings to adjacent surfaces.

The letters shown in parentheses refer to positions in figure “View” in section View [▶ 11].

Note

Mounting positions

The nominal mounting position is (see also figure “View” in View [▶ 11]): front side facing forwards, marking legible, bottom ventilation openings (b) facing upwards and downwards

Mounting

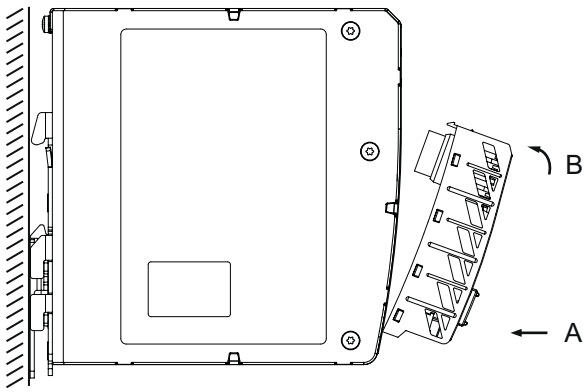


Figure 6: Mounting

Install the product by snapping it onto the WAGO Power Supply Pro 2 (see figure “Installation”):

1. Remove the cap from the communication interface on the WAGO Power Supply Pro 2.
2. Keep the cap in a safe place so that you can cover the communication interface again when this interface is not required.
3. Remove the mounted marker carrier from the WAGO Power Supply Pro 2.

4. Insert the product with the lower latches into the lower mounting slots of the WAGO Power Supply Pro 2 [A].
5. Slide the product toward the communication interface [B] until the top latches latch into the top mounting slots.
6. Verify that the product is snapped on properly.

Removal

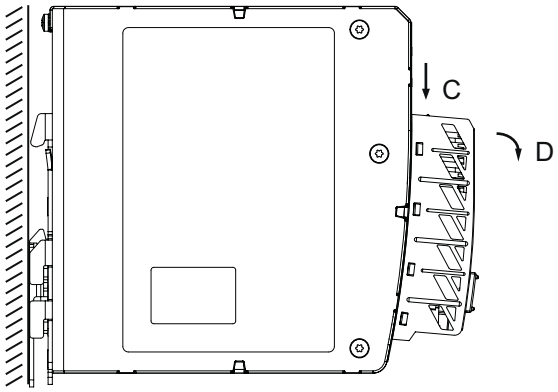


Figure 7: Removal

1. Press the top locking tab (a) of the product [C].
2. Pivot the product to remove it from the WAGO Power Supply Pro 2 [D].

Commissioning

7.1 Version Information

- The Modbus TCP communication module with firmware version 01.00.03 is not compatible with Pro 2 Power Supplies with firmware versions >= 01.05.13.
  In such cases, proceed as follows:

1. Update the communication module to a firmware version > 02.00.00.
2. Then update the firmware version of the power supply.

- If you have a communication module with firmware version 01.00.03 and only have a power supply with firmware version > 01.05.17, proceed as follows:

1. Snap the module onto a power supply with version <= 01.05.13, or downgrade the power supply to a version <= 01.05.17.
2. Update the communication module.
3. Update the power supply to the current firmware.

7.1.1 Compatibility

Table 33: Compatibility

Firmware Version of 2789-9052 Communication Module	Compatible with Firmware Versions of the Pro 2 Power Supply (2787-2xxxx Power Supplies)
01.00.03	From 01.04.00 to 01.05.13
02.00.04	01.04.00 and above

7.2 Setting an IP address

7.2.1 Assigning an IP Address Using DHCP

✓ Install the Modbus TCP Communication Module on a lower-level WAGO Power Supplies Pro 2 (firmware 01.04 or higher).

✓ Connect the Modbus TCP Communication Module to a computer via a network cable and integrate it into a network.

✓ Supply the lower-level WAGO Power Supplies Pro 2 with power.

✓ If there is a DHCP in the network:

- Assign the network settings to the Modbus TCP Communication Module.

✓ For the communication module, dynamic assignment of the IP address using the “Dynamic Host Configuration Protocol” (DHCP) is enabled by default.

- When the DHCP protocol is enabled, make sure a DHCP is always available.

✓ If the IP address was assigned via DHCP:

1. Determine this address via the settings or the output of the respective DHCP server, for example via the output of “Open DHCP.”
2. If no DHCP server is available after a power-on reset, the default network settings are made after four attempts (approx. 30 seconds).

⇨ Configuration type: static IP address

⇨ IP address: 192.168.1.17

⇨ Gateway address: 192.168.1.1

ⓘ Note

Total network failure if there are two DHCP servers on the network!

To prevent network failure, never connect a PC on which a DHCP server is installed to a global network. In larger networks, there is usually already a DHCP server that can cause collisions and subsequent network failure.

ⓘ Note

Assign a fixed IP address to the DHCP server and ensure that a common subnet exists!

Note that the DHCP server must have a fixed IP address and that the communication module and DHCP server must be in the same subnet.

ⓘ Note

IP addresses obtained via DHCP server only valid temporarily!

Note that an IP address obtained via a DHCP server is only valid for a limited period of time. If the DHCP server is not available after the service life has elapsed, the fieldbus node releases the IP address and can then no longer be reached!

7.2.2 Setting a Fixed IP Address

To use the IP address permanently, you can switch the addressing to “static.” The following options are available for this:

- Setting the IP address via the WBM
- Setting the default IP address with the reset button
- Setting the IP address via the Modbus command

Setting the IP Address via the WBM

1. Open the WBM (Web-Based Management) of the communication module in a browser.
2. Switch to the **Module Settings > Network** page of the WBM.
3. In the **Ethernet Settings** area, you can make the required network settings.

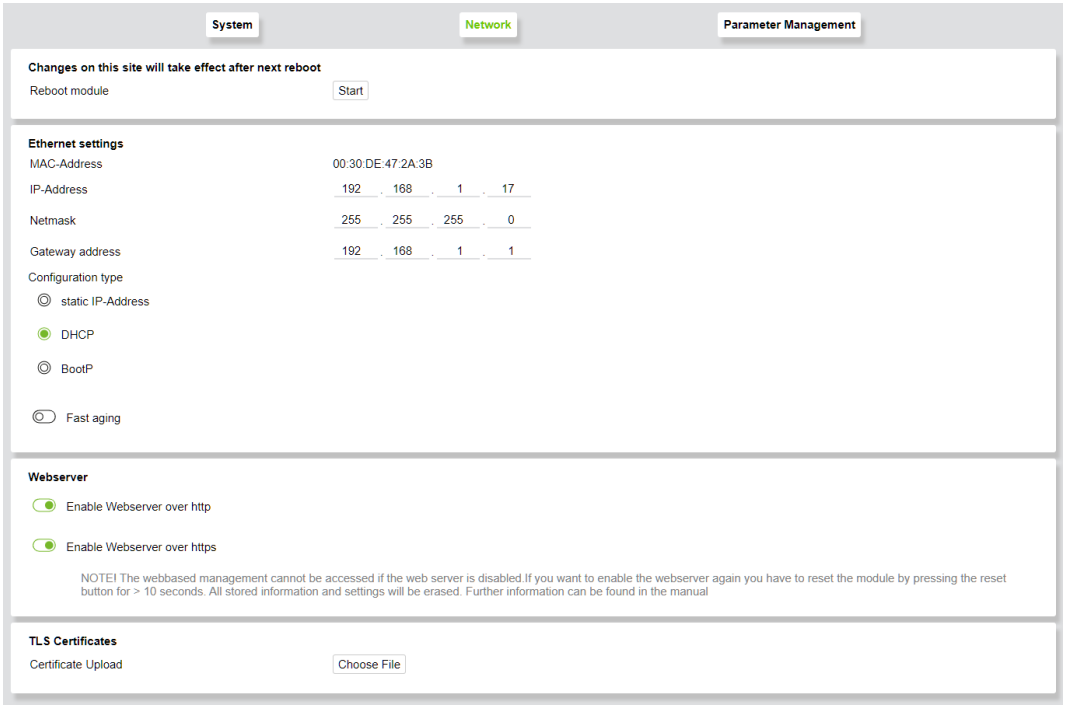


*Figure 8: **Module Settings > Network** Page*

Note

The communication module must be restarted for the settings to be applied.

4. To do so, press the **[Start]** button in the **Reboot** section of the **Module Settings > System** page of the WBM, or power cycle your system.

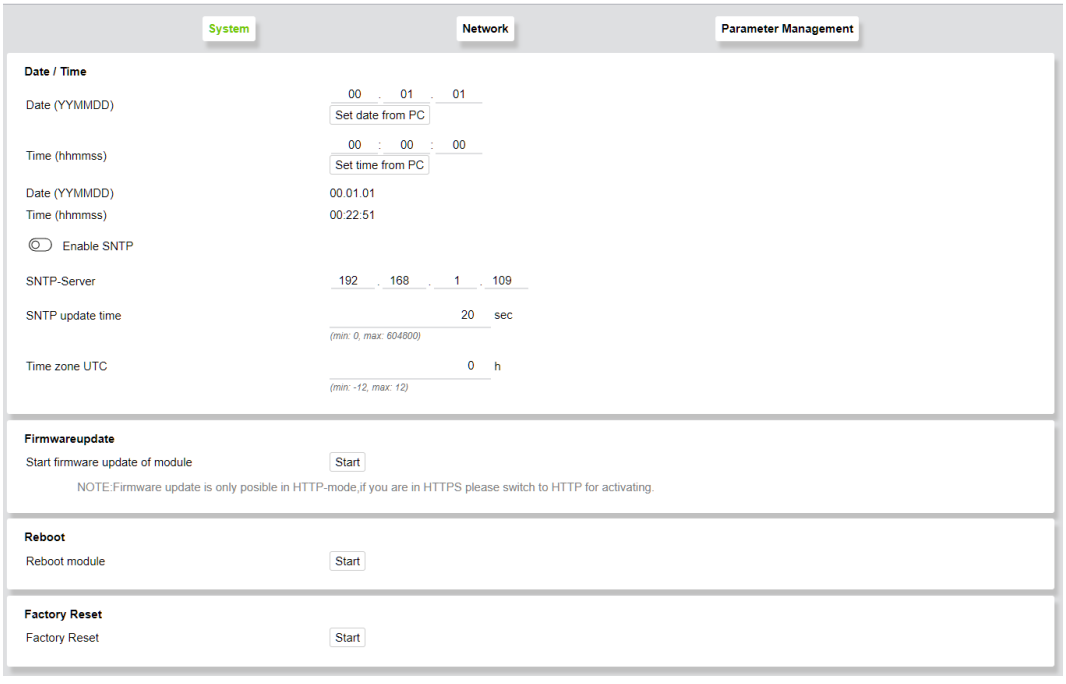


*Figure 9: **Module Settings > System** Page*

Setting the Default IP Address with the Reset Button

Note

If you no longer have the IP address of the module, you can reset the network settings with the reset button on the module.

1. Hold the reset button down for eight seconds until the “COM OK” LED lights up briefly.
2. Release the reset button.

⇨ The Modbus TCP Communication Module reboots, and the following network settings are made:
Configuration type: Static IP address
IP address: 192.168.1.17
Gateway address: 192.168.1.1

Setting the IP Address via the Modbus Command

- Via Modbus FC10, write to the corresponding addresses from section **Internal Module Parameters [▶ 20]**

7.2.3 Assigning an IP Address Using BootP

Note

Assigning the IP address with the BootP server

A fixed IP address is assigned automatically with a BootP server. The process of assigning the IP address using a BootP server depends on the specific BootP program. The procedure is described in the corresponding manual for the program or in the corresponding integrated help texts.

✓ A BootP server is installed on your local PC.
✓ DHCP is enabled by default upon delivery. Therefore, for IP address assignment via BootP, it is necessary to enable BootP, for example via the WBM.
✓ When the BootP protocol is enabled, the communication module expects a BootP to always be available. If no BootP server is available after a power-on reset, the default setting is made after four attempts (about 0.5 min).

1. Assign the desired IP address for your fieldbus node according to the specifications of the manual (or the help texts) for the BootP program.
2. Restart the communication module.

⇨ The communication module then starts up with the new IP address assigned via BootP.

Reasons for Failed IP Address Assignment

- The PC on which the BootP server is running is not in the same network as the fieldbus coupler/controller, i.e. the IP addresses do not match

  - Example:
    Subnet mask: 255.255.255.0 (default value of the communication module)
    PC IP: 192.168.2.100
    Communication module IP: 192.168.1.17
  - Due to the subnet mask, the first three digits of the IP addresses must match.
- PC and/or fieldbus coupler/controller has no ETHERNET connection

Operation

8.1 Operating via Reset Button

The reset button can be used to reset the product.

The following settings options are available:

Table 34: Using the Reset Button

Settings Options	Description	Signaling via Visual Status Display
Hold reset button down for eight seconds	Disables DHCP and sets the IP address to 192.168.1.17	COM OK flashes once
Hold reset button down for ten seconds	Resets the Modbus TCP Communication Module to factory settings	ERR flashes at 16 Hz

Configuration

9.1 Configuring with WBM

Using the Web-Based Management (WBM), you can view parameters and measured values of the communication module and the lower-level device and make changes via a Web browser.

9.1.1 Logging In

If the lower-level device is password-protected, one of the following messages appears, depending on the password level:

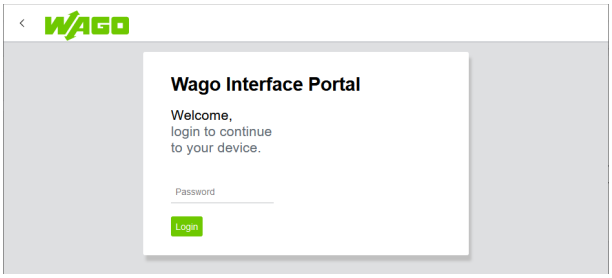


Figure 10: Login with Read/Write Protection

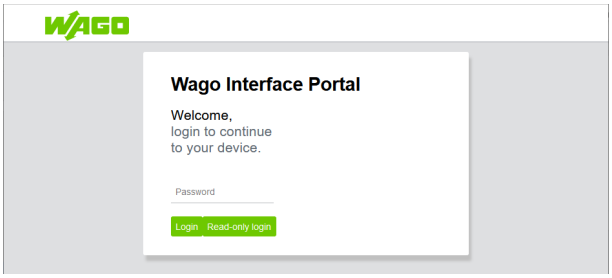


Figure 11: Login with Read Protection

If the lower-level device is read and write protected, it must always be unlocked with a password (see figure “Login with Read/Write Protection”). With read protection, it is possible to either log in with **[Read-Only Login]** without entering a password or unlock it completely by entering the correct password.

9.1.2 Menu Page

✓ The lower-level device is not password-protected
OR

✓ Logging in with a password is possible

• Log in.

⇨ The menu page of the WBM appears with the pages offered.

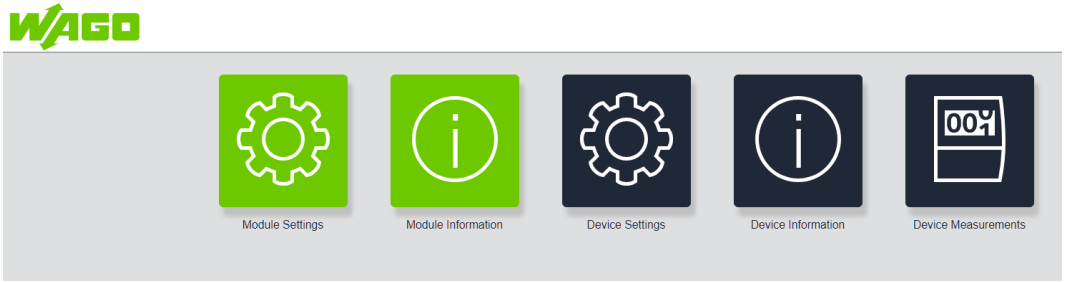


Figure 12: Menu Page

On the menu page, you will see tiles offering the following entry points:
- Module Settings
- Module Information
- Device Settings
- Device Information
- Device Measurements

9.1.3 Module Settings

System

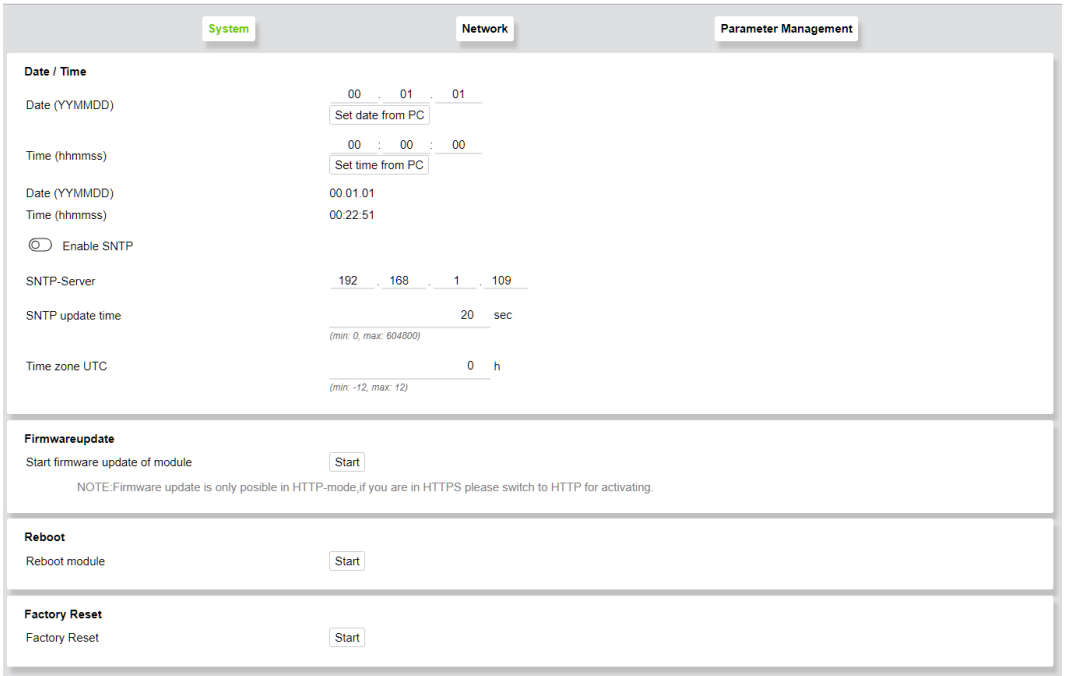


*Figure 13: **Module Settings > System***

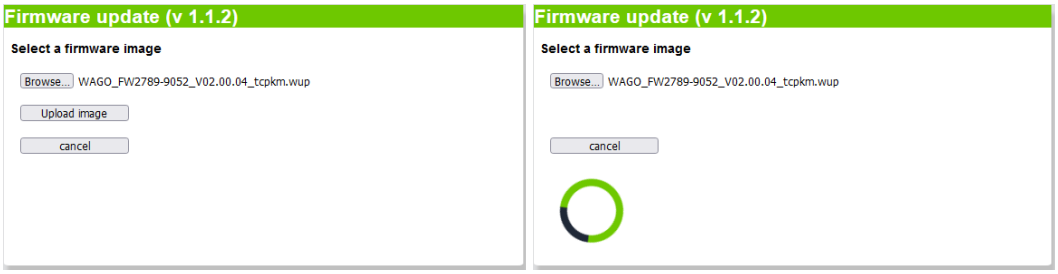
Date / Time: Here you can set the module's date and time.
- Manual
- Use current PC time
- Get the time from an SNTP server

ⓘ Note

Restart after configuring SNTP

After SNTP is configured, the module must be restarted with **[Reboot Module]** or a by power cycling it.

Firmware Update: You can also update the firmware of the module. Clicking the **[Start]** button takes you out of the application and launches the internal firmware loader.



Note

Notes on updating the firmware

Please note that the module firmware can only be updated via the HTTP protocol. If the WBM was accessed via HTTPS, it is necessary to access the Web page manually via HTTP.

While the firmware loader is active, module tasks cannot be executed.

If the firmware loader is interrupted during the update process, the module remains in firmware loader mode permanently until a firmware image is loaded.

After the firmware update ends, it may be necessary to manually refresh the page.

[Reboot] button: module restart; necessary after network settings are modified

[Factory Reset] button: resets the module parameters to the factory settings

Network

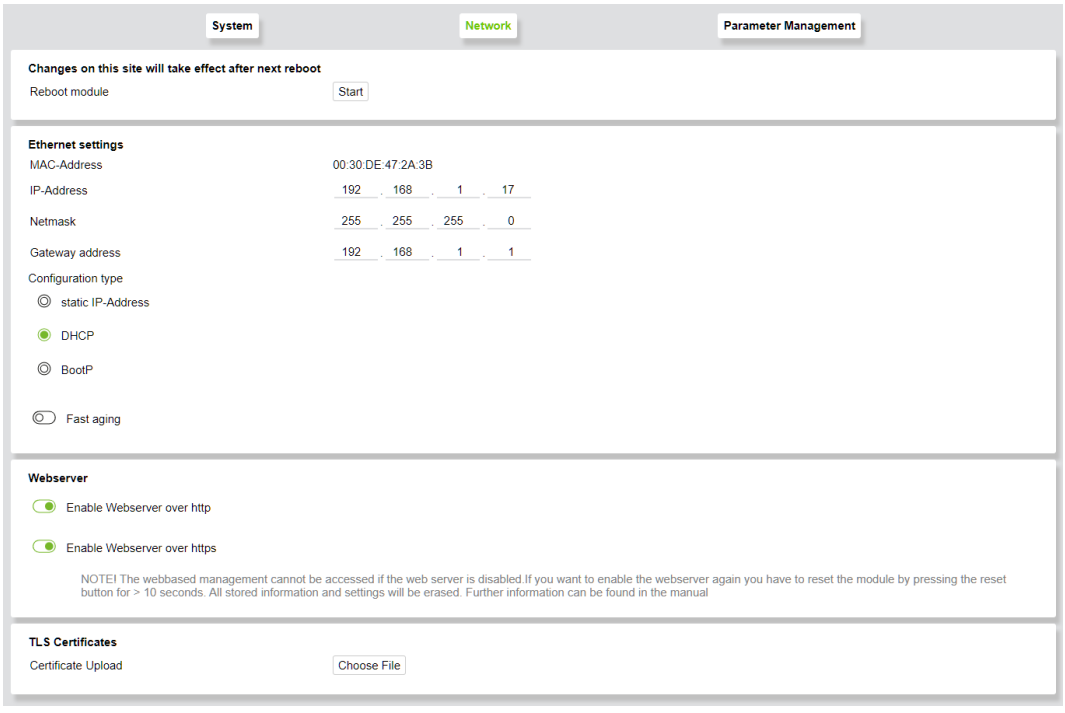


*Figure 14: **Module Settings > Network***

[Ethernet Settings] button: for setting the network parameters and addressing type

[Webserver] button: Here you can switch the HTTP and HTTPS protocols on or off

ⓘ Note

Re-enabling Webserver access

Disabling the Webserver closes ports 80 and 443; the module is then no longer accessible via Web browser. To re-enable access via the Webserver, you must hold the reset button on the module down physically on site for longer than ten seconds – the module then resets to the factory settings – or set register 0xFD76 for HTTP or 0xFD77 for HTTPS to 1 via Modbus TCP.

[TLS Certificates] button: for loading your own TLS certificates for the HTTPS protocol

Parameter Management

Here you can save the current settings of the module and lower-level device and transfer them to other devices of the same type.

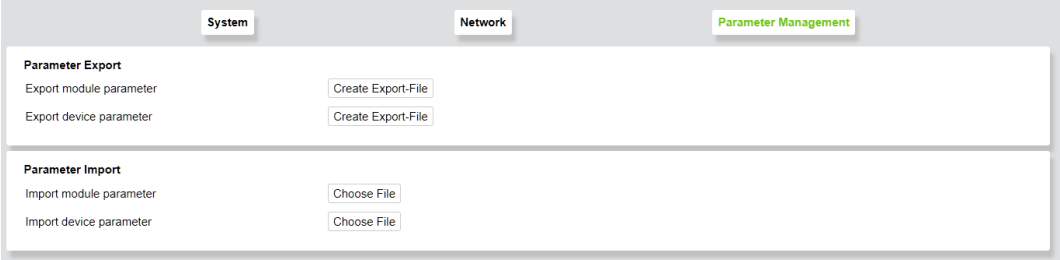


Figure 15: ***Parameter Management***

Switch Settings

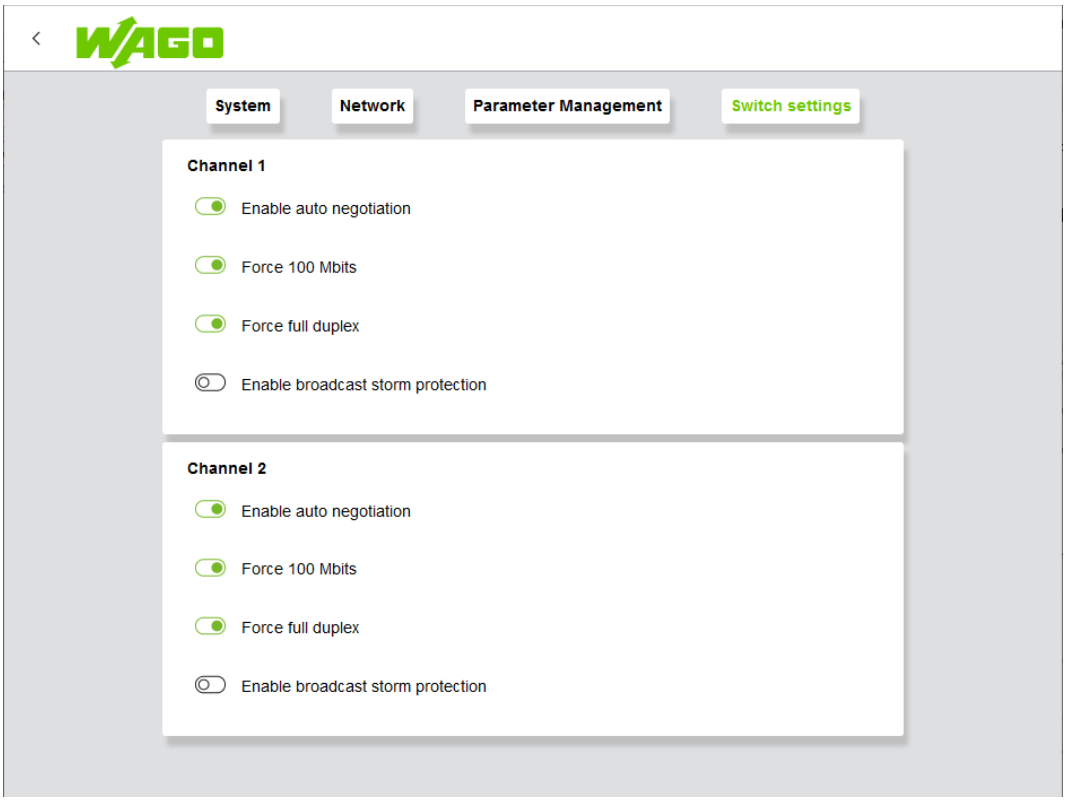


Figure 16: ***Switch Settings***

- **Enable Autonegotiation:** Autonegotiation allows the UTP (Unshielded Twisted Pair) link partners to select the best common operating mode in accordance with Clause 28 of the IEEE 802.3u specification. With autonegotiation, the link partners share their capabilities with each other over the link.
- **Force 100 Mbits:** forces the connection over 100 Mbit
- **Force Full Duplex:** forces the connection using full duplex
- **Enable Broadcast Storm Protection:** option to protect the switch system from receiving too many broadcast packets. Since the broadcast packets are forwarded to all ports except the source port, an excessive number of switch resources (bandwidth and available space in the send queues) can be consumed. The module can optionally take “multicast packets” into account for storm control.

9.1.4 Module Information

Information from the communication module

General

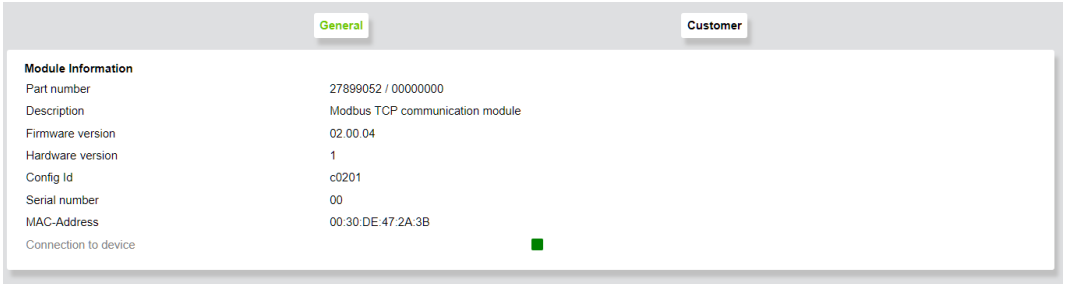


Figure 17: ***Modul Information > General***

Displays all module information and indicates the status of the connection to the lower-level device:

- Green: connection established
- Red: connection interrupted

Customer

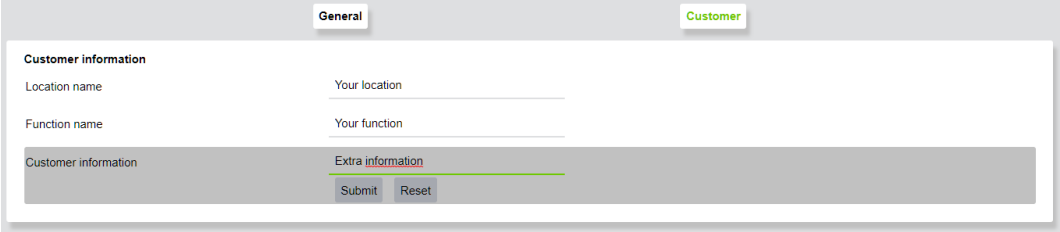


Figure 18: ***Modul Information > Customer***

Users can enter system and location information here.

9.1.5 Device Settings

All parameters are read from the lower-level device and displayed on the **Device Parameter** page. In what follows, this is illustrated on the example of a Pro 2 Power Supply.

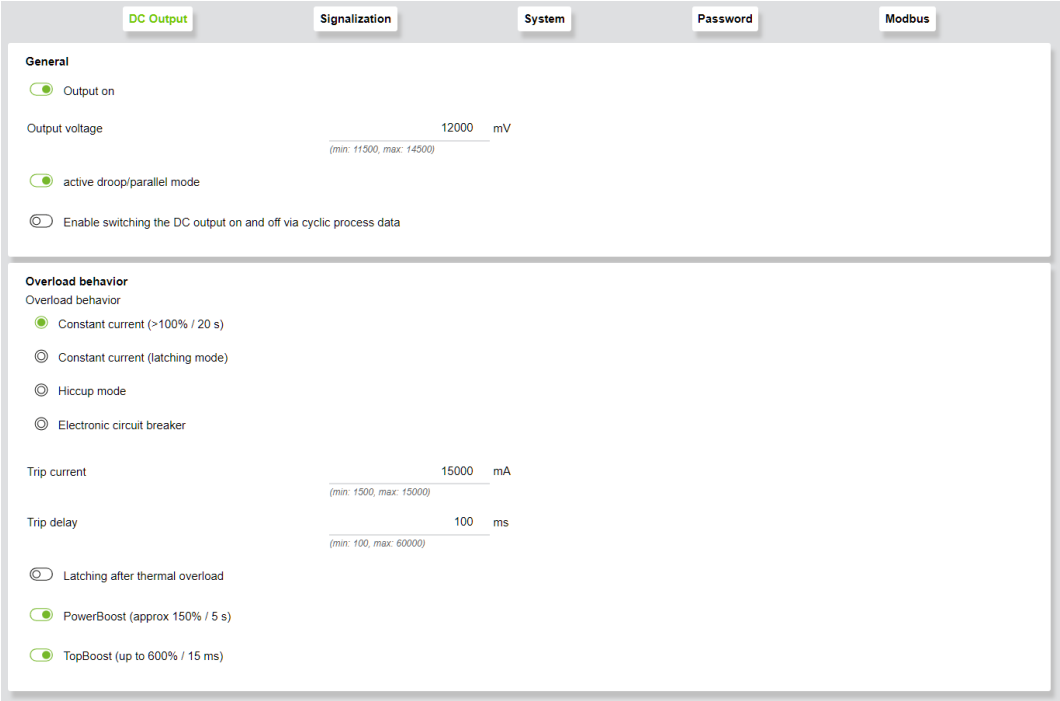


Figure 19: ***Device Settings > DC Output***

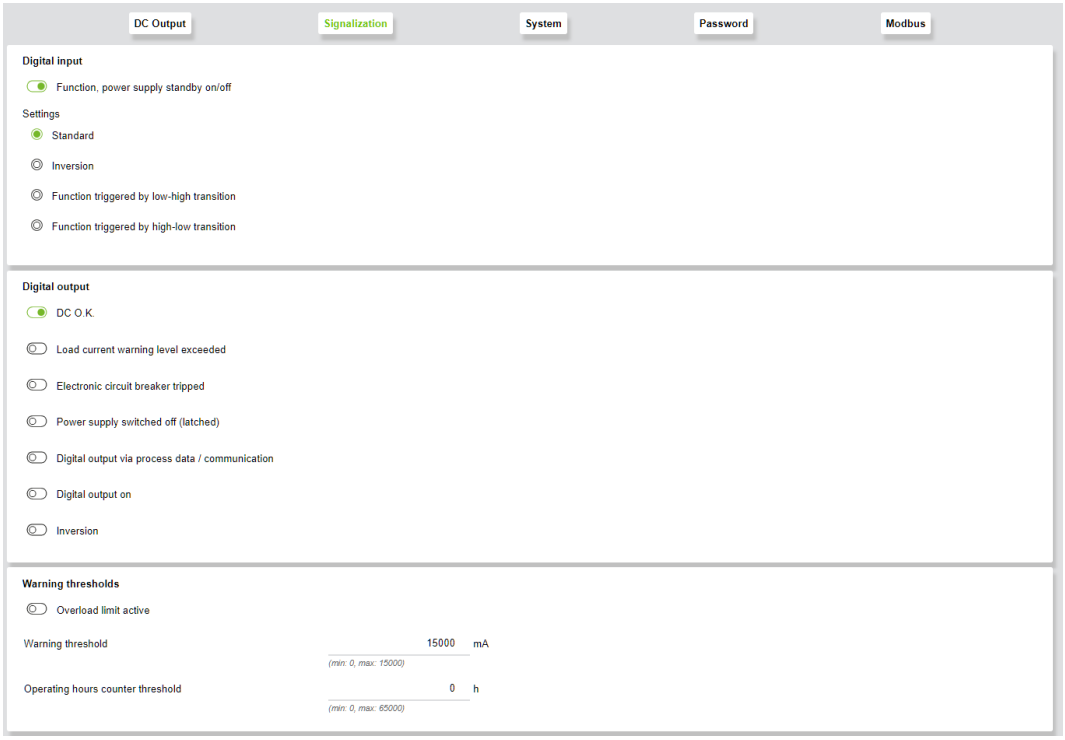


Figure 20: ***Device Settings > Signalization***

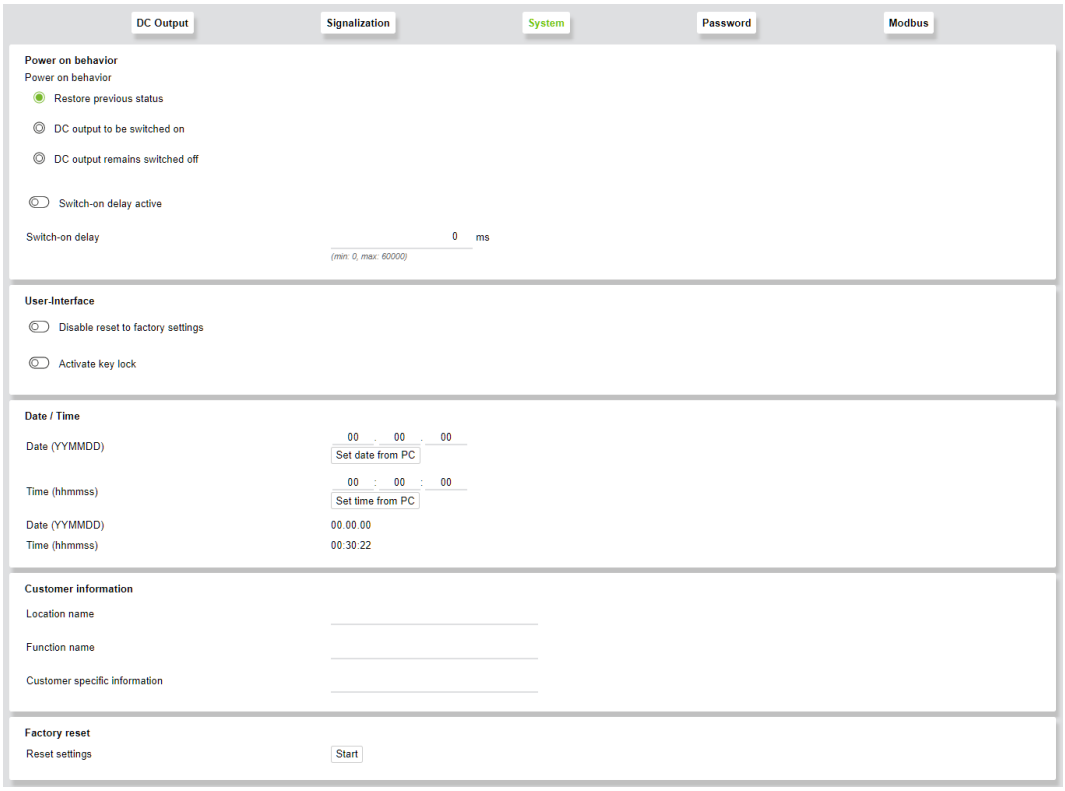


Figure 21: ***Device Settings > System***

Figure 22: ***Device Settings > Password***

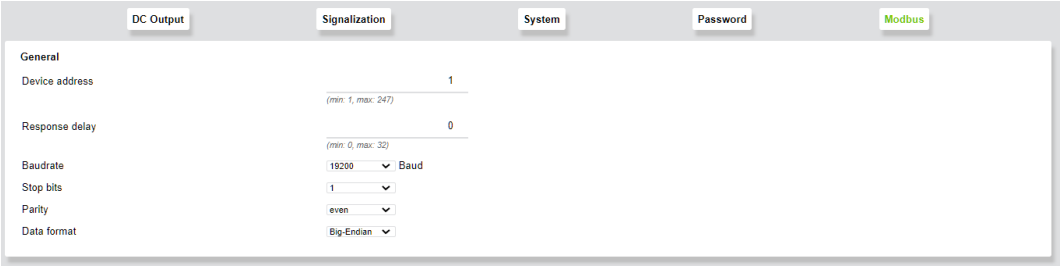


Figure 23: ***Device Settings > Modbus***

9.1.6 Device Information

Here you can view the information on the lower-level device. An example with a Pro 2 Power Supply follows:

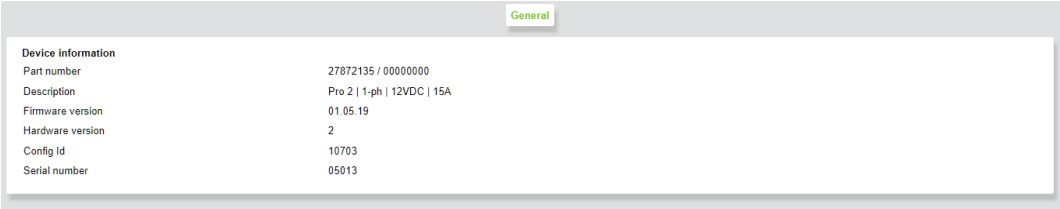


Figure 24: ***Device Information***

9.1.7 Device Measurement

The **Device Measurement** page shows all the measured values and status information of the lower-level device. This is illustrated below on the example of a Pro 2 Power Supply:

- Green: function OK
- Red: function faulty

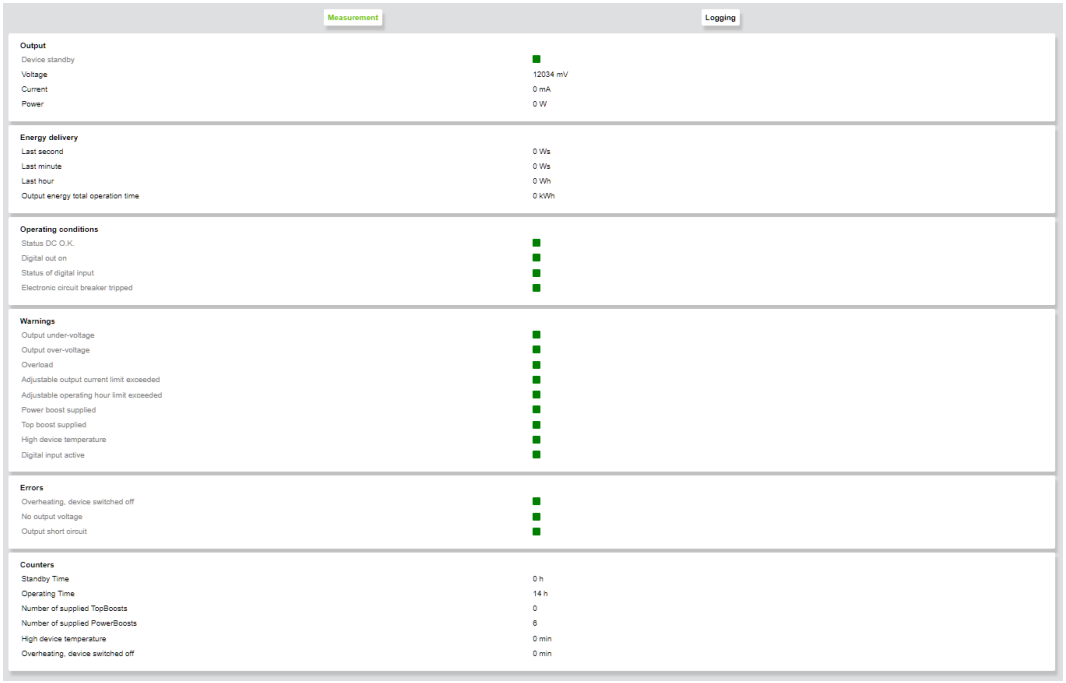


Figure 25: ***Measurement***

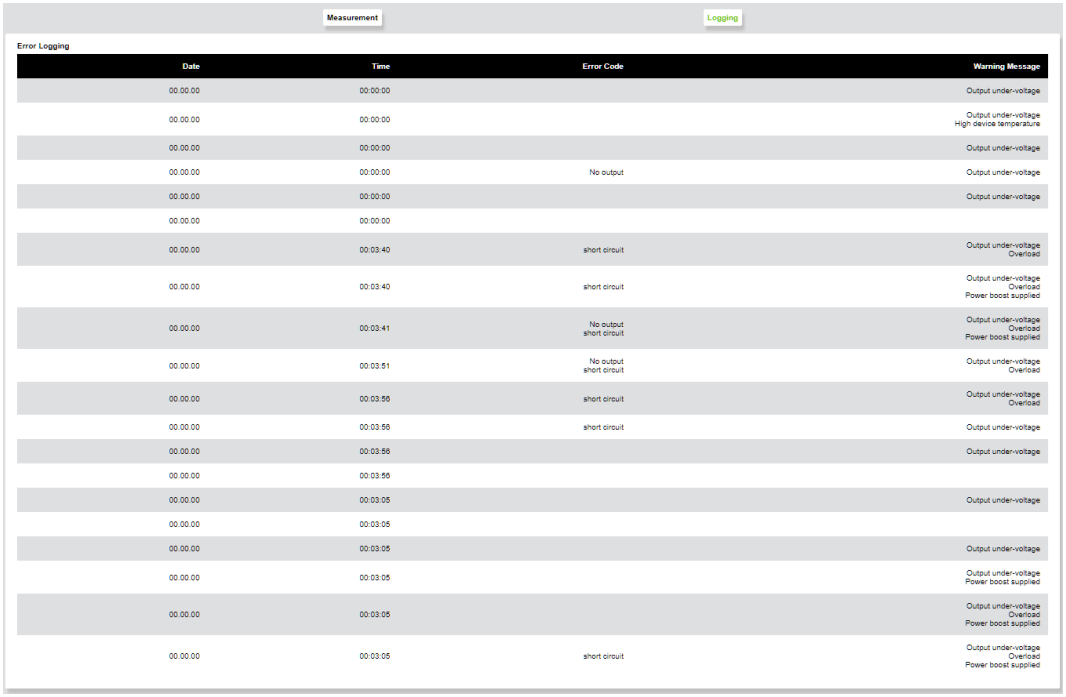


Figure 26: ***Device Measurement > Logging***

Decommissioning

10.1 Disposal and Recycling

	**WEEE Mark** Electrical and electronic equipment may not be disposed of with household waste. This also applies to products without this mark.

Electrical and electronic equipment contain materials and substances that can be harmful to the environment and health. Electrical and electronic equipment must be disposed of properly after use. Environmentally friendly disposal benefits health, protects the environment from harmful substances in electrical and electronic equipment and enables sustainable and efficient use of resources.

- Observe the national and local regulations for the disposal of electrical and electronic equipment, lithium-ion batteries, lead–acid batteries and packaging.
- Clear any data stored on electrical and electronic equipment.
- Remove lithium-ion batteries, lead–acid batteries or memory cards that are added to the electrical and electronic equipment.
- Wear appropriate personal protective equipment when removing the lithium-ion batteries/lead–acid batteries.
- Dispose of the removed lithium-ion batteries/lead–acid batteries according to your local waste regulations (e. g. collection boxes at the retail or local collection points).
- Have electrical and electronic equipment sent to a local collection point.
- Dispose of all types of packaging to ensure a high level of recovery, reuse and recycling.
- Transport packages from the B2B area can be taken back free of charge via a return system in accordance with the Packaging Act. Please contact our service provider Interseroh directly. The corresponding certificate can be found at: **corporate-certificates**
- Throughout Europe, Directives 2006/66/EC, 94/62/EC and 2012/19/EU (WEEE) apply. National directives and laws may differ.

Appendix

11.1 User Certificates

A certificate allows a secure connection for network communication and is used for authenticating the remote host. The lock icon in the browser indicates that this website has a valid, trusted certificate and that the connection is secure. We recommend replacing the self-signed certificates generated in the product with your own.

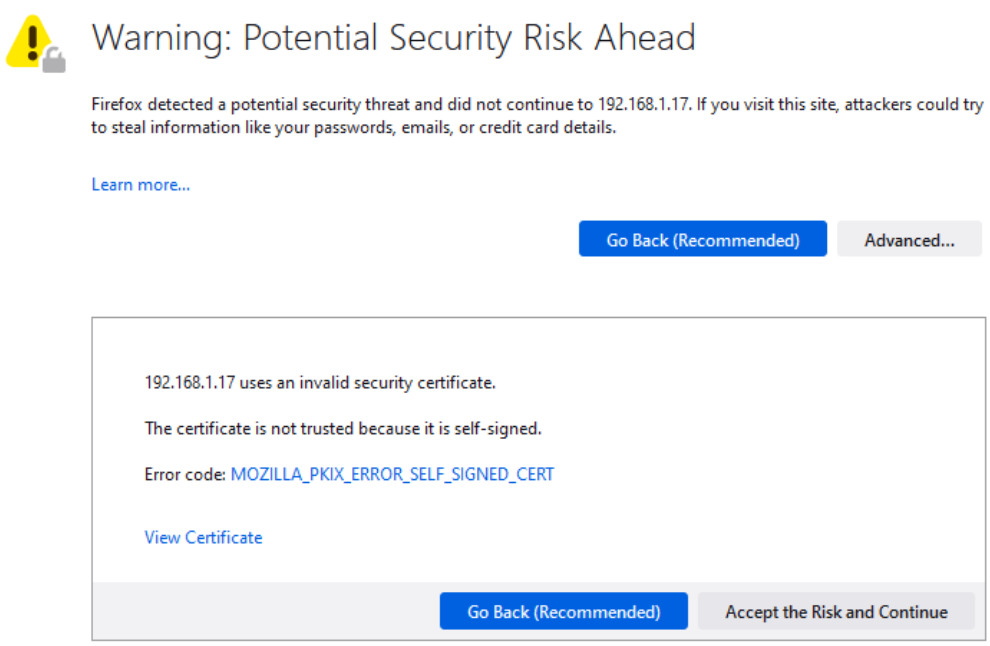


Figure 27: Browser warning message due to self-signed certificate

Certificates you create yourself must be signed by a certificate authority (the so-called root CA). The root certificate forms the shared trust anchor for all certificates subordinate to it and must be stored in the local trust store of the browser or client. The following sections describe an example of creating keys and certificates with the XCA key management software. This free software allows you to create certificates yourself. The certificates/keys are stored in a local database file. The database, which contains private keys among other things, is protected with a password.

11.1.1 Creating and Replacing Certificates

The following table lists the available cipher suites:

Table 35: Available Cipher Suites

IANA No.	Cipher Suite
TLS1.3	
0x13, 0x01	TLS_AES_128_GCM_SHA256
0x13, 0x02	TLS_AES_256_GCM_SHA384
0x13, 0x04	TLS_AES_128_CCM_SHA256
0x13, 0x05	TLS_AES_128_CCM_8_SHA256
TLS1.2	
0xC0, 0xAC	TLS_ECDHE_ECDSA_WITH_AES_128_CCM
0xC0, 0xAE	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
0xC0, 0xAF	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
0xC0, 0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
0xC0, 0x0A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
0xC0, 0x2B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0xC0, 0x2C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
0xC0, 0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
0xC0, 0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

11.1.2 Creating a Template for Certificates

1. Open the XCA software and select the **New Database** submenu under the **File** menu.
2. Select a storage location and an appropriate name for the database.
3. Enter a password to protect the database.

   ⇨ The newly created database opens.

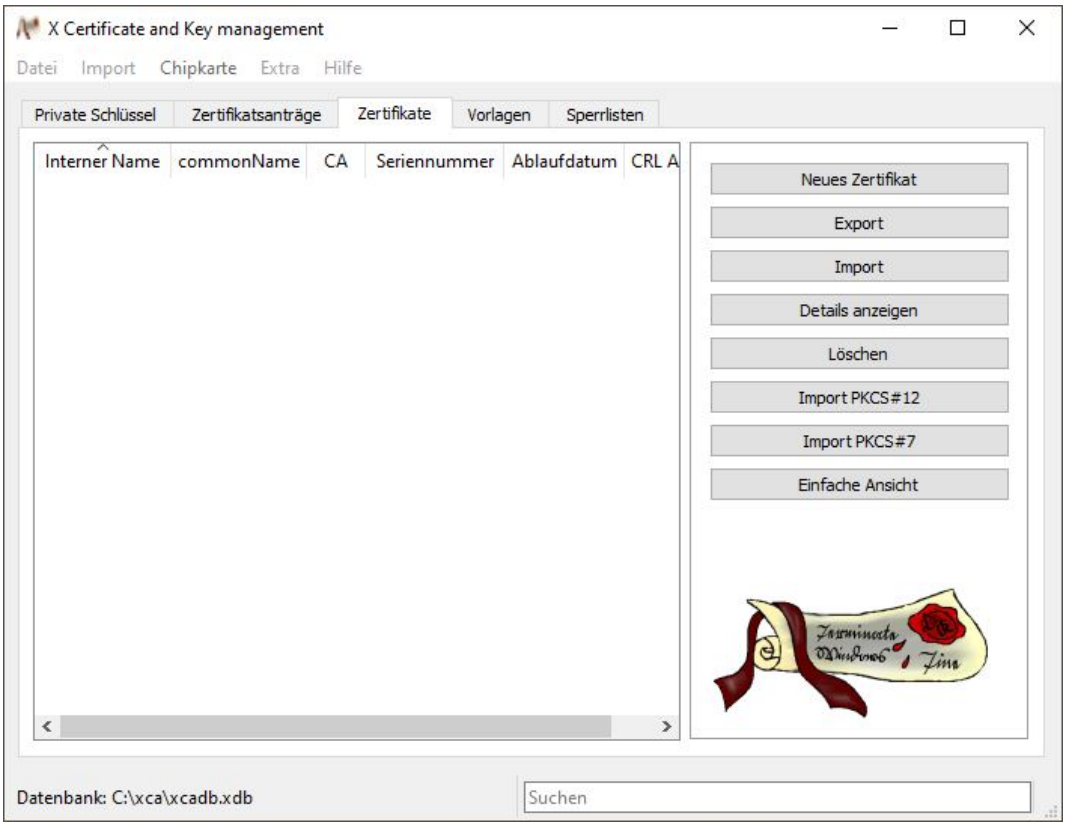


Figure 28: XCA Database

4. On the **Templates** tab, click the **[New Template]** button.
5. Select the "**[Default]** Blank Template" setting in the **Preset Template Values** dialog that opens.
6. Click **[OK]** to confirm the selection.
7. In the **Change XCA Template** dialog that opens, switch to the **Owner** tab.

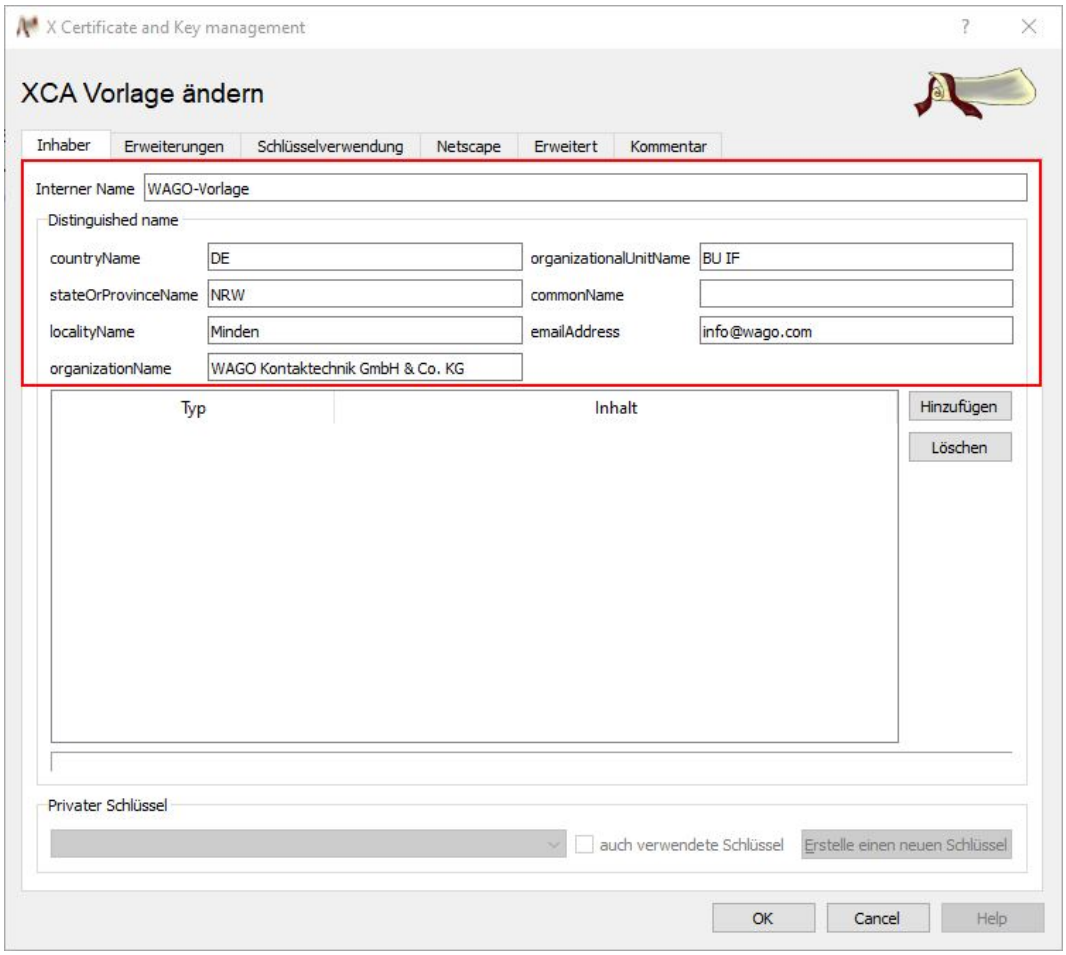


*Figure 29: **Owner** Tab*

Input Field	Explanation
Internal name	The value in this field serves as an internal reference and should identify the certificate uniquely
countryName	Country code (e.g., DE for Germany)
stateOrProvinceName	State or province (e.g., NRW for North Rhine-Westphalia)
localityName	Place where certificate was issued
organizationName	Name of the organization that issued the certificate
organizationUnitName	Department identifier
commonName	A general identifier can be stored here
emailAddress	An email address can be stored here

8. Fill in the marked input fields in the upper section.
   ⇨ The **commonName** field is left blank in the template and filled out later.
9. Click **[OK]** to confirm the entries.
   ⇨ Once the template has been created, it is displayed in the window.

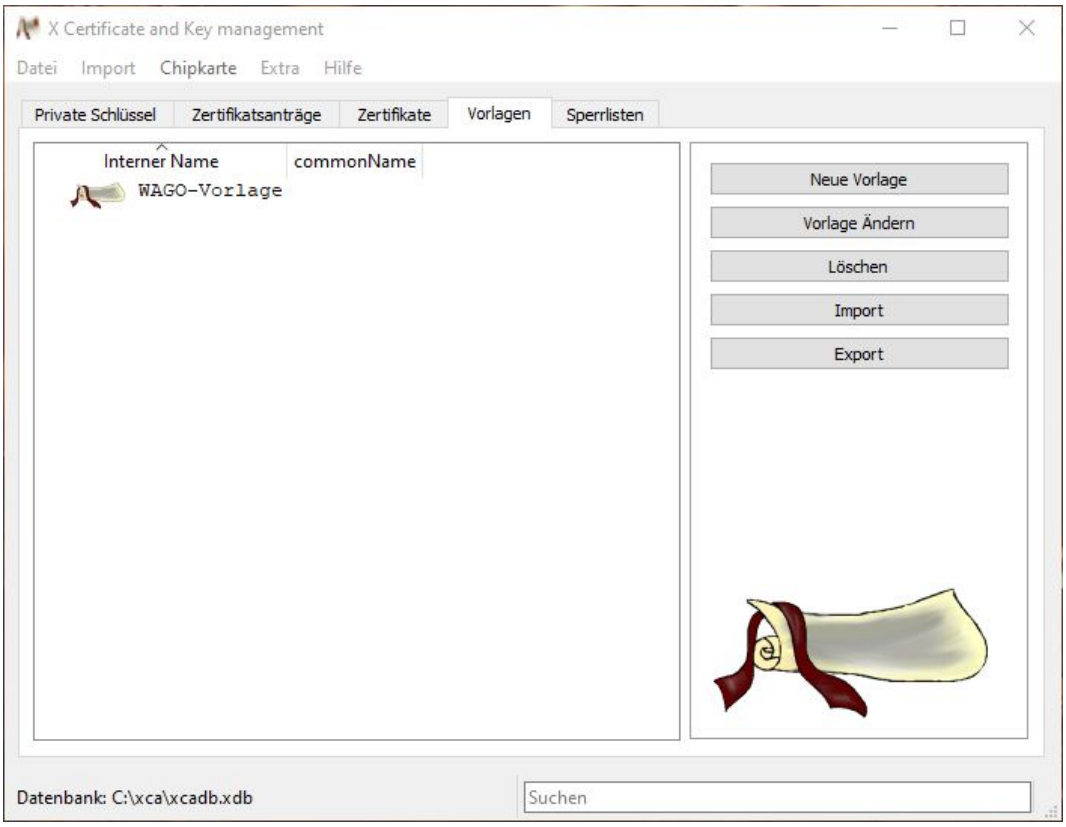


Figure 30: Creating a Template

11.1.3 Creating the Root CA Certificate

1. Switch to the **Certificates** tab to create the Root CA certificate. Click the **[New Certificate]** button.

   ⇨ The following dialog appears.

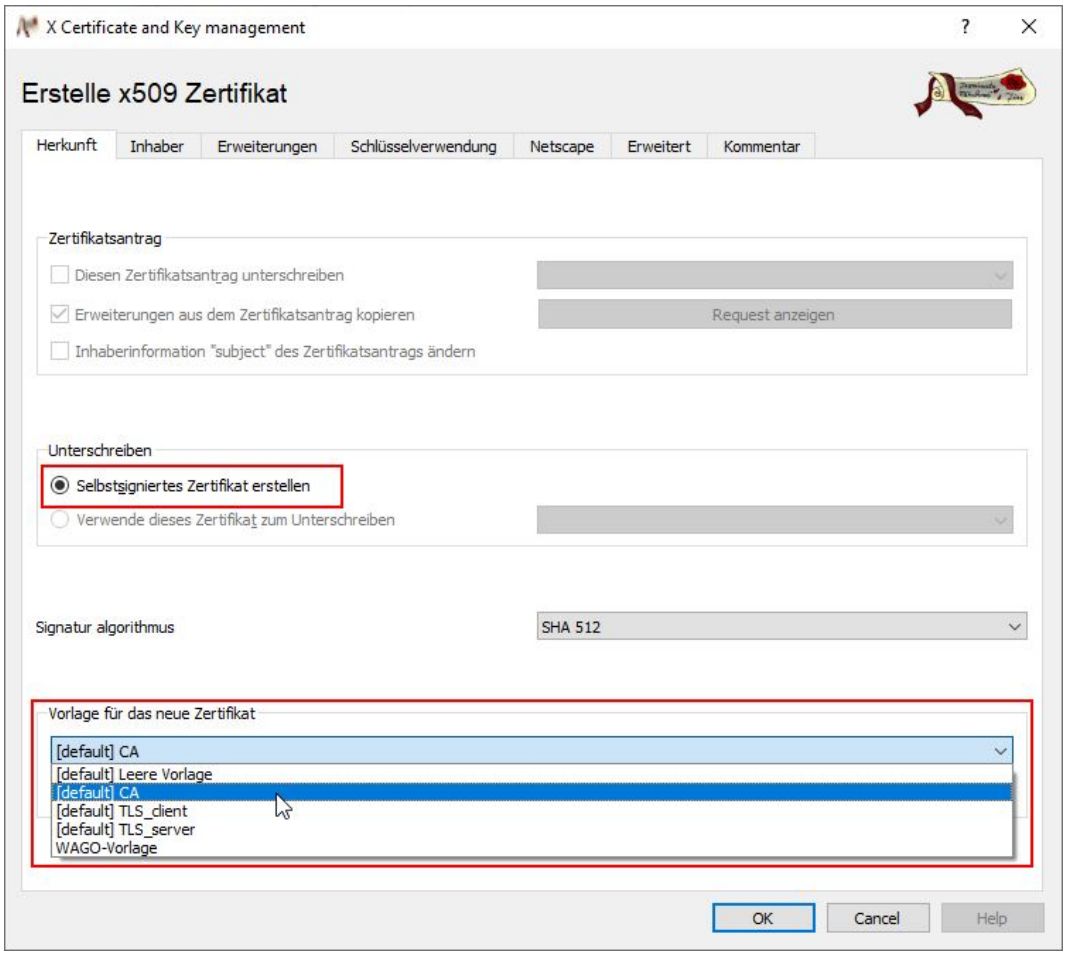


Figure 31: Creating a Certificate – Selecting a Template

2. Select your created template from the **Template for the New Certificate** selection field.
3. Click the **[Apply Subject]** button.
4. Select the **[Default] CA** template from the **Template for the New Certificate** selection field.
5. Click the **[Apply Extensions]** button.
6. Switch to the **Owner** tab.

   ⇨ The following dialog appears.

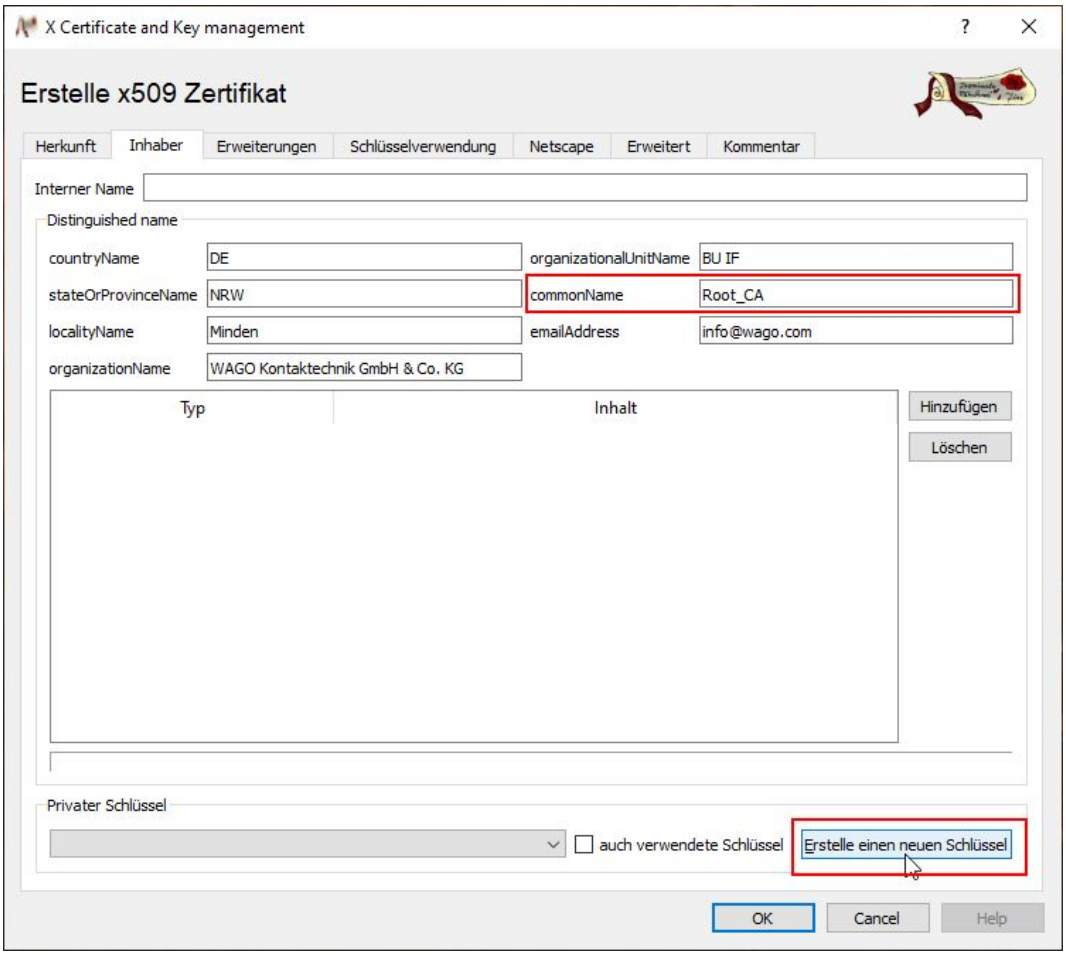


Figure 32: Creating a Certificate – Entering a Name

7. Enter an identifier in the **CommonName** input field (e.g., “Root_CA”).
8. Click the **[Create a New Key]** button.

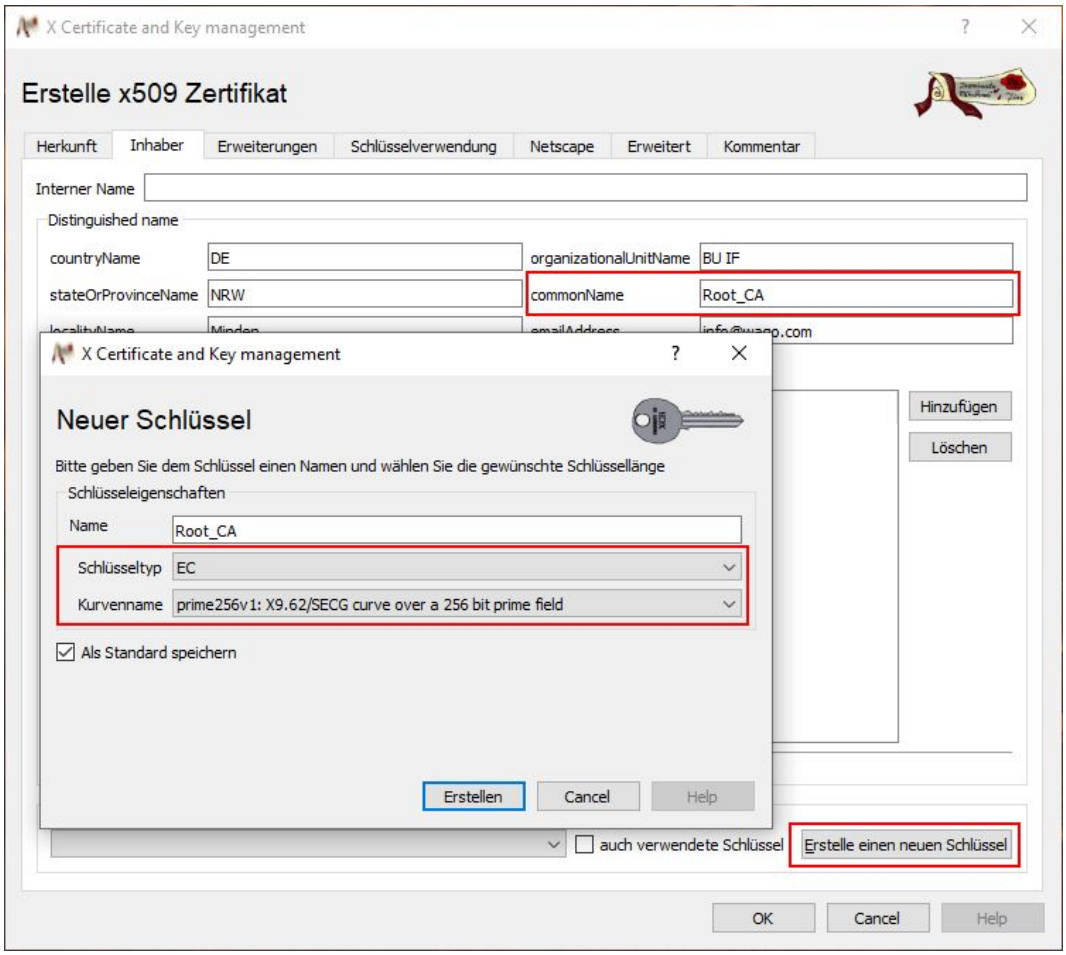


Figure 33: Creating a New Key

9. Set the key type to “EC” and select an EC curve for the root CA. The name is preset. The assignment depends on whether the key is generated for the root CA or for the module. The prime256r1 curve according to BSI TR 02102 2 (named prime256v1 in the XCA) is supported.

   ⓘ Note

   No RSA keys are supported.

10. Click the **[Create]** button to create the key.
11. Click **[OK]** to exit the dialog after notification of successful key creation.

    ⇨ The created certificate is displayed on the **Certificates** tab.

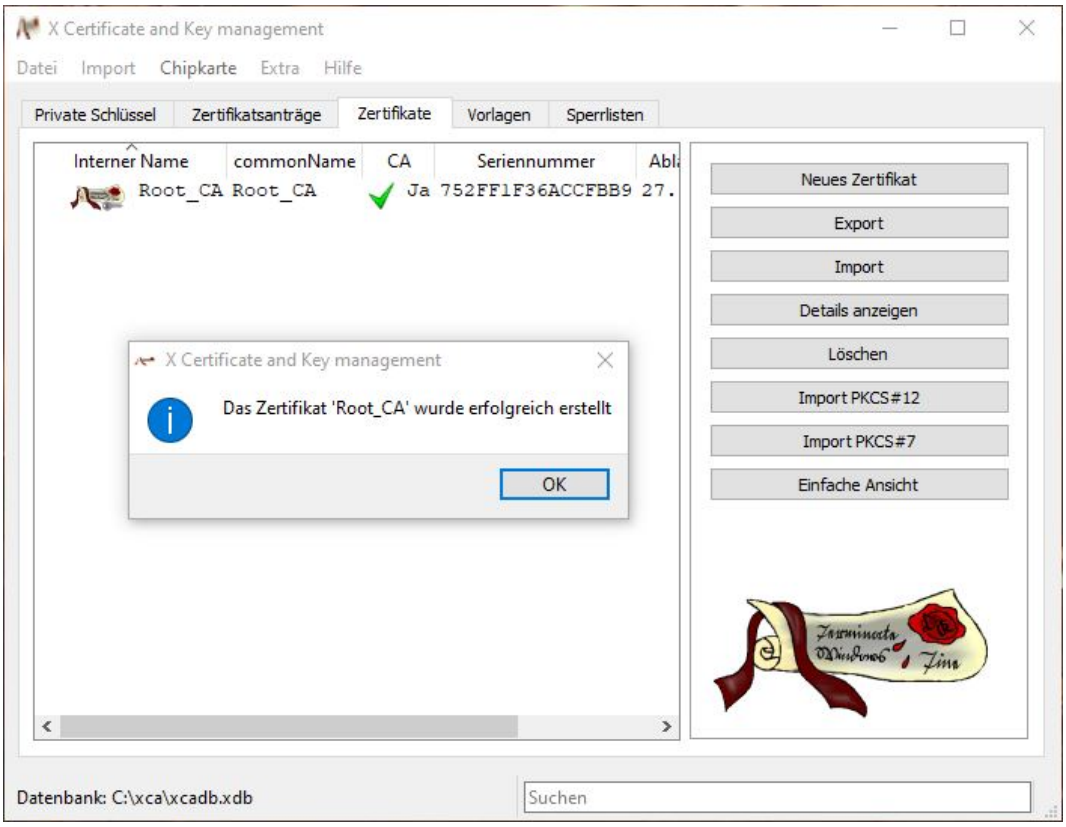


Figure 34: New Certificate Created

11.1.4 Creating the Device Certificate

1. Go to the **Certificates** tab to create the device certificate.
2. Click the **[New Certificate]** button.

   ⇨ The following dialog appears.

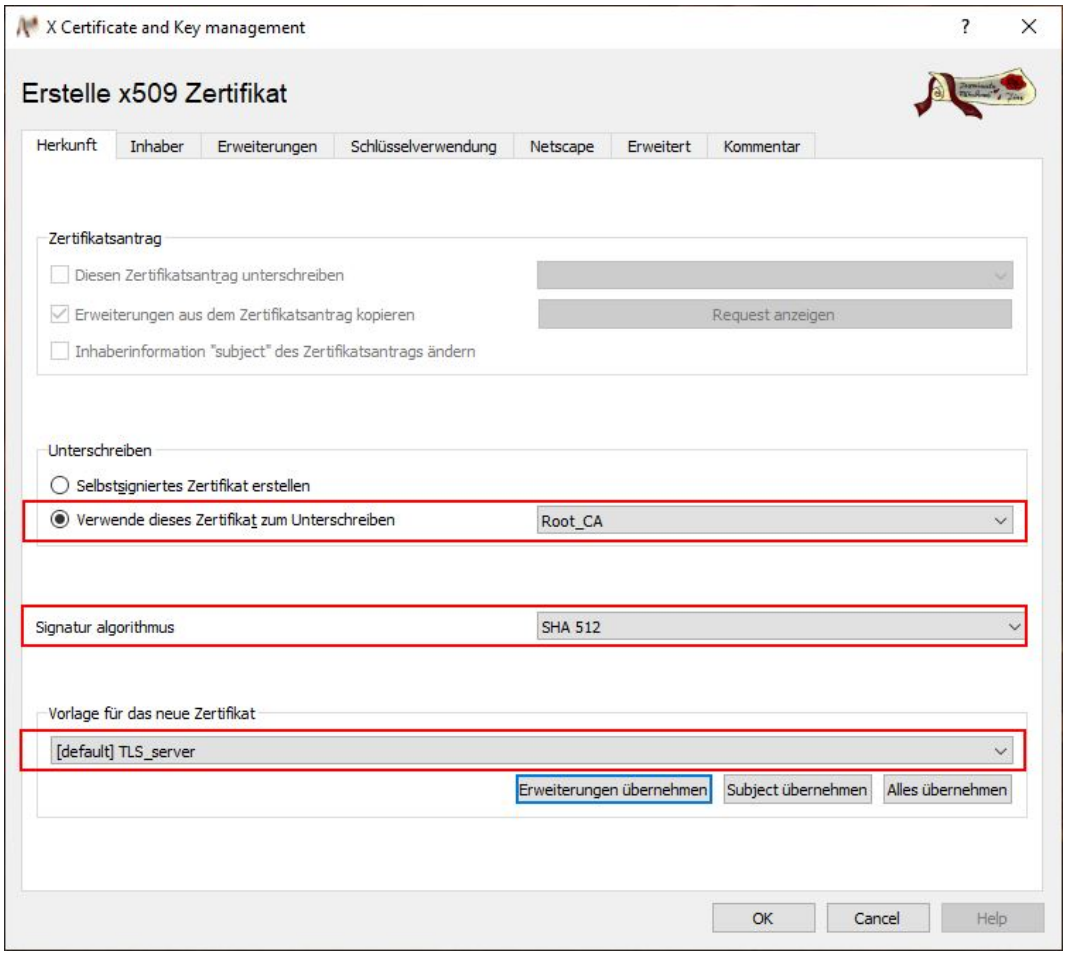


Figure 35: Creating a New Device Certificate

3. Check the **Use This Certificate for Signing** box and select the root CA certificate that has been created.
4. In the **Signature Algorithm** selection field, select the value “SHA 512” (see the BSI TR-02102 technical guidelines).
5. Select your created template from the **Template for the New Certificate** selection field.
6. Click the **[Apply Subject]** button.
7. Select the “**[Default]** TLS_server” template from the **Template for the New Certificate** selection field.
8. Click the **[Apply Extensions]** button.
9. Switch to the **Owner** tab.
10. In the **CommonName** input field, enter the IP address of your device.
11. Click the **[Create a New Key]** button.

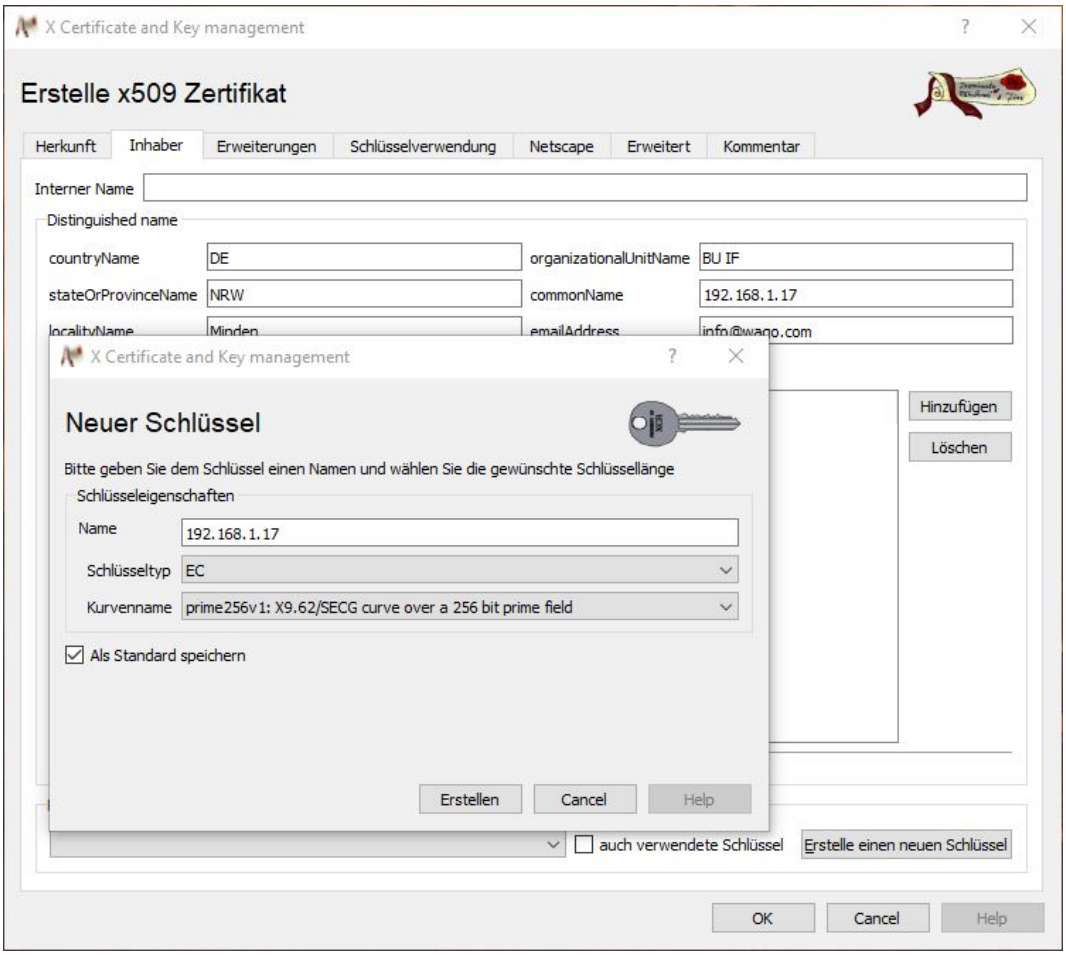


Figure 36: Creating a New Key

12. Change the key type to elliptic curve and select the prime256v1 curve.
13. Click the **[Create]** button to create the key.
14. Switch to the **Extensions** tab.

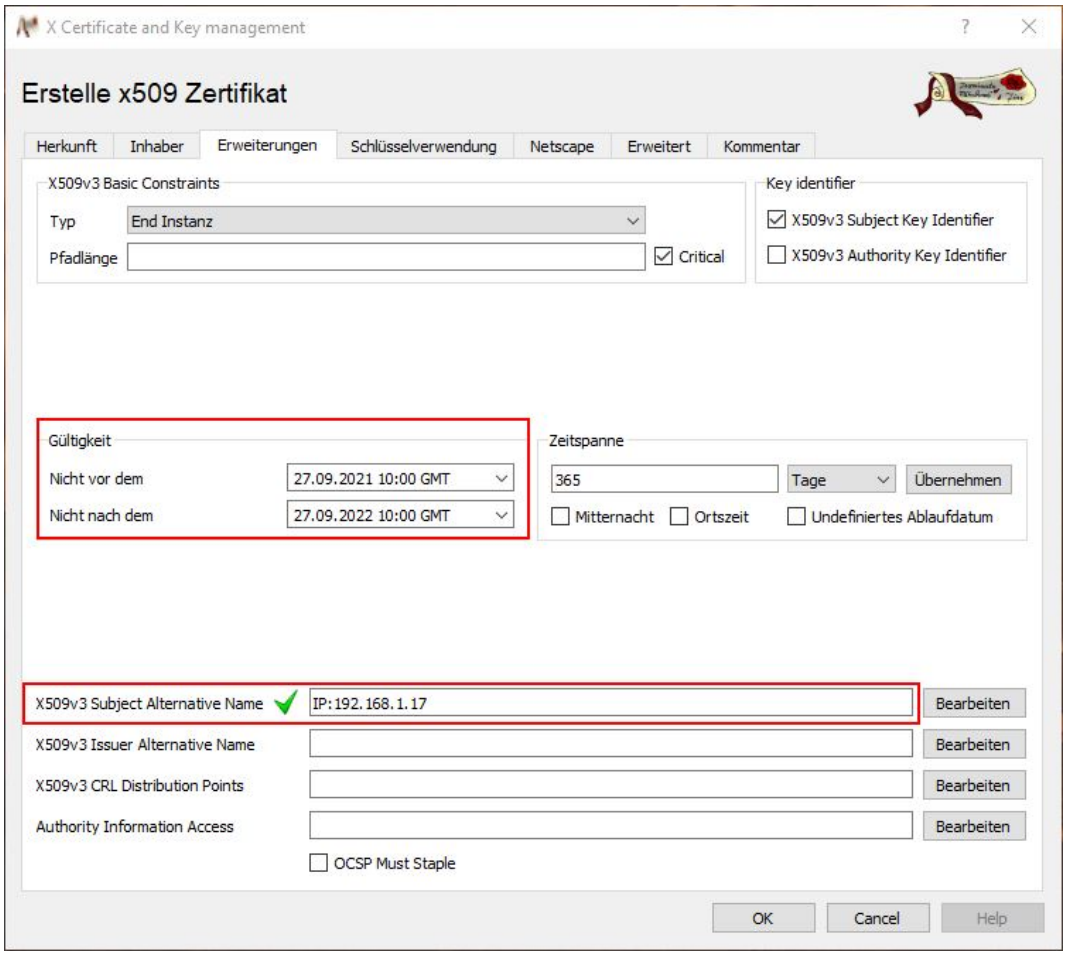


Figure 37: "Extensions" Tab

15. Set the validity of the device certificate. Please note the recommendations of the BSI TR-02102-2 technical guidelines.
16. Add the IP address and/or host name in the **X509v3 Subject Alternative Name** input field.

Note

The value in the "X509v3 Subject Alternative Name" input field must be identical to the address bar!

The IP address/host name is used by browsers to determine the identity. If the value entered in the **X509v3 Subject Alternative Name** input field differs from the value in the address bar, the certificate is recognized as invalid.

17. Switch back to the **Key Management** tab to restrict the use of the certificates.
18. Enter the values marked in the figure.

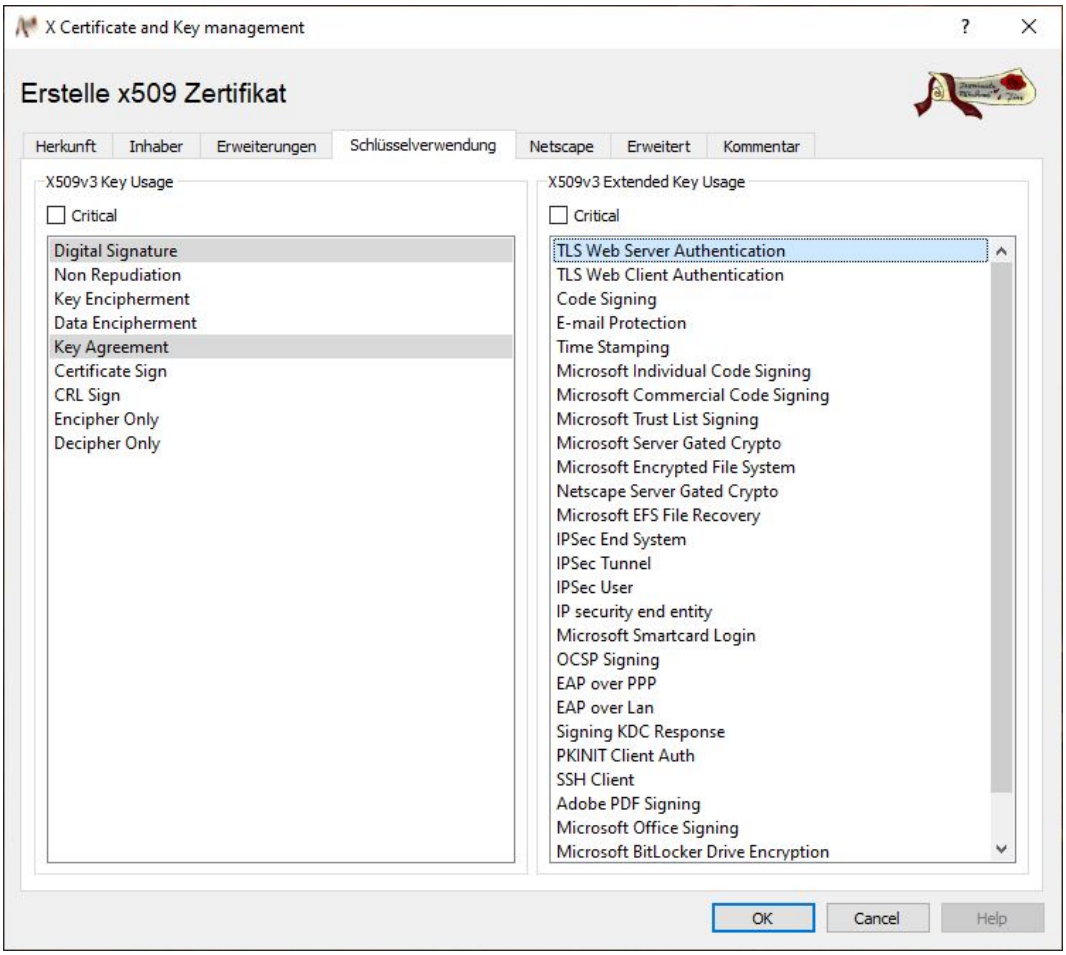


Figure 38: New Certificate Request, “Client” Key Use

19. Click **[OK]** to confirm the entries. The new certificate is shown below the root CA certificate on the **Certificates** tab.

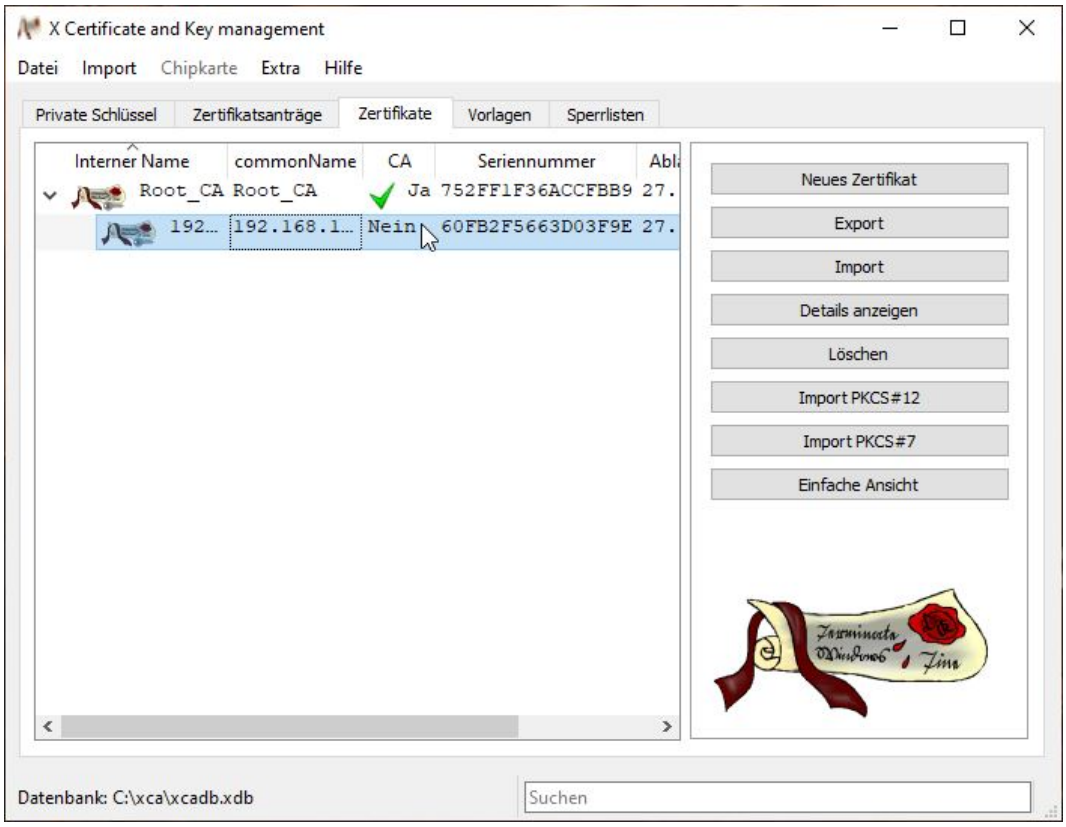


Figure 39: Device Certificate Created

11.1.5 Exporting Certificates

1. In the main window, switch to the **Certificates** tab and expand the tree structure fully.
2. Select your root CA certificate and open the context menu by right-clicking.
3. Select “Export” > “File.”

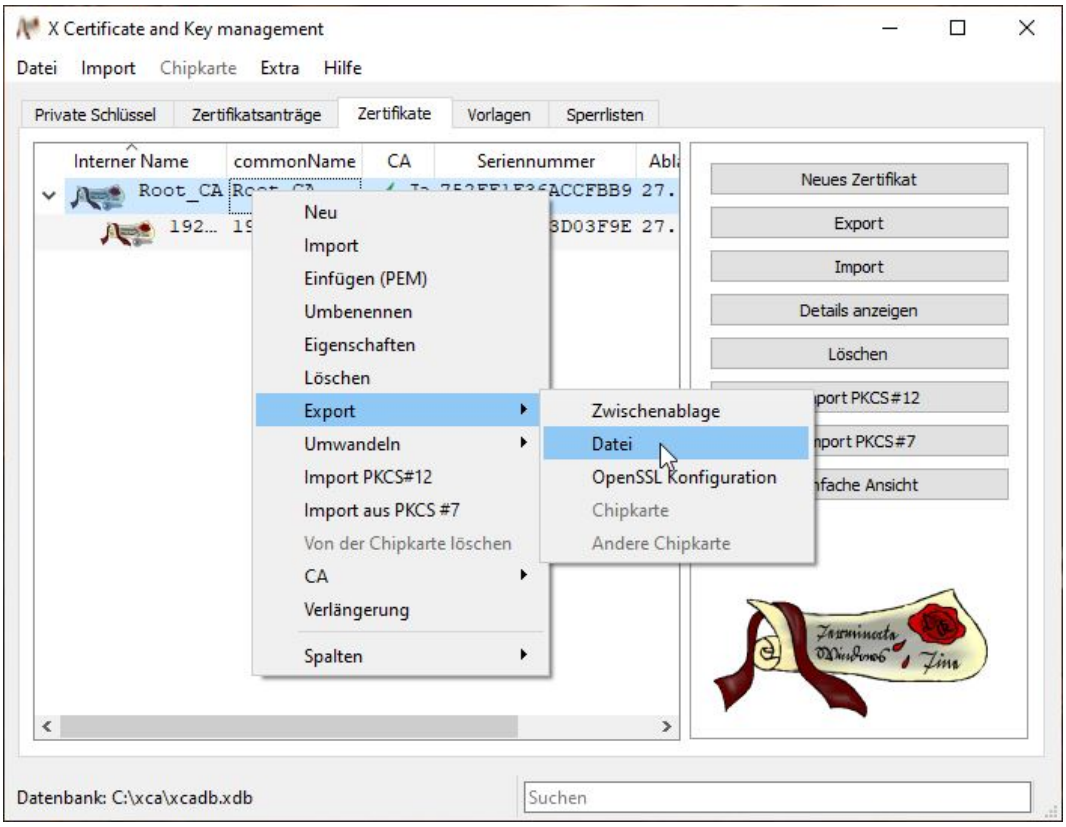


Figure 40: Exporting Root CA Certificate 1

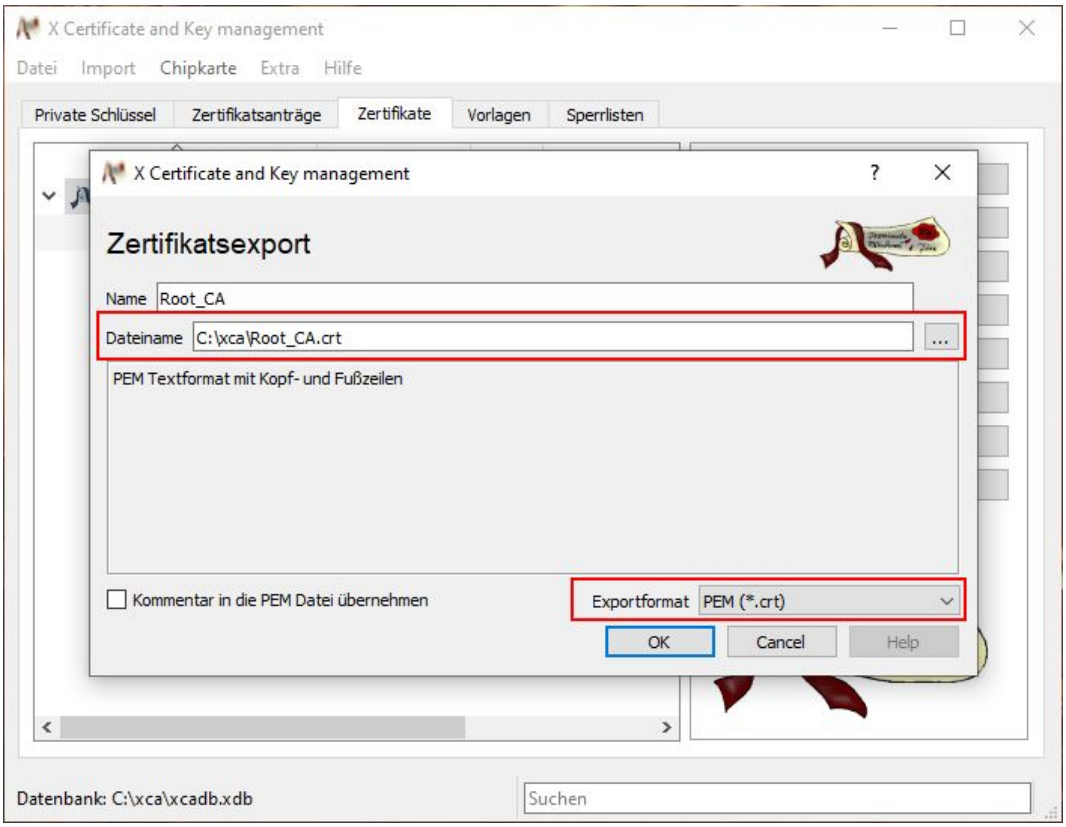


Figure 41: Exporting Root CA Certificate 2

4. Select the storage location by clicking the **[…]** button.
5. From the **Export Format** selection list, select the “PEM (*.crt)” entry.

6. Click **[OK]** to confirm.
7. Select your device certificate and right-click to open the context menu.
8. Select “Export” > “File.”

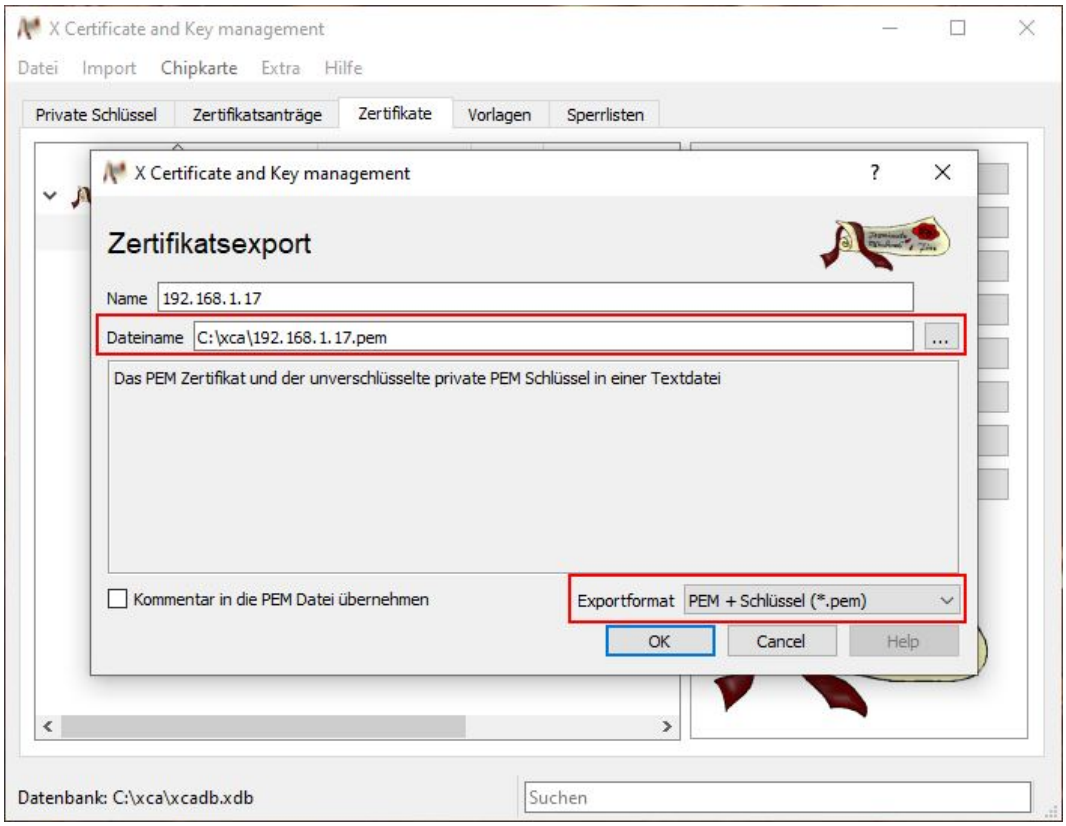


Figure 42: Exporting the Device Certificate

9. Select a storage location by clicking the **[…]** button.
10. From the **Export Format** selection list, select the “PEM with Key” entry.
11. Click **[OK]** to confirm.

11.1.6 Installing Certificates on the Client and Product

ⓘ Note

New device certificate necessary if IP address/host name changes:

If the IP address or host name has changed, the certificate must be recreated for the device with the correct IP address or host name (see **Creating the Device Certificate [▶ 55]**)!

1. Import your root CA certificate into the browser. The procedure depends on the browser used.
2. Transfer your device certificate via the WBM to the “Modbus TCP Communication Module” product. On the **Module Settings > Network** page, click **[Choose File]** under **TLS Certificates**.

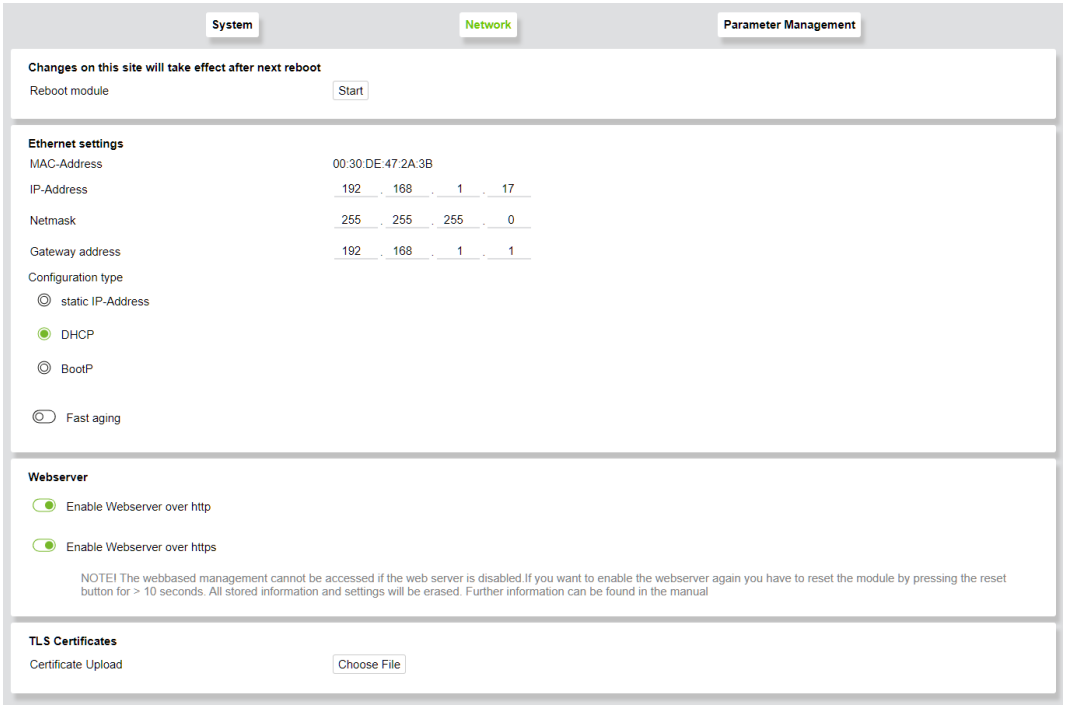


Figure 43: Importing the Device Certificate

3. Select the certificate you created and click **[Save Certificate]**.
4. Reboot by clicking the **[Start]** button under “Reboot” on the **Module Settings > System** page.

⇨ As soon as a lock icon appears to the left or right (depending on the browser) of your Web address, the action has been successful, and your connection is secure from now on. Browsers often indicate how trusted a connection is in the address bar. For example, Firefox displays a lock icon if the certificate is signed by a trusted root CA.

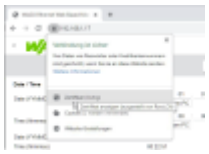


Figure 44: Importing the Device Certificate – Secure Connection

11.2 Accessories

The following accessories are available for the product:

Accessories – Marking

Table 36: Accessories – Marking

Description	Designation	Item Number
Marker Carrier	-	2789-1233
Marking System	-	2009-0110
WMB Multi Marking System	-	2009-0115
	-	2009-0115/0000-0002

Accessories – Other

Table 37: Accessories – Other

Description	Item Number
ETHERNET Plug RJ-45, IP20; ETHERNET 10/100 Mbit/s; for field assembly	750-975

11.3 Protected Rights

- Adobe® and Acrobat® are registered trademarks of Adobe Systems Inc.
- Android™ is a trademark of Google LLC.
- Apple, the Apple logo, iPhone, iPad and iPod touch are registered trademarks of Apple Inc. registered in the USA and other countries. “App Store” is a service mark of Apple Inc.
- AS-Interface® is a registered trademark of the AS-International Association e.V.
- BACnet® is a registered trademark of the American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® is a registered trademark of Bluetooth SIG, Inc.
- CiA® and CANopen® are registered trademarks of CAN in AUTOMATION – International Users and Manufacturers Group e.V.
- CODESYS is a registered trademark of CODESYS Development GmbH.
- DALI is a registered trademark of the Digital Illumination Interface Alliance (DiiA).
- EtherCAT® is a registered trademark and patented technology licensed by Beckhoff Automation GmbH, Germany.
- ETHERNET/IP™ is a registered trademark of the Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® is a registered trademark of EnOcean GmbH.
- Google Play™ is a registered trademark of Google Inc.
- IO-Link is a registered trademark of PROFIBUS Nutzerorganisation e.V.
- KNX® is a registered trademark of the KNX Association cvba.
- Linux® is a registered trademark of Linus Torvalds.
- LON® is a registered trademark of the Echelon Corporation.
- Modbus® is a registered trademark of Schneider Electric, licensed for Modbus Organization, Inc.
- OPC UA is a registered trademark of the OPC Foundation.
- PROFIBUS® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).
- PROFINET® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).
- QR Code is a registered trademark of DENSO WAVE INCORPORATED.
- Subversion® is a trademark of the Apache Software Foundation.
- Windows® is a registered trademark of Microsoft Corporation.

List of Tables

List of Figures

WAGO GmbH & Co. KG
Postfach 2880 · D - 32385 Minden
Hansastraße 27 · D - 32423 Minden
✉ **info@wago.com**
www.wago.com

Headquaters	+49 571/887 – 0
Sales	+49 (0) 571/887 – 44 222
Order Service	+49 (0) 571/887 – 44 333
Fax	+49 571/887 – 844169