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.

Table of Contents

Provisions

This documentation applies to Modbus TCP Communication Module (2789-9052).

Note

Observe the applicable documentation!

This product must only be installed and operated according to the instructions of the complete Instructions for use. Knowledge of the complete Instructions for use is required for proper use.

1. Carefully read the Product Manual.
2. Before commissioning, follow the instructions in section Safety [▶ 9].

Table 1: Complete instructions for use

Document Type	Contents
Product Manual	Contains all the product-specific information for a product.
Instruction leaflet	Is included with each product. Contains initial information on safe handling of the product.

Table 2: Additional documentation

Document Type	Contents
Product Manual	WAGO Power Supply Pro 2
Instruction leaflet	WAGO Power Supply Pro 2

All the documentation is available at: www.wago.com.

1.1 Intended Use

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.

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

Unless barred by applicable legal provisions, unauthorized copying and distribution of this document, as well as the use and communication of its content are strictly prohibited unless expressly authorized by prior agreement. Third-party products are always mentioned without any reference to patent rights. WAGO GmbH & Co. KG, or for third-party products, their manufacturer, retain 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 [▶ 59]).

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

This section contains safety regulations that must be observed for the safe use of the product.

The following content is aimed at the following target groups:

- Planners and installers
- Operators
- Qualified assembly personnel
- Qualified installation personnel (electrical installation, technician network installation etc.)
- Qualified operating personnel
- Qualified service and maintenance personnel

Obey the following safety rules:

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.
- 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.

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 Introduction

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

- Modbus TCP/UDP [2]
- BootP [2]
- DHCP
- SNTP
- HTTP
- HTTPS with TLS 1.3

The integrated switch with two external RJ-45 ports allows the setup of 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.
[2] Pending

3.2 View

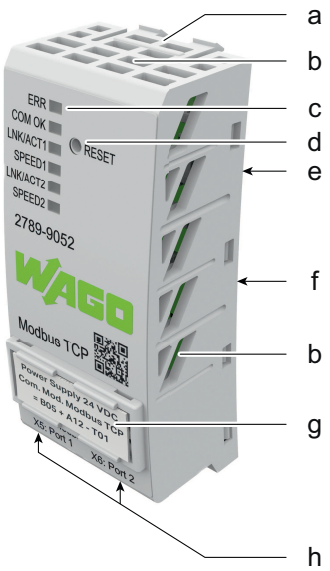


Figure 1: View

Table 3: Legend for "View" Figure

Position	Comment	For Details, See Area
a	Locking tab	–
b	Ventilation openings	–
c	Optical status indication	Indicators [▶ 14]
d	Reset button	Control elements [▶ 14]
e	Communication interface	–
f	Type label	Type label [▶ 12]
g	Marker carrier	Accessories – Marking [▶ 59]
h	Ethernet Port 1 (X5); Ethernet Port 2 (X6)	RJ-45 Interfaces [▶ 13]

3.3 Type label

The type label for the product is attached to the back of the housing. It contains the following information:

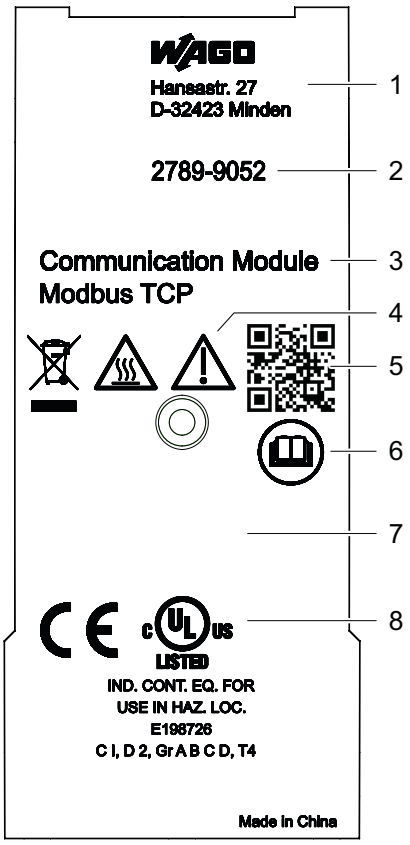


Figure 2: Type label

Table 4: Legend for Figure "Type label"

Position	Comment	For Details, See Area
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

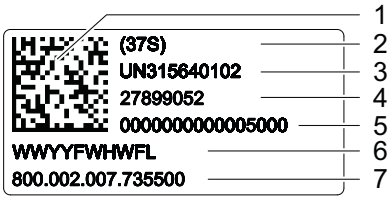


Figure 3: Product-Specific Information

Table 5: Legend for Figure “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 6: Revision index structure

Software index	Hardware index	Boot loader index
xx	yy	zz

3.5 Connections

3.5.1 Power Supply

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

3.5.2 RJ-45 Interfaces

The connection to ETHERNET-based fieldbuses is made via two RJ-45 connectors (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 for each port, supports transmission speeds 10/100 Mbit/s as well as the full and half-duplex transmission modes.

The RJ-45 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. Cable types S/UTP (Screened Unshielded Twisted Pair) and STP (Shielded Twisted Pair) with a maximum segment length of 100 m can be used.

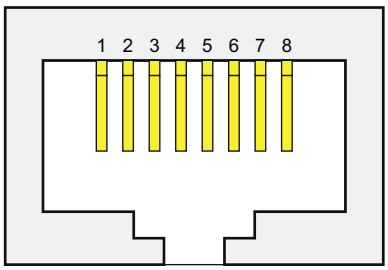


Figure 4: RJ-45 Interfaces X5/X6

Table 7: Legend for Figure “RJ-45 Interfaces X5/X6”

Pin	Description
1	Transmit Data +
2	Transmit Data -
3	Receive Data +
4	not assigned

Pin	Description
5	not assigned
6	Receive Data -
7	not assigned
8	not assigned

3.6 Indicators

The product has an optical status indicator. This indicator consists of six LEDs.

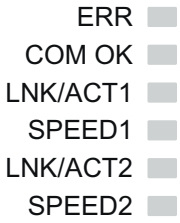


Figure 5: Optical status indication

Table 8: Operating Status Indication

Indicator		LED Description	State	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 reset 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

3.7.1 Control Elements

There is a reset button on the front of the product. This button can be used to reset the product.

Section **Operation [▶ 33]** contains a detailed description of how you can use these buttons to make settings.

3.8 Technical data

3.8.1 Product

Table 9: 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 10: Technical Data – Power Loss

Property	Value
Power loss (max.)	1.1 W

3.8.3 Communication

Table 11: Technical Data – Communication

Property	Value
Communication	Modbus TCP/UDP
Interface	RJ-45 interface
Cable length	≤ 100 m
Transmission medium	ETHERNET: Twisted Pair S-UTP; 100 Ω; Cat. 5
Transmission rate	100 MBd (ETHERNET: 10/100 Mbit/s)
ETHERNET protocols	HTTP(s), BootP*, DHCP, SNTP
Specifications of the conductors used	≥ +75 °C (ambient air temperature: ≤ +60 °C)

*) *Pending*

3.8.4 Environmental Conditions

Table 12: Technical Data – Environmental Conditions

Property	Value
Test voltage (fieldbus)	0.775 kVAC, 50 Hz, 1 min.
Type of insulation	Functional insulation
Surrounding air temperature, operation [1]	−40 … +55 °C
Surrounding air 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 using the Modbus TCP Communication Module in combination with a WAGO Power Supply Pro 2, which is approved for a maximum ambient temperature of +70 °C, a maximum ambient temperature of +55 °C must not be exceeded during operation.*
[2] *The subordinateWAGO 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:

Table 13: Guidelines

Logo	Explanation	Verification
CE	CE marking	WAGO website

3.9.2 Approvals

The following approvals have been granted for the product:

Table 14: Approvals

Logo	Certification Body	Standard
c UL us	Underwriters Laboratories Inc. (Ordinary Locations)	UL 61010-1
c UL us	Underwriters Laboratories Inc. (Ordinary Locations)	UL 61010-2-201
c UL us	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 15: 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
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 16: 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

Standard	Title
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 17: EMC – Emission of Interference

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

3.9.4 Special Requirements

Observe the following:

- Perform installation according to the local conditions, applicable regulations (e.g., VDE 0100), national accident prevention specifications (e.g., UVV-VBG4 or DGUV Regulation 2) and accepted technical regulations.
- This product is intended for installation in electrical systems or machines and fulfills the requirements of the Low Voltage Directive.

When installing in machines, the following also applies:

- When installing in machines, normal operation must not commence until it is determined that the machine complies with the requirements of the Machinery Directive, EN 60204.
- Commencement of normal operation is allowed only on the condition of compliance with the EMC Directive.
- The manufacturer of the system or machine is responsible for ensuring compliance with the limit values required by EMC legislation.

Fieldbus Description

4.1 Technology

4.1.1 TCP/IP (Internet Protocol)

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 either be located 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, this includes the possibility of certain segments being chosen that are shorter than others, thus allowing the data telegrams to overtake each other and falsifying the sequence of the data packets. For this reason, guaranteeing a correct transmission must take place at higher levels; e.g., through TCP. The IP data packets include an abundance of address and additional information in the “Packet Header” aside from the user data which is to be transported.

4.1.2 HTTP/HTTPS

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

The HTTP server uses the port number 80.

The HTTPS server uses the 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 (FC). The following three function codes are supported by all products in the “WAGO Power Supply Pro 2“ Series:

Table 18: Function Codes

FC	Designation	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 acc. Modbus specification (“Frame Exceptions”):

Table 19: Exception Codes

Code	Designation	Description
0x01	Illegal Function	Function is 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 20: User-defined Exception Codes

Code	Designation	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 the 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 General Module Parameters

The Modus TCP communication module uses the following general parameters of a subordinate device. These parameters can be read and written using the function codes FC3 and FC16.

Device Identification

Table 21: General Module Parameters – Device Identification

Address		Access	Data Type	Description
Dec.	Hex.			
2	0002	read only	UNIT32	Item Number
4	0004	read only	UNIT32	Item number extension
8	0008	read/write	UNIT32	Consecutive number (“High Word”)
10	000 A	read/write	UNIT32	Consecutive number (“Low Word”)
12	000C	read only	UNIT16	Firmware version (major)
13	000D	read only	UNIT16	Firmware version (minor)
14	000E	read only	UNIT16	Firmware version (bug fix)
15	000F	read/write	UNIT16	Hardware version
20	0014	read only	CHAR32	Item Description
36	0024	read/write	CHAR32	Device name
52	0034	read/write	CHAR32	Customer information (1)
68	0044	read/write	CHAR32	Customer information (2)
84	0054	read only	CHAR8	Password

Address		Access	Data Type	Description
Dec.	Hex.			
92	005C	read/write	CHAR16	Password Level

“Password Level” Parameter

The behavior of the product with regard to password protection is controlled by the “Password level” parameter. There are four password levels for this:

- 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 write- and read-protected.
- Password level 3 (value 3): All parameters are write- and read-protected. In addition, process data outputs (e.g., “Switch product on and off” or “Activate digital output”) are write-protected.

Table 22: General Module 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

4.3.2 Specific Module Parameters of the WAGO Power Supply Pro 2

The Modus TCP communication module uses the following general parameters of a subordinate WAGO Pro 2 Power Supply. These parameters can be read and written using the function codes FC3 and FC16.

DC Output

Table 23: Parameter – DC Output

Address		Access	Data Type	Description	
Dec.	Hex.				
136	0088	read/write	UNIT16	Output voltage (unit: mV)	
137	0089	read/write	UNIT16	Warning threshold (unit: mA)	
138	008 A	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

Address		Access	Data Type	Description	
Dec.	Hex.				
				Bit 13	PowerBoost
				Bit 14	TopBoost
				Bit 15	reserved
139	008B	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	0094	read/write	UNIT16	Trip current (unit: mA)
149	0095	read/write	UNIT16	Trip delay (unit: ms)

Signaling – Digital Input

Table 25: Parameter – Signaling – Digital Input

Address		Access	Data Type	Description	
Dec.	Hex.				
168	00A8	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	00B0	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	Switch digital output on and off.

Address		Access	Data Type	Description	
Dec.	Hex.				
				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	00BD	read/write	UNIT16	Bit 0[1)]	Behavior on application of power — previous state restored.
				Bit 1[1)]	Behavior on application of power — DC output is switched on.
				Bit 2[1)]	Behavior on application of power — 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 reset 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.

4.3.3 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 using the 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	Status DC O.K.
					Bit 1	Overtemperature
					Bit 2	No output voltage
					Bit 3	Short circuit at output
					Bit 4	Status on 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 for the previous second (unit: Ws)
1290	0x050A	10	0x000A	UNIT32	Output level for the previous minute (unit: Ws)
1292	0x050C	12	0x000C	UNIT32	Output level for the previous hour (unit: Wh)

4.3.4 Internal Module Parameters

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

Cross-device Information for Identification

Table 33: Internal Module Parameters — Cross-device Information for Identification

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

General ETHERNET Settings

Table 34: Internal Module Parameters – General ETHERNET Settings

Address		Access	Data Type	Description	Value Limits		
Dec.	Hex.				Factory Settings	min	max
0xFD6A	64874	read only	CHAR[6]	MAC address of the communication module			
0xFD6D	64877	read/write	CHAR[4]	IP address of the communication module	192 168 1 17		
0xFD6F	64879	read/write	CHAR[4]	Subnet mask of the communication module	255 255 255 0		
0xFD71	64881	read/write	CHAR[4]	Gateway address	192 168 1 1		
0xFD74	64884	read/write	UINT16	Enables fast aging (0 = off, 1 = on).	0		
0xFD76	64886	read/write	UINT16	Enables WBM via http (0 = off, 1 = on).	1	0	1
0xFD77	64887	read/write	UINT16	Enables WBM via https.	1	0	1
0xFD78	64888	read/write	UINT16	Enables SNTP (0 = off, 1 = on).	0	0	1

Address		Access	Data Type	Description	Value Limits		
Dec.	Hex.				Factory Settings	min	max
0xFD7C	64892	read/write	CHAR[4]	IP address of the SNTP server	192 168 1 109		

Switch Settings for Channel 1

Table 35: Internal Module Parameters – Switch Settings for Channel 1

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

Switch Settings for Channel 2

Table 36: Internal Module Parameters – Switch Settings for Channel 2

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

Date

Table 37: Internal Module Parameters – Date

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

Time

Table 38: Internal Module Parameters – Time

Address		Access	Data Type	Description	Value Limits		
Dec.	Hex.				Factory Settings	min	max
0xFE06	65030	read/write	CHAR	Hours	4	0	24
0xFE06	65030.5	read/write	CHAR	Minutes	26	0	59
0xFE07	65031	read/write	CHAR	Seconds	37	0	59
0xFE08	65032	read/write	INT16	Timezone	2	-12	12

Address		Access	Data Type	Description	Value Limits		
Dec.	Hex.				Factory Settings	min	max
0xFE09	65033	read/write	UINT16	Synchronization mode (1 = off, 2 = Read time from the lower-level device, 4 = Write time from module, 8 = Update time with SNTP)	1		

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 (**Technical data [▶ 15]**).

Installation and Removal

NOTICE

Avoid electrostatic discharge!

The products are equipped with electronic components that may be destroyed by electrostatic discharge when touched. Please observe the safety precautions against electrostatic discharge per DIN EN 61340-5-1/-3. When handling the products, please ensure that environmental elements (personnel, work space and packaging) are properly grounded.

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.

Mounting Positions

Nominal mounting position: Front side facing forwards, marking legible, and bottom ventilation openings facing upwards and downwards.

Mounting

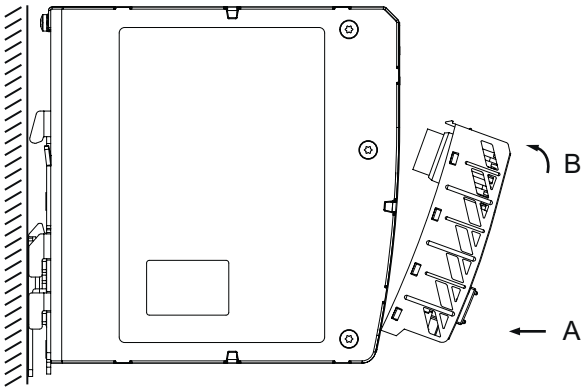


Figure 6: Mounting

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

1. Remove the cap of 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 on 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 catch in the top mounting slots.
6. Check that the product is properly locked position.

Removal

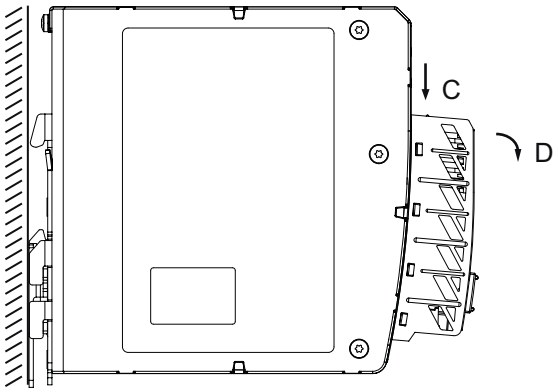


Figure 7: Removal

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 Preparation

- Install the Modbus TCP Communication Module on a subordinate 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.

7.2 Setting an IP address

7.2.1 Assigning an IP Address Using DHCP

If there is a DHCP server in the network, the network settings are assigned 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, the communication module expects a DHCP to always be available.

If an IP address has been assigned by DHCP, it can be determined by the settings or the output of the respective DHCP server, e.g., via the output of “Open DHCP”.

If no DHCP server is available after a power-on reset, the default network settings are made after 4 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 when 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 there is a common subnet!

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

Note

IP addresses obtained via DHCP server are 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”. There are multiple options for switching the addressing.

7.2.2.1 Setting the IP Address via the WBM

Call up the WBM of the communication module in a browser.

Go to the **[Module Settings]** menu item. In the **[ETHERNET Settings]** area, you can make the required network settings.

The communication module must be restarted for the settings to be applied. Press the **[Reboot module]** button or power cycle your system.

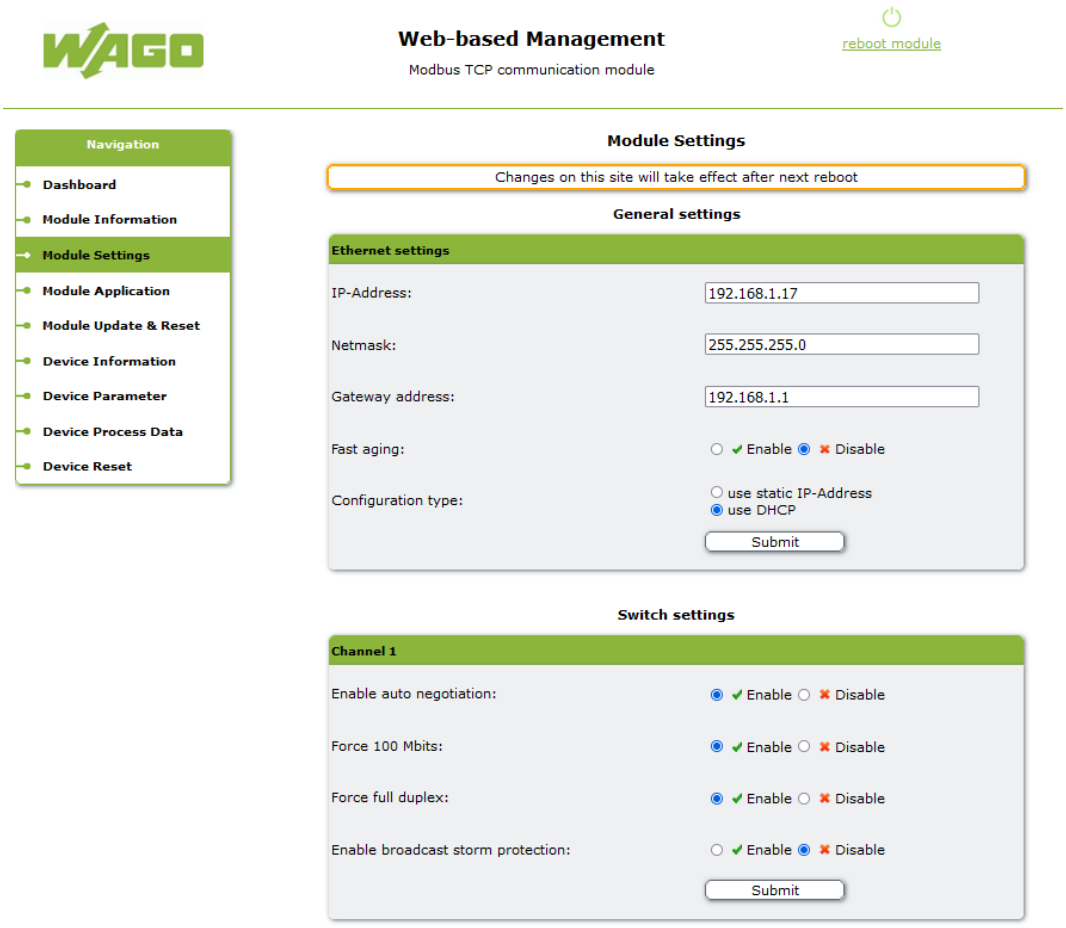


Figure 8: WBM “Module Settings” Page

7.2.2.2 Setting the IP Address with the Reset Button

Press the reset button for 8 seconds until the “COM OK” LED lights up briefly. Release the 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

Operation

8.1 Operating the Reset Button

You can reset the product using the reset button.

The following settings options are available:

Table 39: Operating the Reset Button

Settings Option	Description	Signaling via Optical Status Display
Press the reset button for 8 seconds.	Disables DHCP and sets the IP address to 192.168.1.17.	COM OK flashes once.
Press the reset button for 10 seconds.	Resets the Modbus TCP Communication Module to factory settings	ERR flashes at 16 Hz.

Configuration

9.1 Configuration with the Web-Based Management System

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

9.1.1 “Dashboard” Page

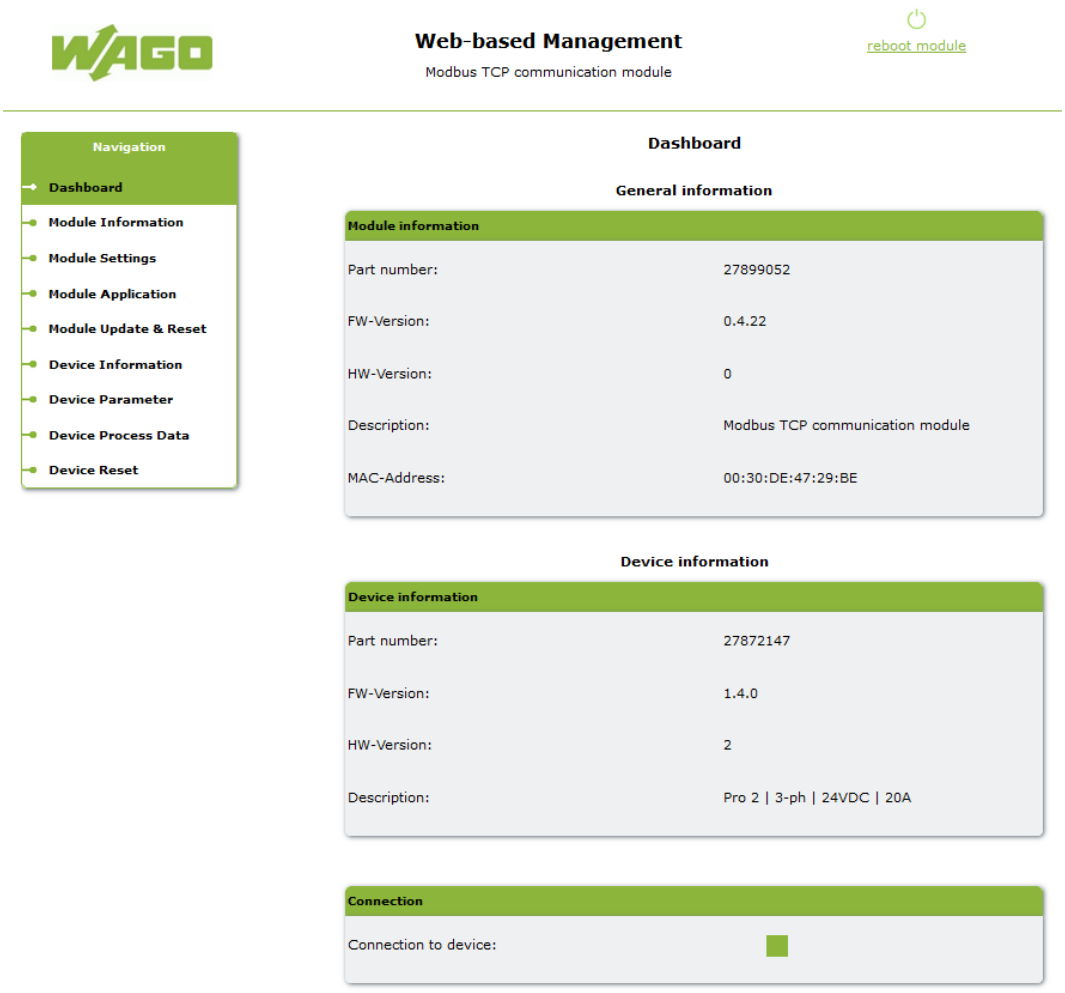


Figure 9: WBM “Dashboard” Page

The dashboard is used to provide a brief overview of essential information from the communication module and the subordinate device.

9.1.1.1 Module Information

Information from the communication module

9.1.1.2 Device Information

Information from the subordinate device

9.1.1.3 Connection

Display of the status of the connection to the subordinate device

- Green: Connection established
- Red: Connection interrupted

9.1.1.4 “Module Information” Page

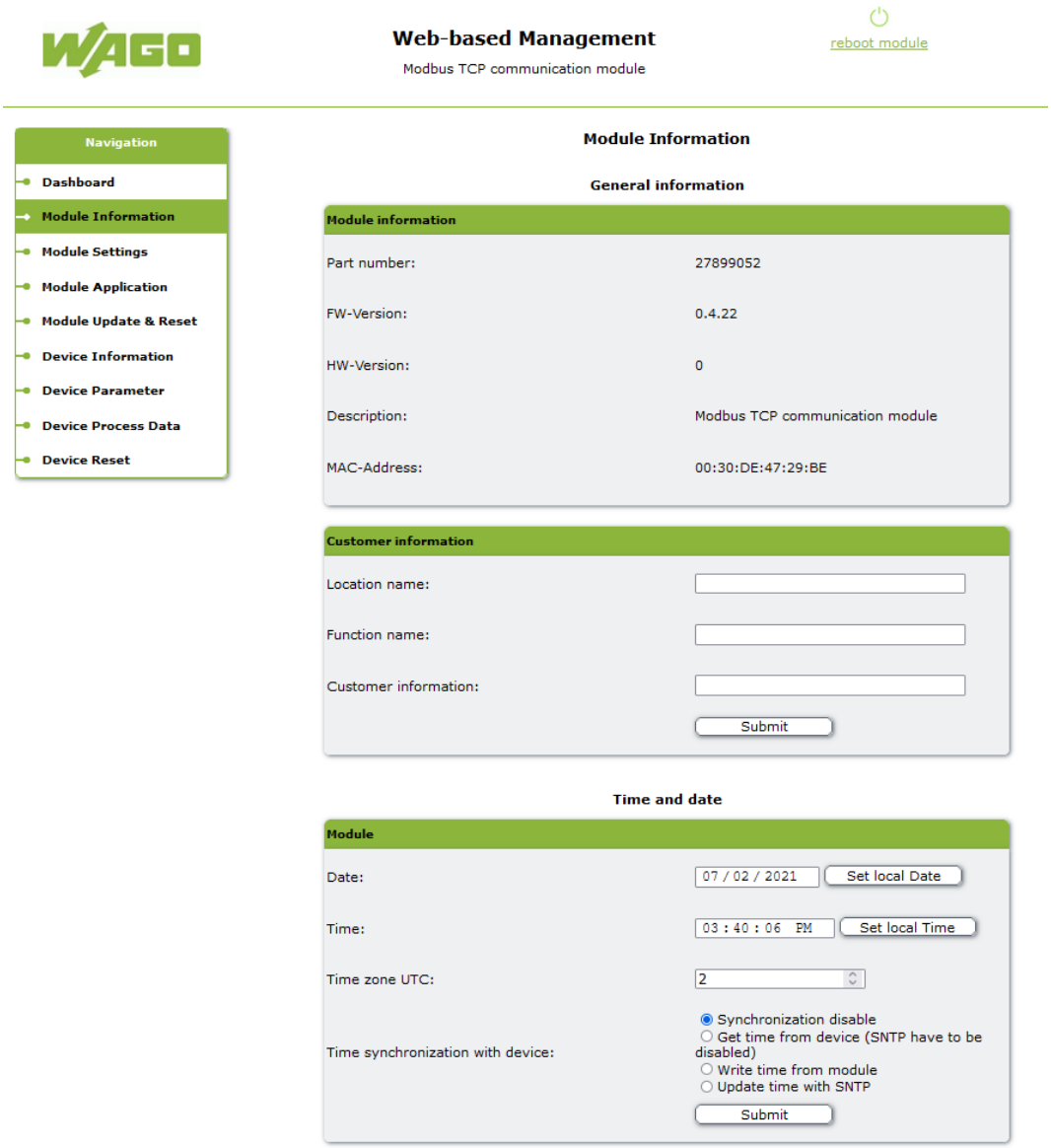


Figure 10: WBM “Module Information” Page

Display or change of the parameters of the communication module

9.1.2 “Module Settings” Page

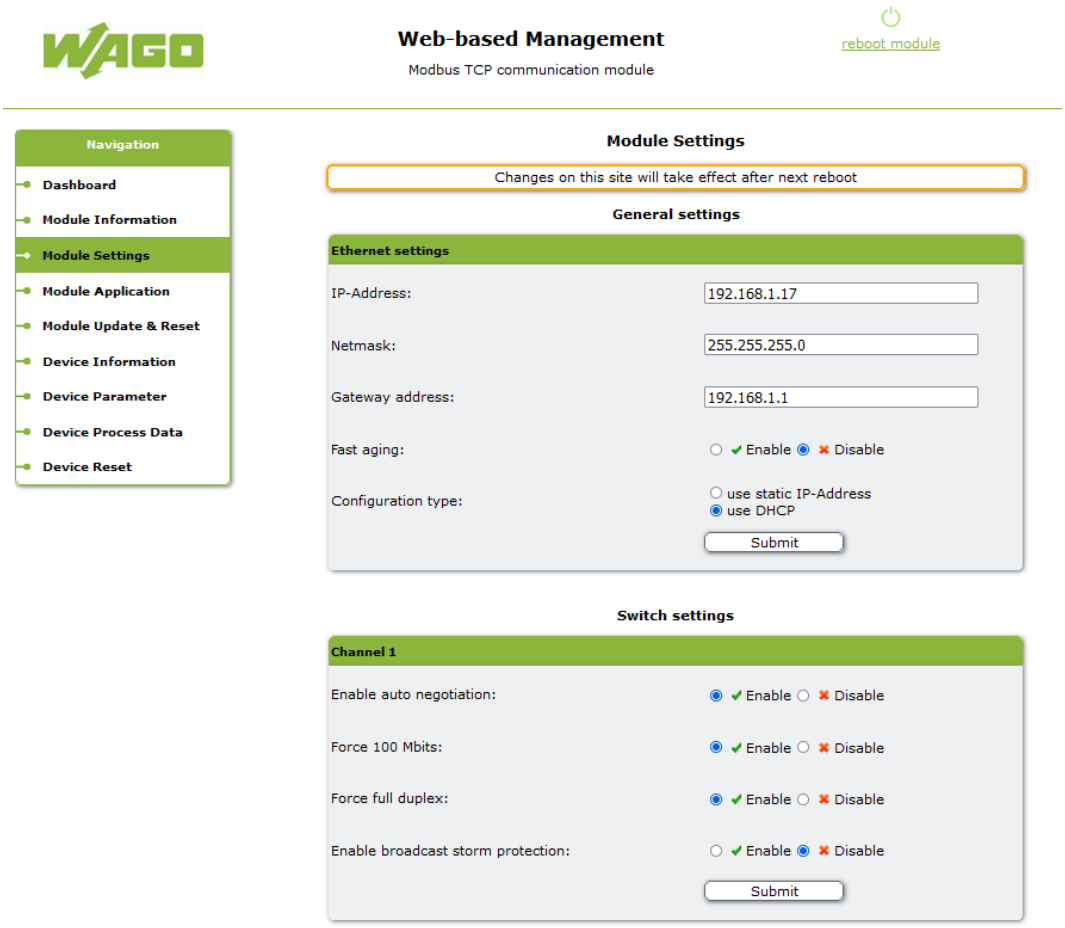


Figure 11: WBM “Module Settings” Page

9.1.2.1 General Settings (ETHERNET Settings)

Display or change of the network settings of the module

9.1.2.2 Switch Settings (Channel1), Switch Settings (Channel2)

- Enable Auto Negotiation
  - Auto Negotiation allows the UTP link partners (Unshielded Twisted Pair) to select the best common operating mode in accordance with Clause 28 of the IEEE 802.3u specification.
    With Auto Negotiation, the link partners share their capabilities with each other via the connection.
- Force 100 Mbits
  - Forces the connection over 100 Mbits.
- Force Full Duplex
  - Forces the connection using full duplex.
- Enable Broadcast Storm Protection
  - This is an 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 into account “multicast packets” for storm control.

9.1.3 “Module Application” Page

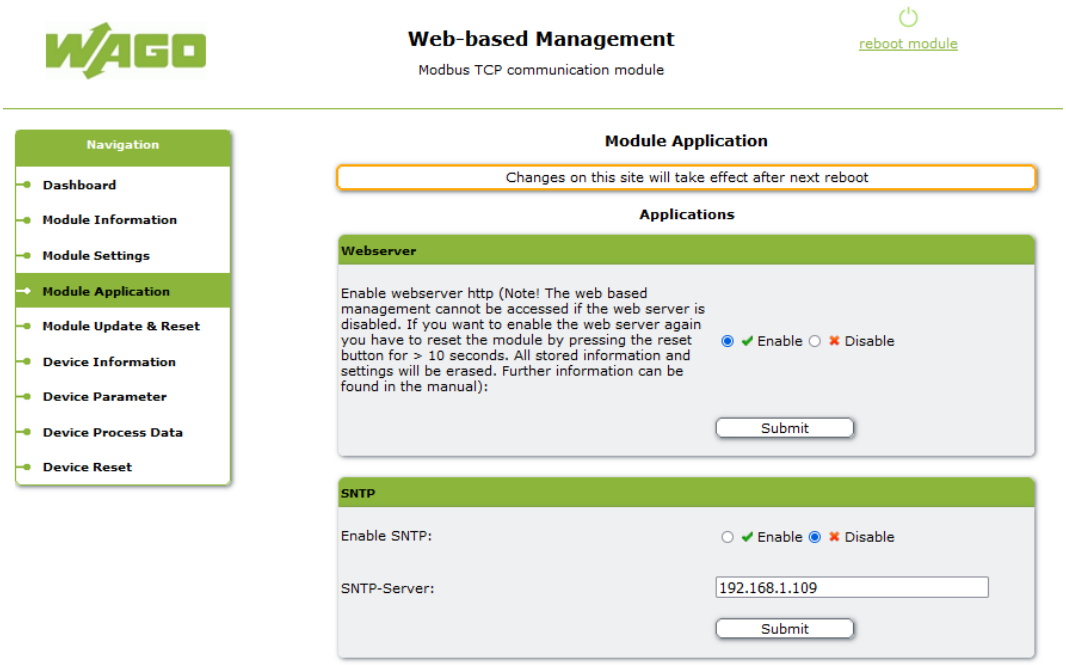


Figure 12: WBM “Module Application” Page

ⓘ Note

Disabling the Web server closes ports 80 and 443 and the module can then no longer be accessed via a web browser.
To enable access again via the Web server, the reset button on the module must be physically pressed on site for longer than 10 seconds and the module is reset to the factory settings, or the register 0xFD76 for HTTP or 0xFD77 for HTTPS must be set to 1 via Modbus TCP.

9.1.4 “Module Update and Reset” Page

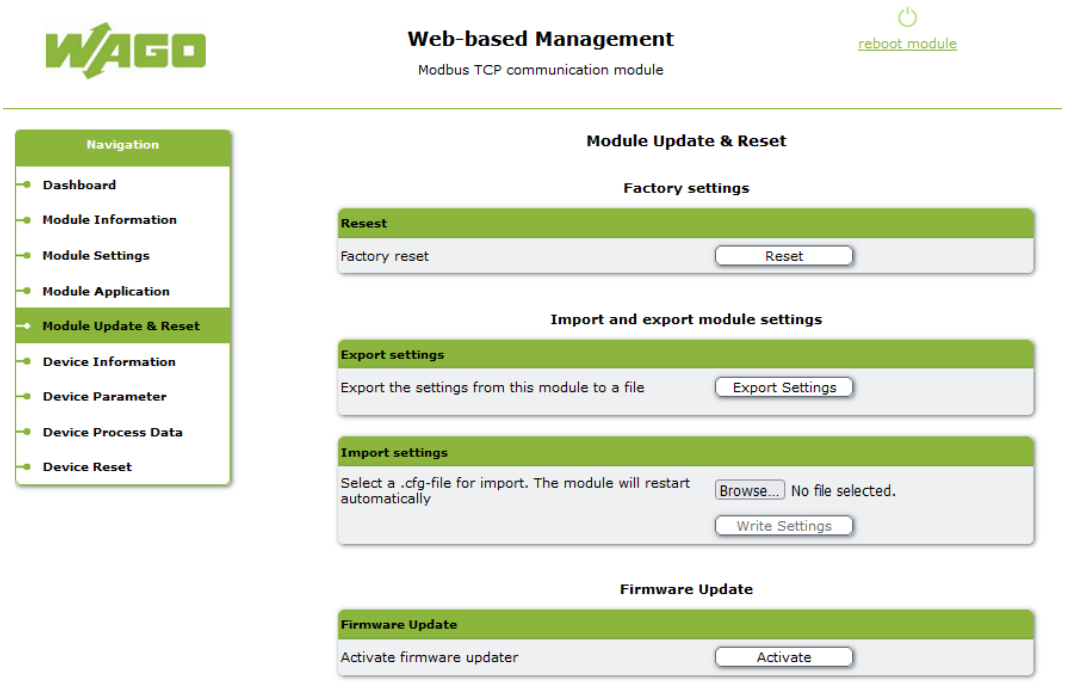


Figure 13: WBM “Module Update and Reset” Page

On the “Module Update and Reset” page, you can restore the module to the factory settings, export module parameters and transfer them to another module.

You can also update the firmware of the module. Please note that the module firmware can only be updated via the http protocol.

9.1.5 “Device Information” Page

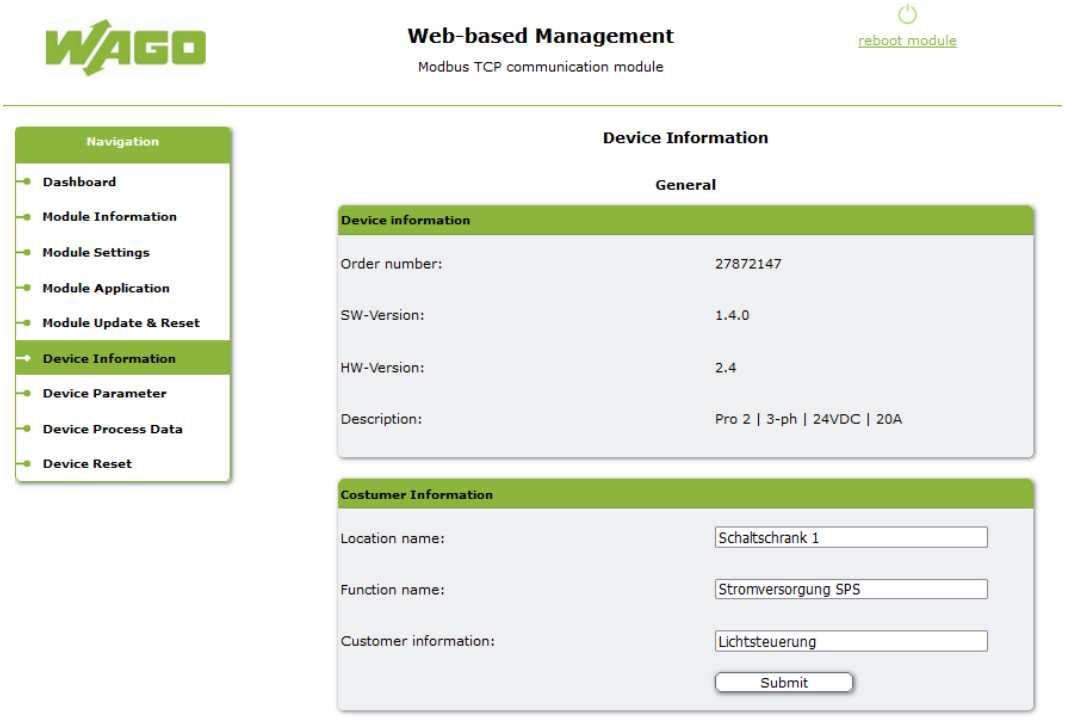


Figure 14: WBM “Device Information” Page

Displays the device information of the subordinate device.

9.1.6 “Device Parameter” Page

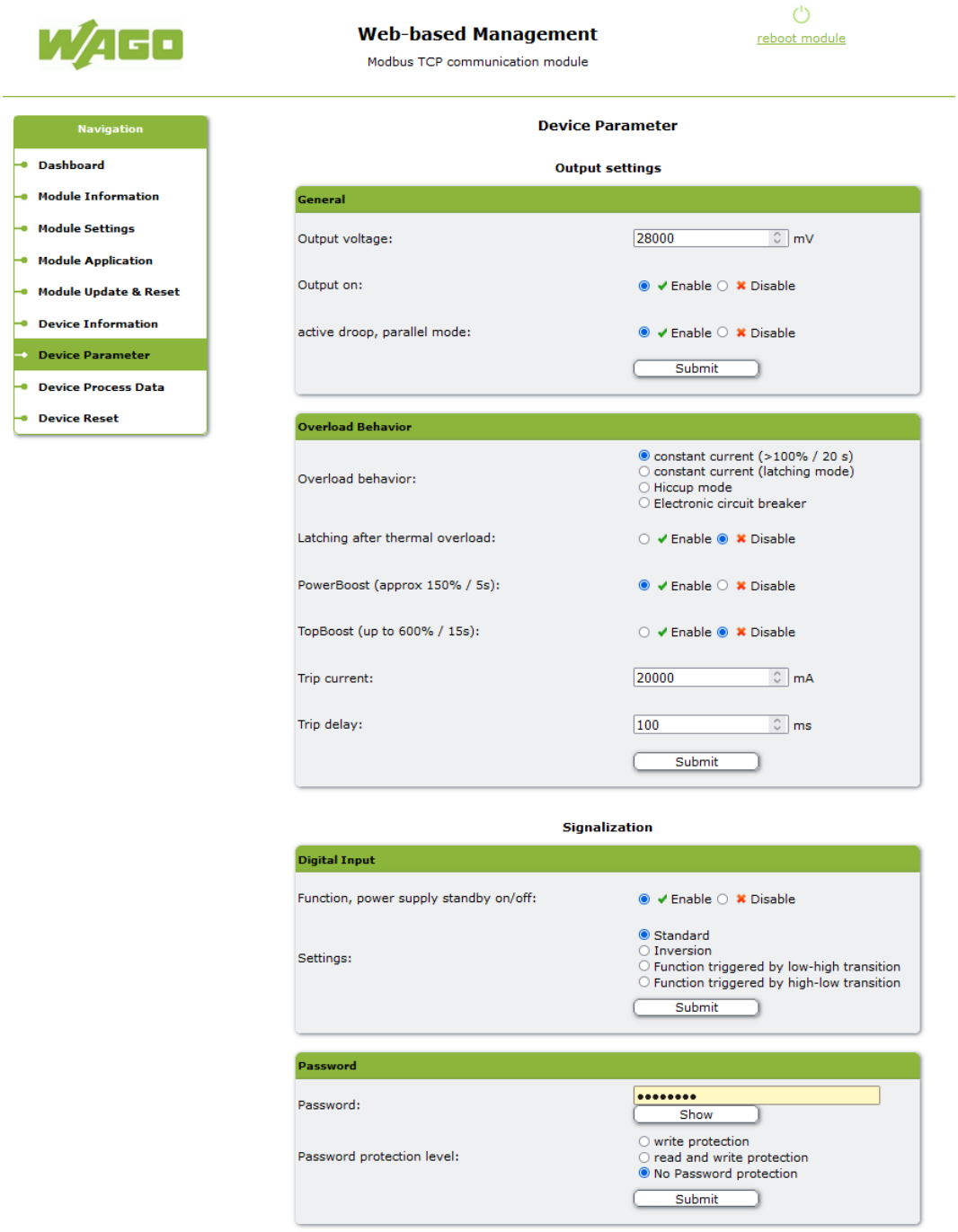


Figure 15: WBM “Device Parameter” Page

All parameters are read from the subordinate device and displayed on the “Device Parameter” page.

9.1.7 “Device Process Data” Page

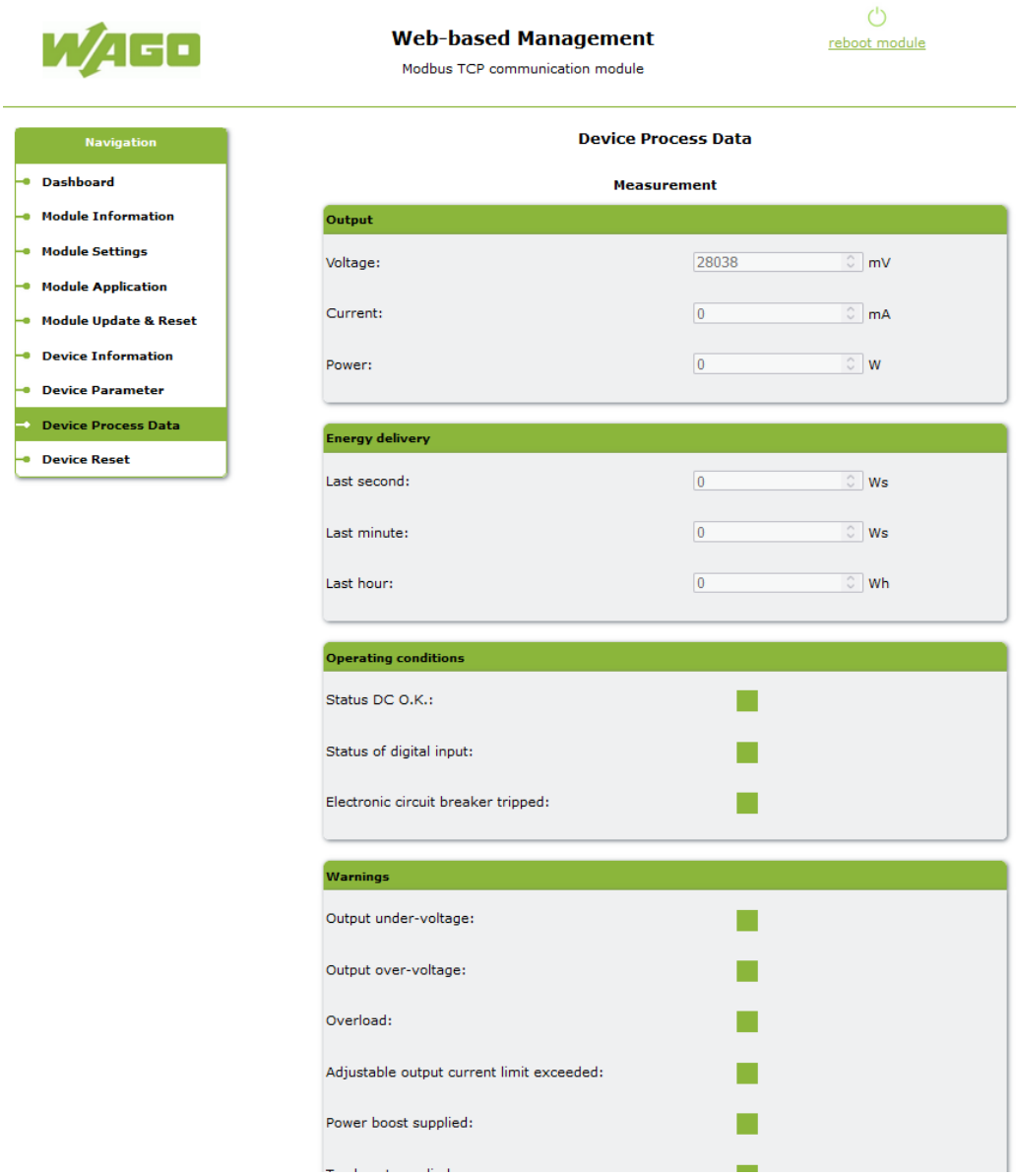


Figure 16: WBM “Device Process Data” Page

All measured values and status information are read out from the subordinate device and displayed on the “Device Process Data” page.

9.1.8 “Device Reset” Page

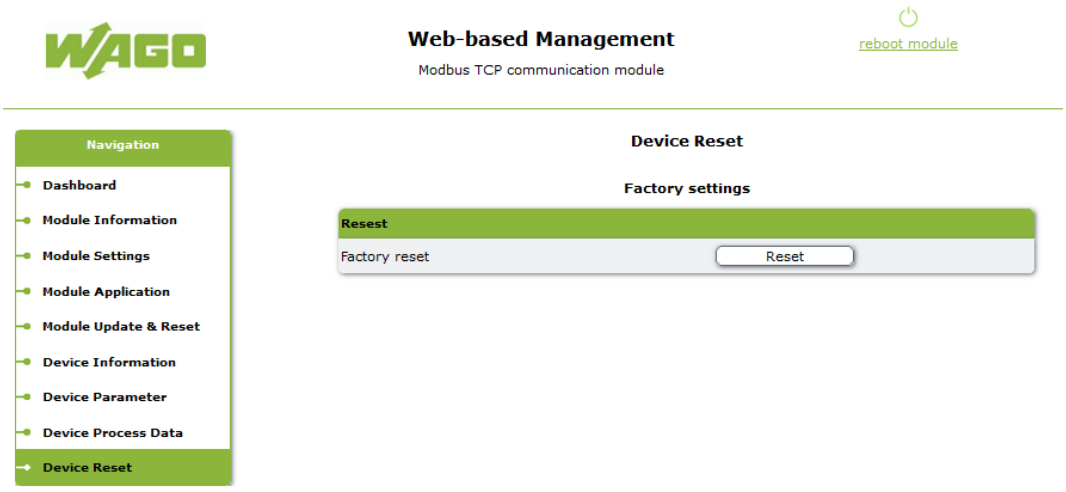


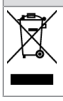
Figure 17: WBM “Device Reset” Page

On the “Device Reset” page, you can restore the subordinate device to the factory settings.

Decommissioning

10.1 Entsorgung und Recycling

Table 40: WEEE Mark

Logo	Description
	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 national and local regulations for the disposal of batteries, packaging and electrical and electronic equipment.
- Clear any data stored on electrical and electronic equipment.
- Remove any batteries or memory cards installed in electrical and electronic equipment.
- Dispose of all types of packaging to ensure a high level of recovery, reuse and recycling.
- Have electrical and electronic equipment sent to a local collection point.
- The guidelines 2006/66/EG, PPWD 2018/852/EU and WEEE 2012/19/EU apply throughout Europe. National directives and laws may vary.

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.

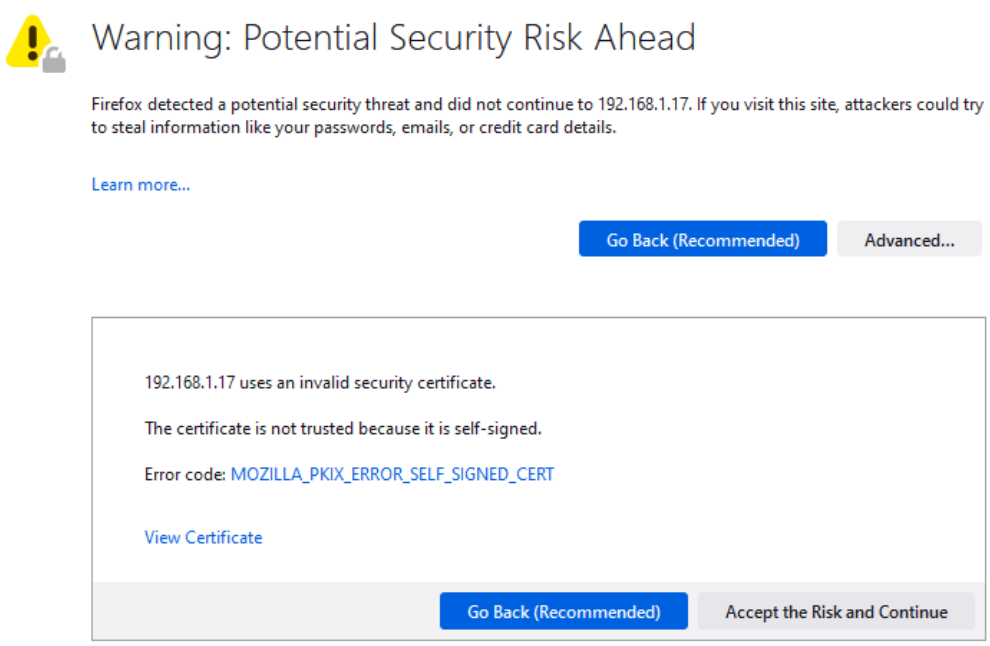


Figure 18: Browser warning message due to self-signed certificate

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 41: 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

IANA No.	Cipher Suite
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 from the **File** menu, select the **New Database** sub-menu.
2. Select a storage location and appropriate name for the database.
3. Enter a password to protect the database.

   ⇨ The newly created database then opens automatically:

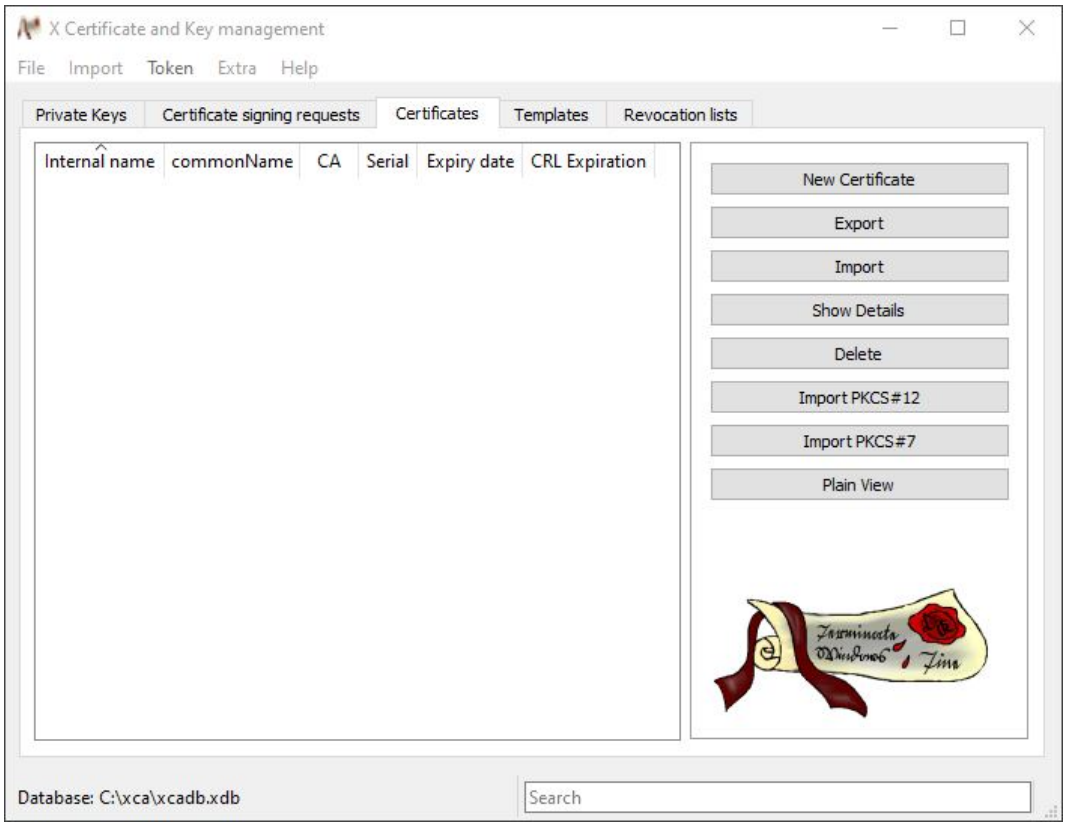


Figure 19: XCA Database

4. On the **Templates** tab, click the die **[New Template]** button.
5. Select the “**[default]** Blank Template” setting in the open “Preset Template Values” dialog.
6. Click **[OK]** to confirm the selection.
7. In the “Edit XCA Template” dialog that opens, switch to the **Subject** tab.

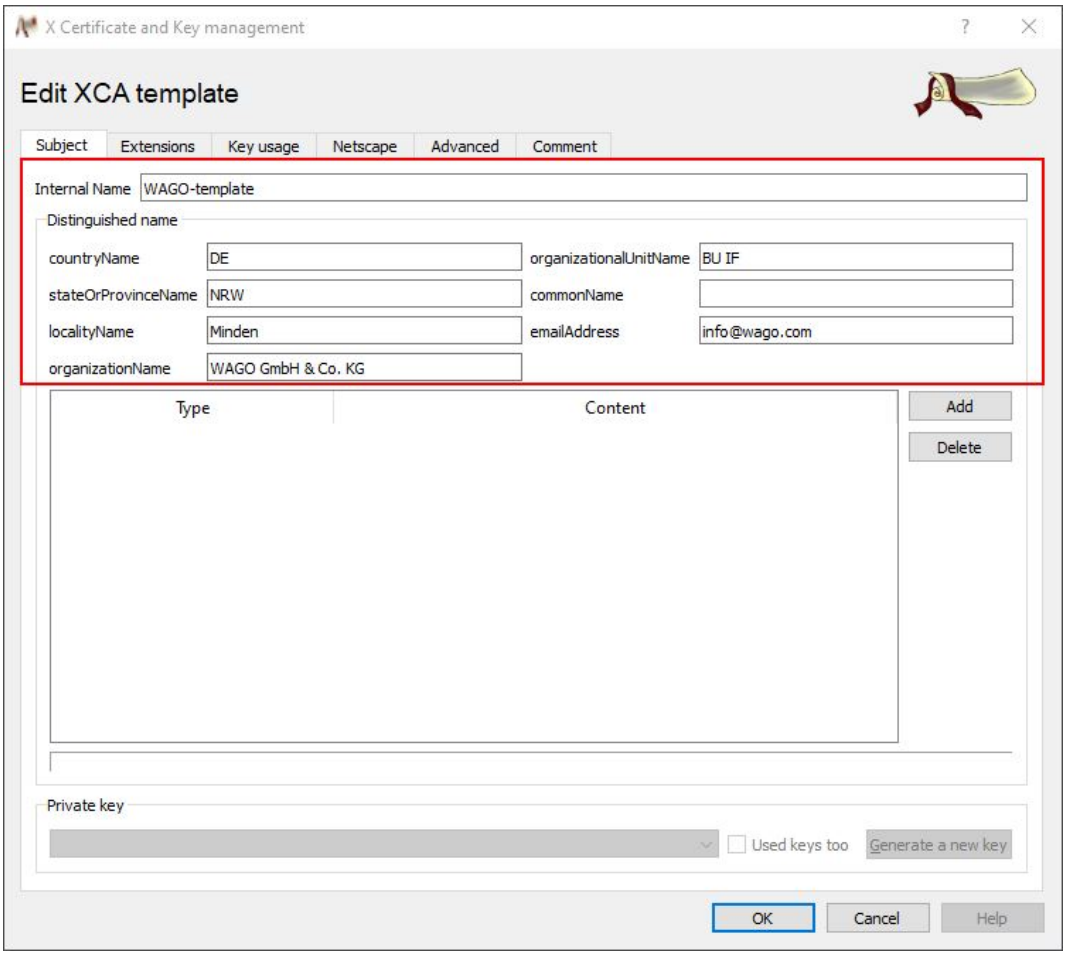


Figure 20: `Subject´ Tab

*Legend for Figure `**Subject´ 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 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 entries.

   ⇨ Once the template has been created, it is displayed in the window.

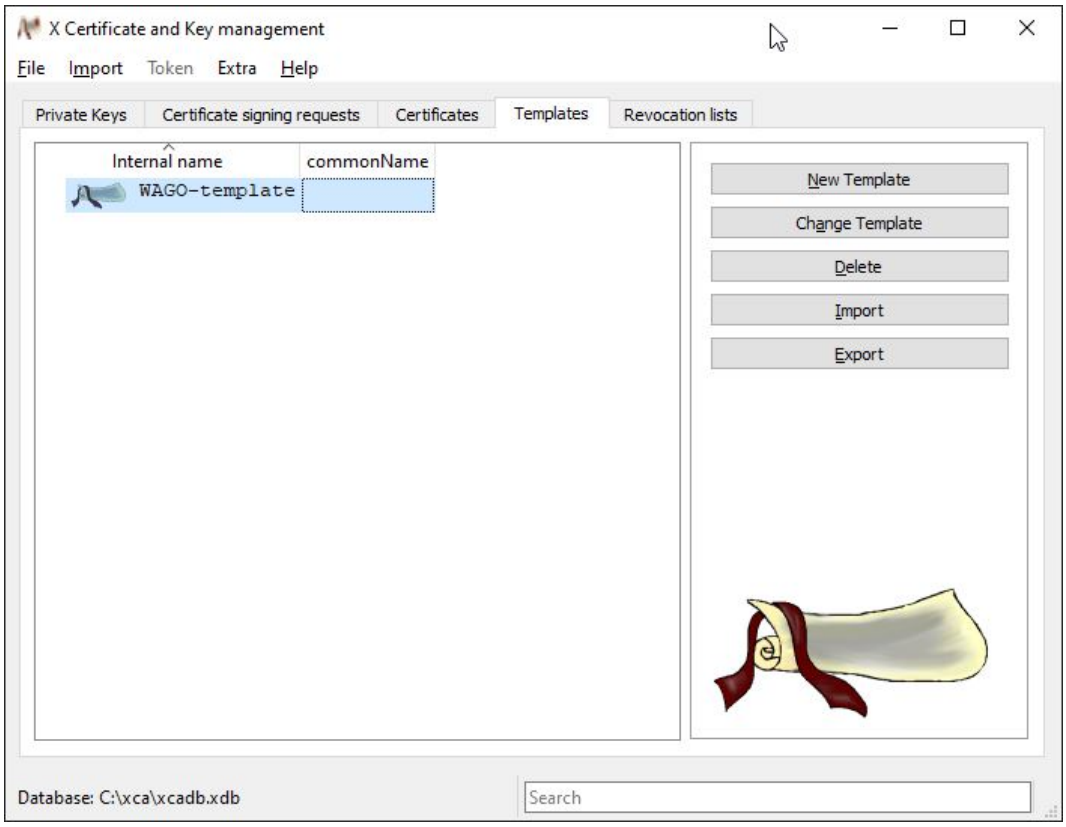


Figure 21: Create Template

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.

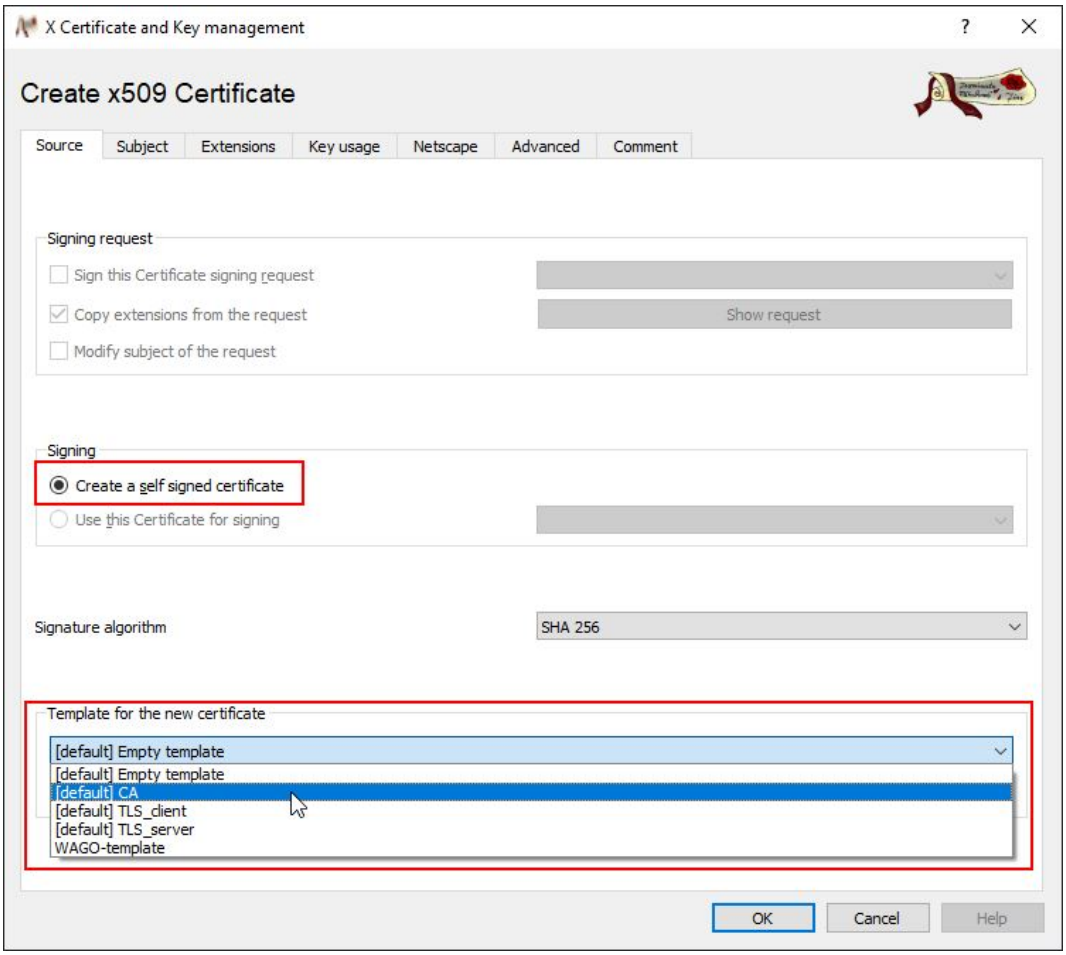


Figure 22: Create Certificate — Select Template

2. Select your created template from the **Template for the new certificate** selection field.
3. Click the **[Apply Subject]** button.
4. Select the "**[default]**" template from the **Template for the new certificate** selection field.
5. Click the **[Apply Extensions]** button.
6. Switch to the **Subject** tab.

   ⇨ The following dialog appears.

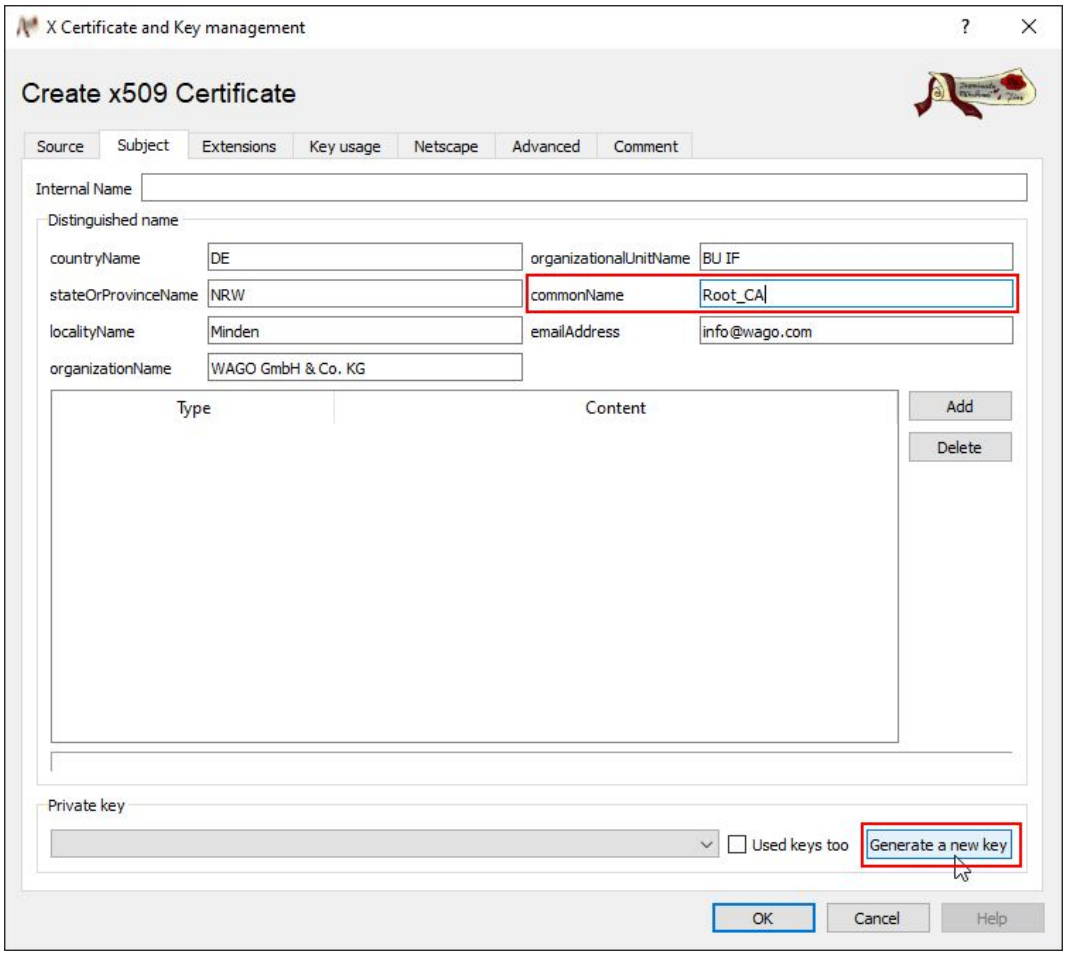


Figure 23: Create Certificate – Enter Name

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

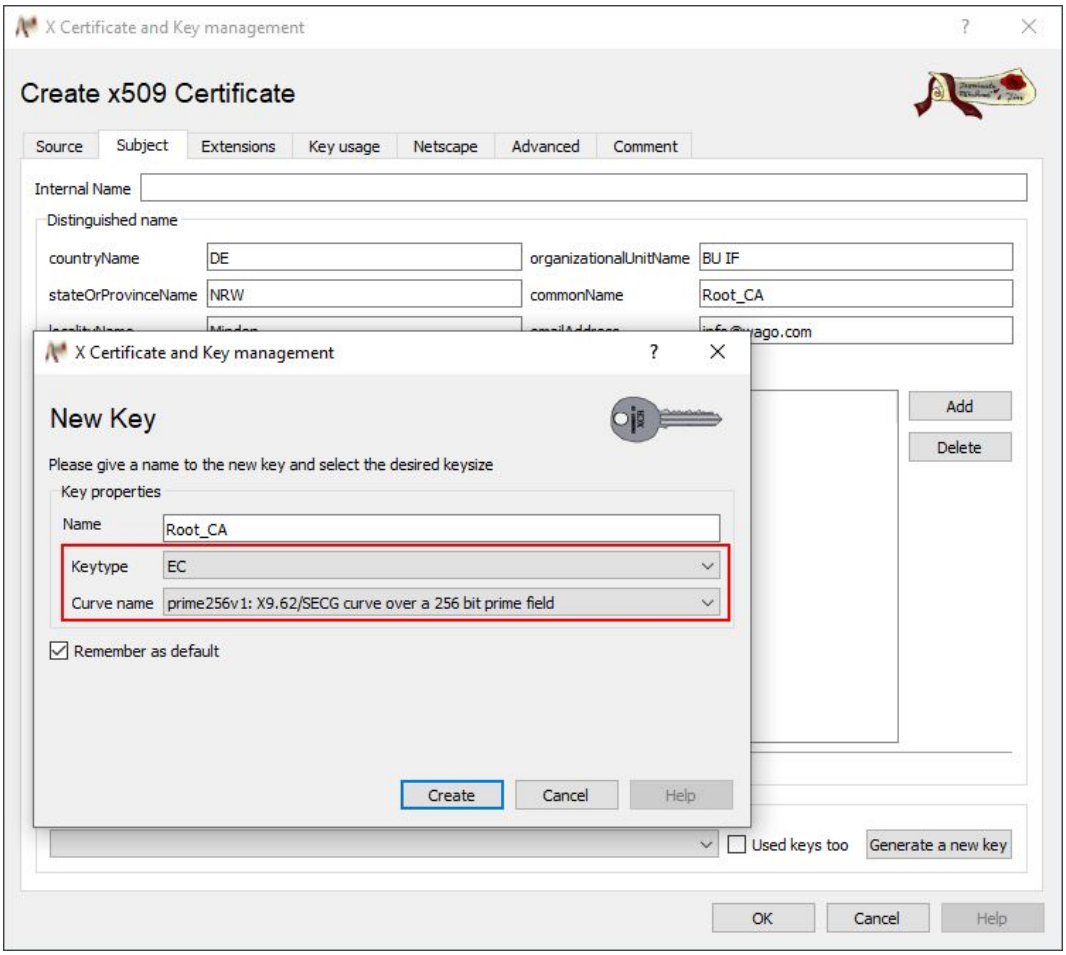


Figure 24: Create a New Key

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 is supported according to BSI TR 02102 2 (named prime256v1 in the XCA).

   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 in the **Certificates** tab.

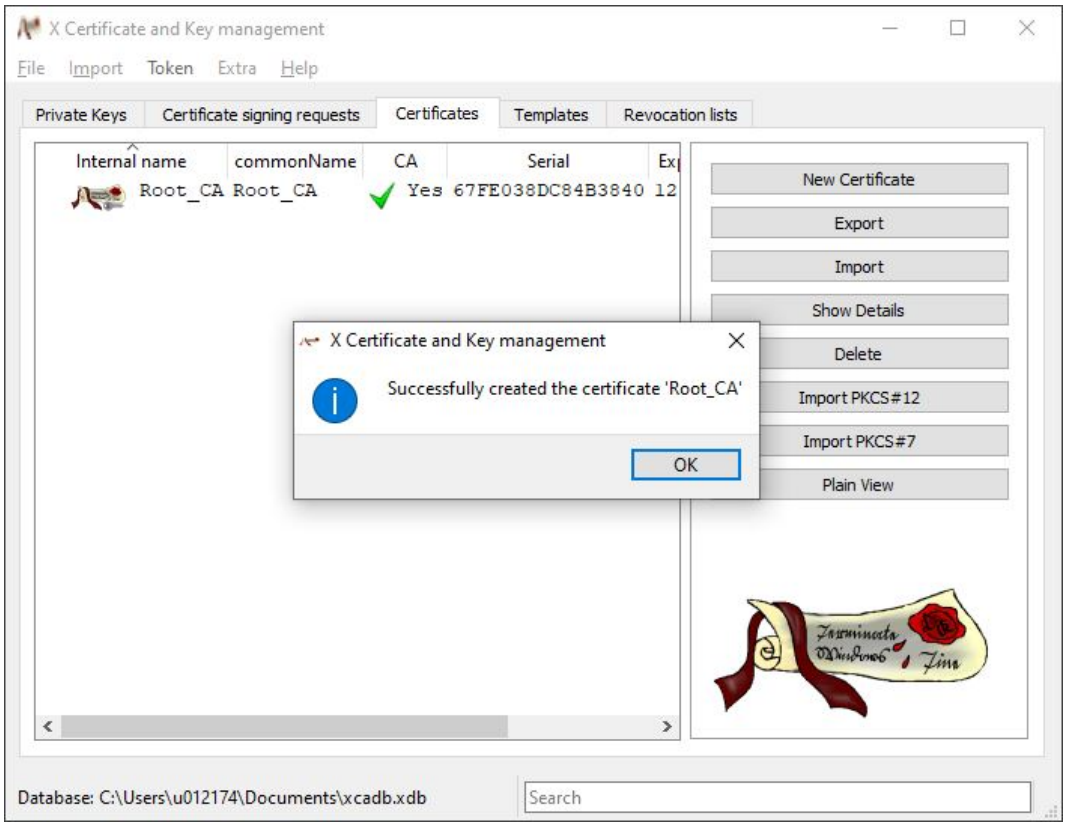


Figure 25: New Certificate Created

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.

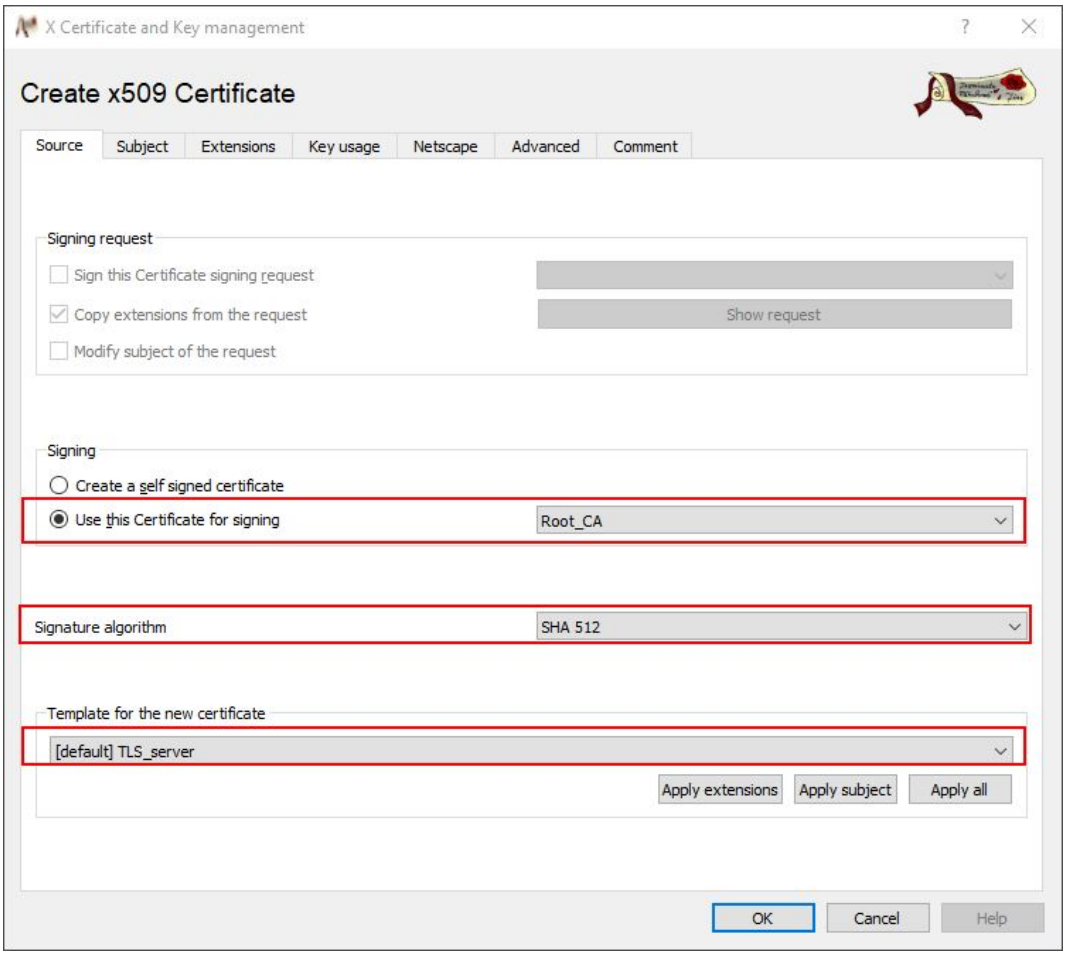


Figure 26: Create a New Device Certificate

3. Check the box **Use This Certificate for Signing** 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.

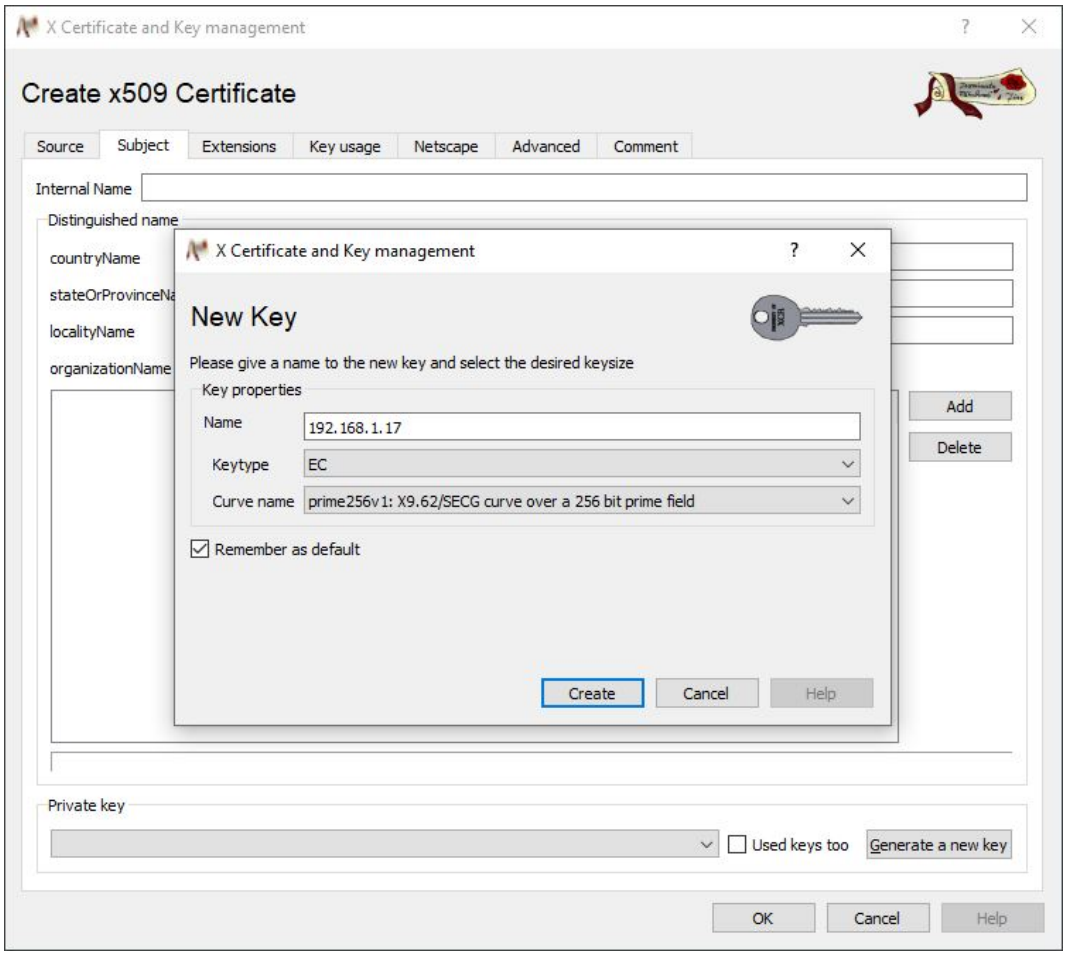


Figure 27: Create a New Key

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.

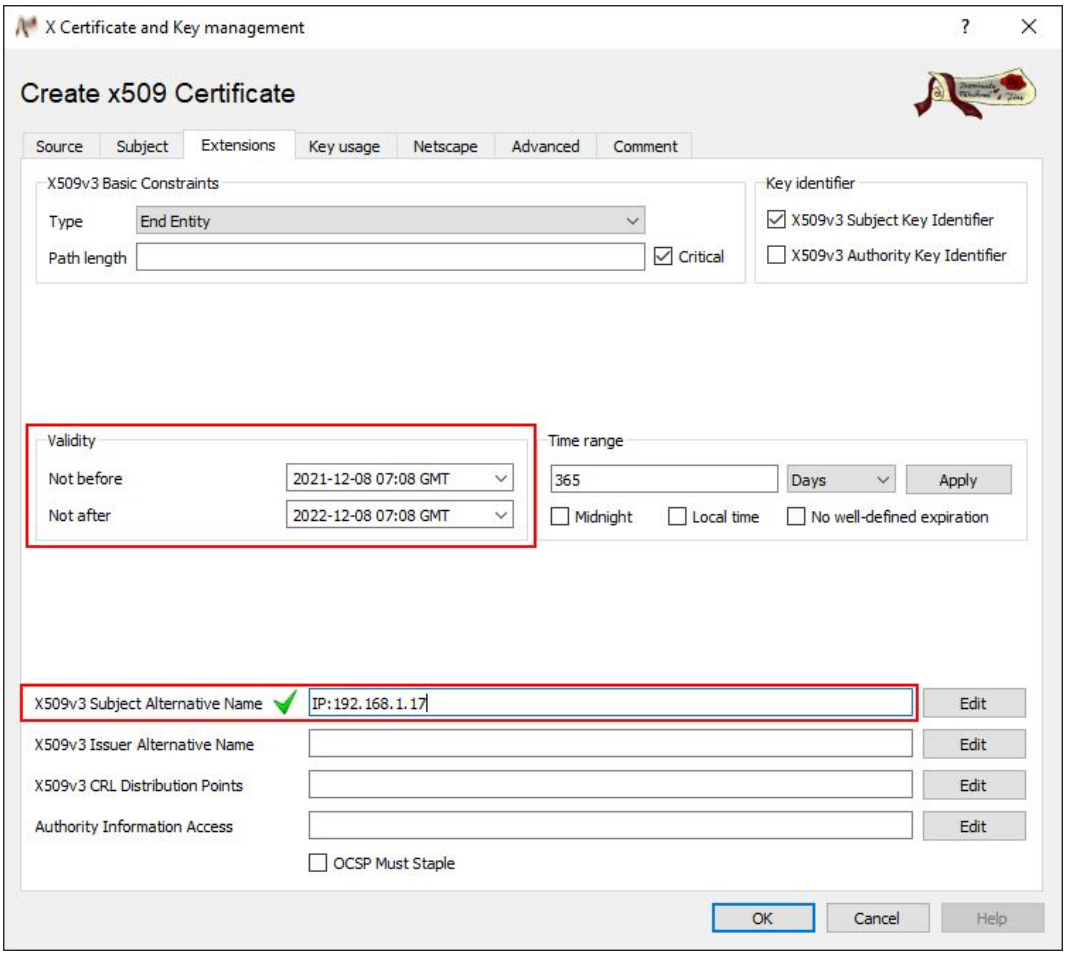


Figure 28: "Extensions" Tab

15. Set the validity of the device certificate. Please note the recommendations of the "technical guidelines of the BSI TR-02102-2".
16. Add the IP address and/or hostname 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.

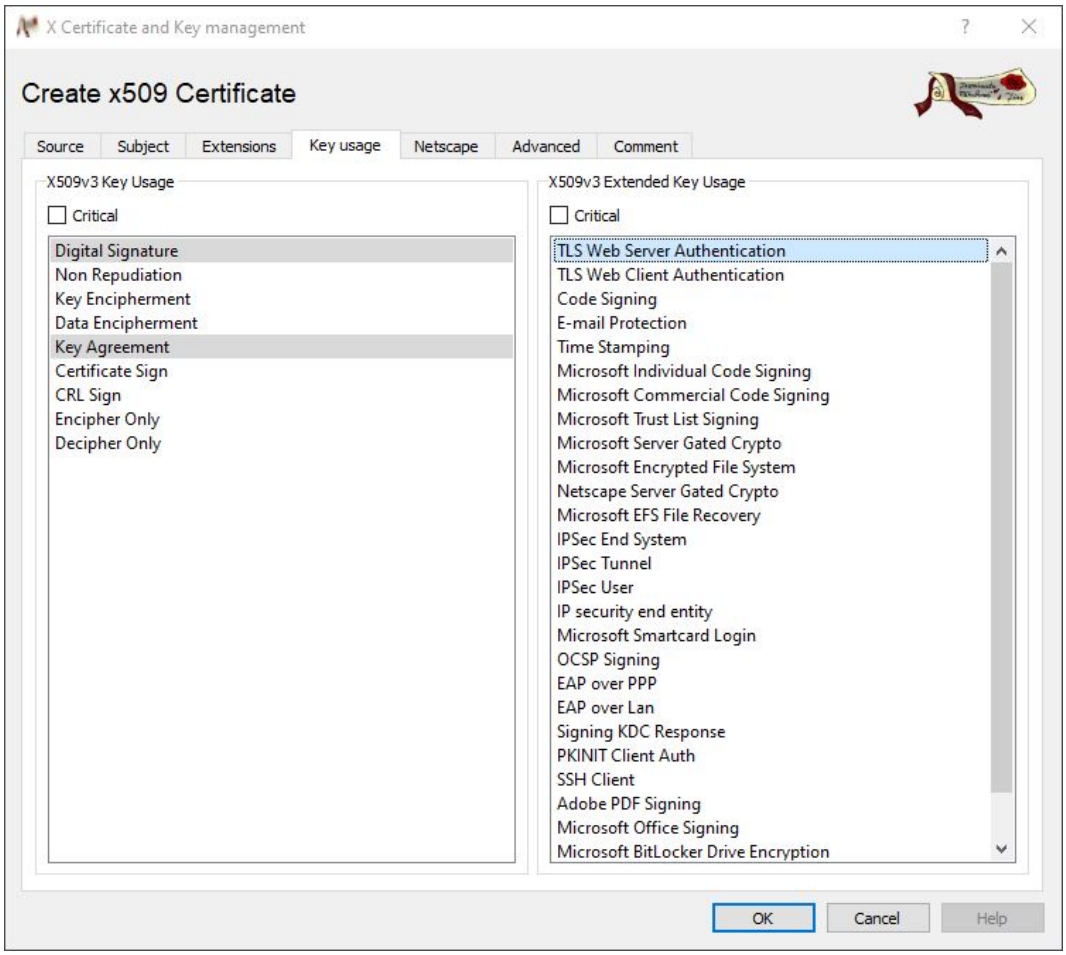


Figure 29: New Certificate Request, "Client" Key Usage

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

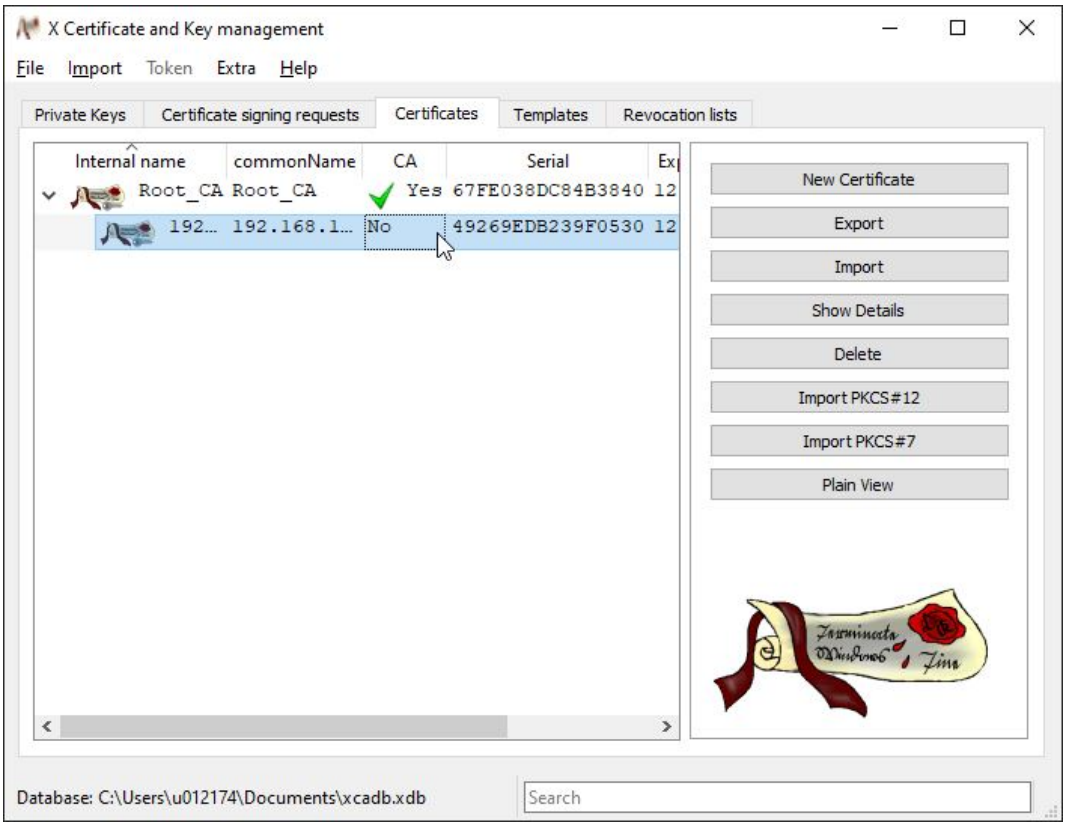


Figure 30: Device Certificate Created

11.1.5 Exporting Certificates

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

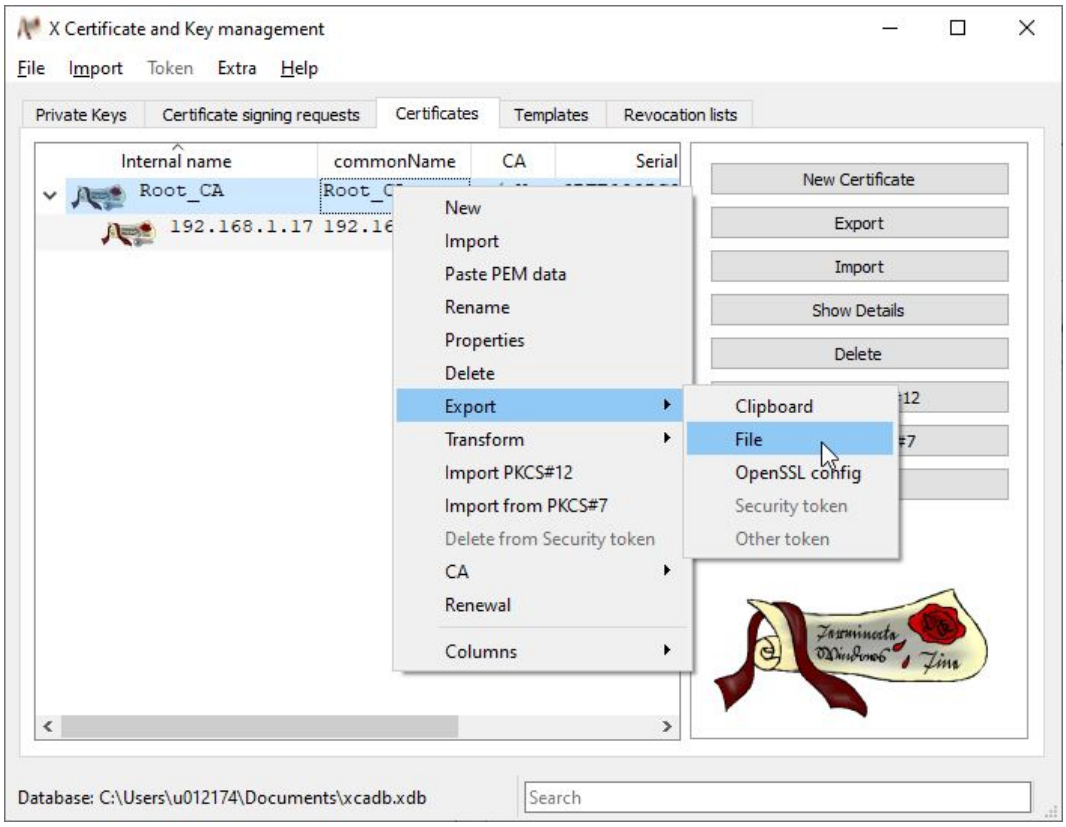


Figure 31: Export Root CA Certificate 1

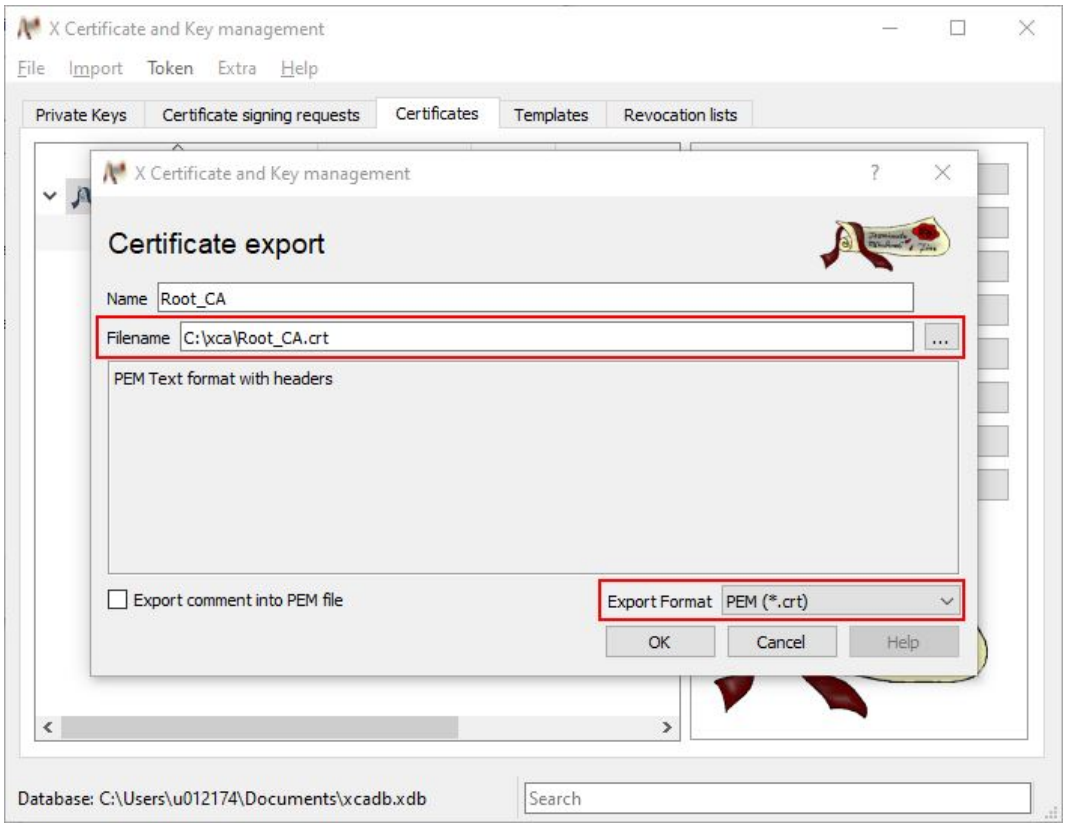


Figure 32: Export Root CA Certificate 2

4. Select the storage location by clicking the **[…]** button.
5. In 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”.

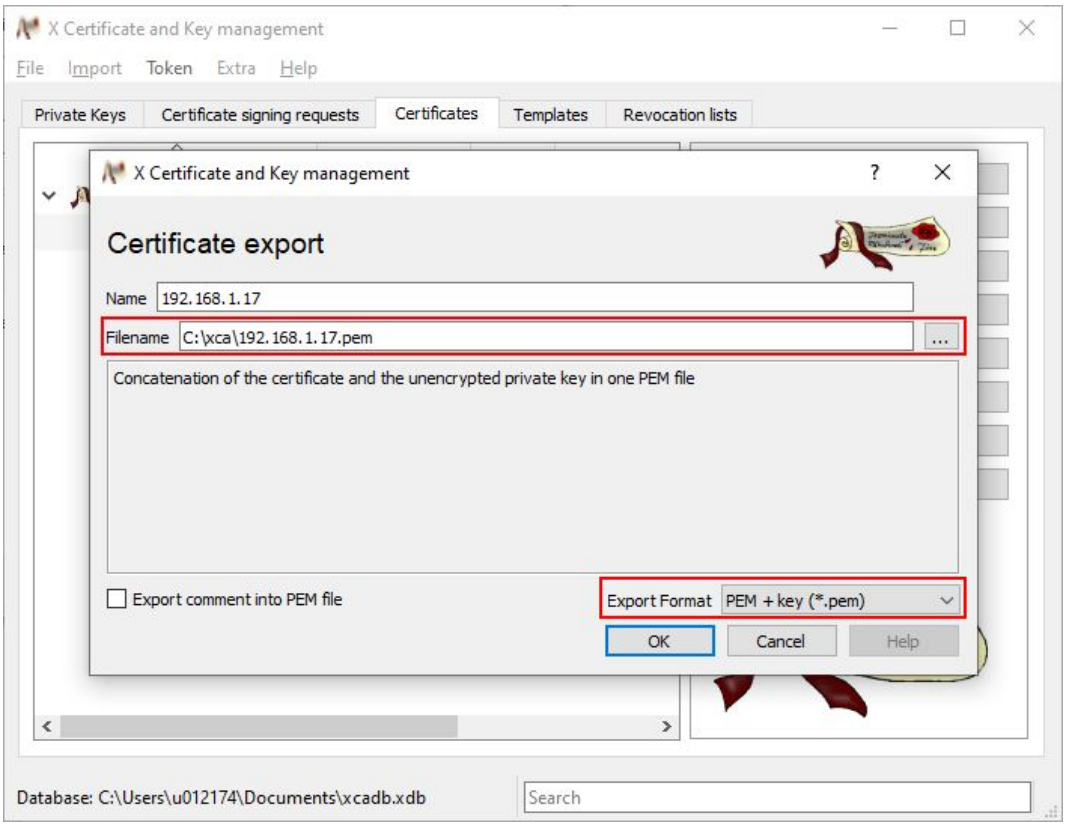


Figure 33: Exporting the Device Certificate

9. Select a storage location by clicking the **[…]** button.
10. In the **Export Format** selection list, select the “PEM + Key (*.pem)” 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 been changed, the certificate must be recreated for the device with the correct IP address or host name (see **Creating the Device Certificate [▶ 50]**)!

1. Import your root CA certificate into the browser. The process depends on the browser used.
2. Transfer your device certificate via the device WBM to the “Modbus TCP Communication Module” product. Navigate to the **Module Application** menu item and click **[Choose File]** in the **Import user certificate** submenu.

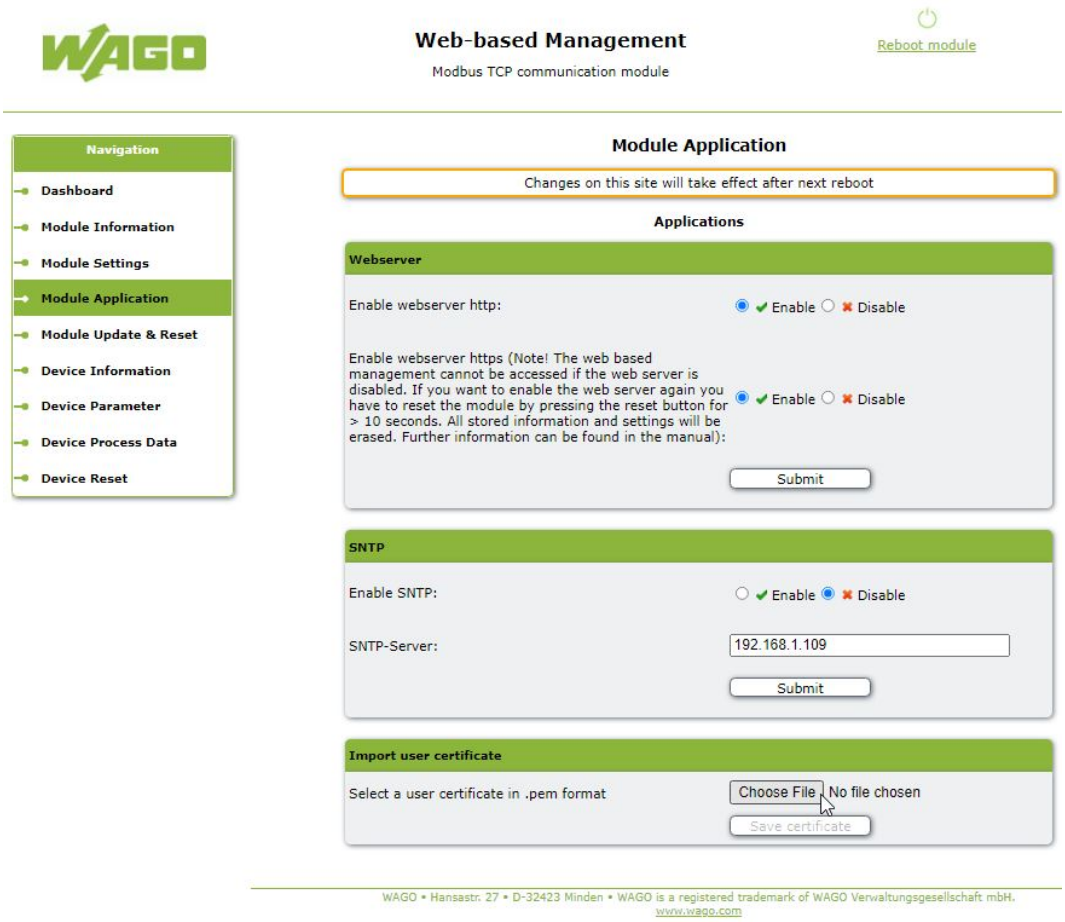


Figure 34: Importing the Device Certificate

3. Select the certificate you created and click **[Save certificate]**.
4. Reboot the device by clicking the **[Reboot module]** button.

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. The browsers often indicate how trusted a connection is in the address bar. Firefox, for example, displays a lock icon if the certificate is signed by a trusted root CA.

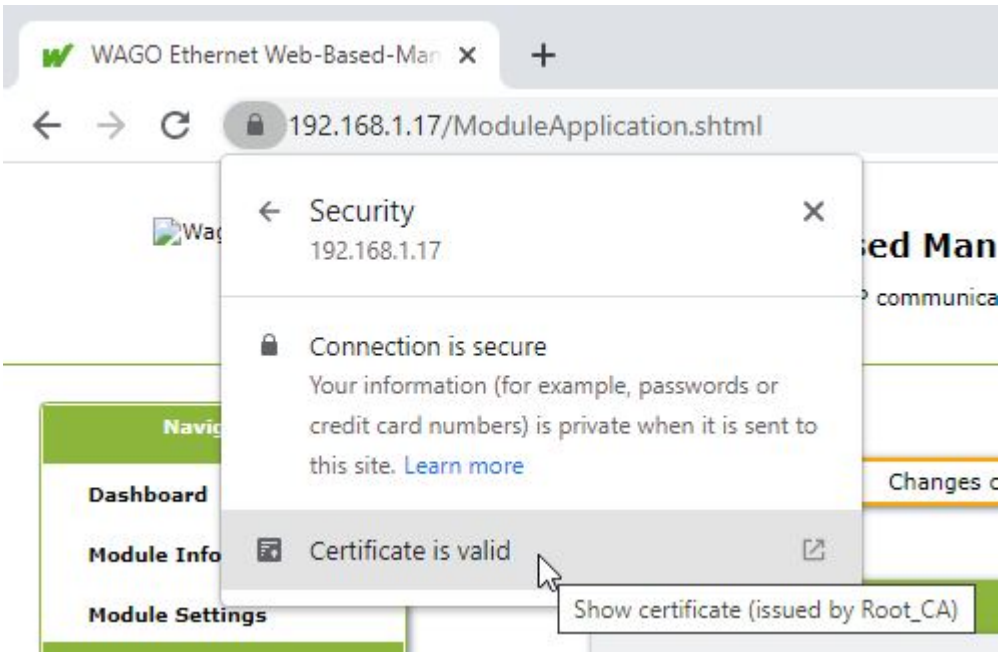


Figure 35: Importing the Device Certificate – Secure Connection

11.2 Accessories

The following accessories are available for the product:

Accessories – Marking

Table 42: 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 43: 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