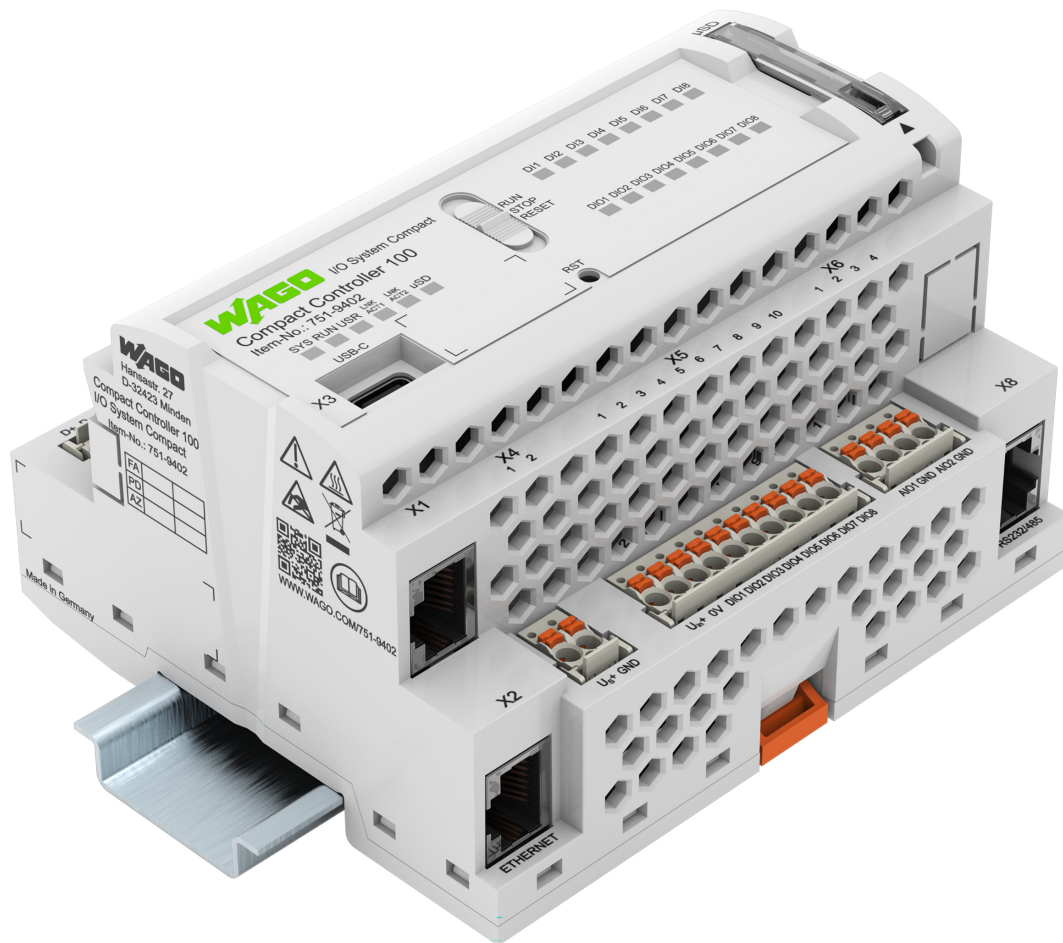


WAGO I/O System Compact

Compact Controller 100; 8DI 8DIO 2AI 2AIO 2NI/PT 2x RS485; 2x ETHERNET, SD

751-9402



© 2024 WAGO GmbH & Co. KG
All rights reserved.

WAGO GmbH & Co. KG

Hansastraße 27

D - 32423 Minden

Phone: +49 571/887 – 0

E-Mail: ✉ info@wago.comInternet: 🌐 www.wago.com**Technical Support**

Phone: +49 571/887 – 44555

E-Mail: ✉ support@wago.comInternet: 🌐 www.wago.com/support

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 documentation are generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1 Provisions	8
1.1 Scope of Applicability	8
1.2 Intended Use	8
1.3 Typographical Conventions	9
1.4 Legal Information	11
2 Safety	12
2.1 General Safety Regulations	12
2.2 Electrical Safety	12
2.3 Mechanical Safety	13
2.4 Thermal Safety	13
2.5 Indirect Safety	13
3 Overview	14
4 Properties	15
4.1 View	15
4.2 Product Identification	16
4.2.1 Marking	16
4.2.2 Label	17
4.2.3 Update Matrix	17
4.3 Connections	17
4.3.1 ETHERNET Interfaces - X1, X2	17
4.3.2 USB-C Service Interface - X3	18
4.3.3 Supply Voltage - X4	18
4.3.4 Digital Inputs - X12	18
4.3.5 Digital Inputs/Outputs - X5	19
4.3.6 Analog Inputs - X14	19
4.3.7 Analog Inputs/Outputs - X6	20
4.3.8 RTD Inputs - X13	21
4.3.9 Communication Interfaces	21
4.3.9.1 Communication Interface - X8	22
4.3.9.2 Communication Interface - X11	22
4.3.9.3 Bus Termination and Biasing	22
4.4 Memory Card Slot	23
4.5 Indicators	23
4.5.1 System LEDs	23
4.5.2 LNK ACT LEDs	23
4.5.3 Memory Card Slot LED	24
4.5.4 LEDs Status DI/DIO	24
4.6 Control Elements	24
4.6.1 Operating mode switch	24
4.6.2 Reset Button	24
4.7 DIN-Rail Contact	25
4.8 Circuit Diagram	25
5 Functions	26
5.1 Function Overview	26
5.2 Hardware Functions	27
5.2.1 Reset Functions	27

5.3	Network Functions.....	27
5.3.1	Interface Configuration	27
5.3.1.1	Operation in Switch Mode	28
5.3.1.2	Operation with Separate Network Interfaces.....	28
5.3.1.3	MAC ID and IP Address Assignment Examples.....	28
5.3.2	Network Security	29
5.3.2.1	Users and Passwords.....	29
5.3.2.2	Web Server Authentication	31
5.3.2.2.1	TLS Encryption	31
5.3.2.3	Root Certificates	32
5.3.3	Network Configuration.....	32
5.3.3.1	Hostname/Domain Name	32
5.3.3.2	Routing	32
5.3.4	Network Services.....	35
5.3.4.1	DHCP Client	35
5.3.5	Cloud Connectivity.....	35
5.4	Fieldbus Functions.....	37
5.4.1	BACnet	37
5.5	Memory Functions	37
5.5.1	Formatting.....	37
5.5.2	Data Backup	37
5.5.2.1	Backup Function	38
5.5.2.2	Restore Function	39
5.5.3	Inserting a Memory Card during Operation	41
5.5.4	Removing the Memory Card during Operation.....	41
5.5.5	Setting the Home Directory for the Runtime System.....	42
5.5.6	Load Boot Project.....	42
5.6	WAGO Device Access.....	43
5.7	Process Image	43
5.7.1	Analog Inputs AI1, AI2.....	43
5.7.1.1	AI 0 ... 10 V.....	44
5.7.1.2	AI -10 ... +10 V	44
5.7.1.3	AI 0 ... 20 mA	44
5.7.1.4	AI 4 ... 20 mA	44
5.7.1.5	AI 3.6 ... 21 mA.....	45
5.7.2	Analog Inputs/Outputs AIO1, AIO2.....	45
5.7.2.1	AI 0 ... 10 V, -10 ... +10 V, 0 ... 20 mA, 4 ... 20 mA, 3.6 ... 21 mA.....	45
5.7.2.2	AO 0 ... 10 V	45
5.7.2.3	AO -10 ... +10 V	46
5.7.2.4	AO -12 ... +12 V	46
5.7.2.5	AO 0 ... 20 mA.....	46
5.7.2.6	AO 0 ... 22 mA.....	46
5.7.2.7	AO 4 ... 20 mA.....	46
5.7.3	Temperature Inputs PT1+/PT1-, PT2+/PT2-	47
5.7.3.1	Pt100, Pt200, Pt500, Pt1000.....	47
5.7.3.2	Ni100, Ni1000 (TK6180), Ni1000 (TK5000).....	47
5.7.3.3	Ni120.....	48
5.7.3.4	Potentiometer 0 ... 1.2 kOhm.....	48
5.7.3.5	Potentiometer 0 ... 5 kOhm.....	48
5.7.4	Digital Inputs DI	49
5.7.5	Digital Inputs/Outputs DIO.....	49
5.7.5.1	DI 0/24 V	49
5.7.5.2	DO 0/24V.....	49
6	Planning.....	51
6.1	Structure Guidelines	51
6.1.1	Safety Measures at the Installation Location.....	51
6.1.2	Mounting Position and Distances	51

6.1.3	DIN-Rail Characteristics	53
6.1.4	EMC Installation	53
6.1.5	Grounding	54
6.1.6	Data Security	54
6.1.7	Buffering	55
6.2	CODESYS V3 Compatibility	55
7	Transport and Storage.....	56
8	Installation and Removal.....	57
8.1	Mounting on the DIN-Rail.....	57
8.2	Removal from the DIN-Rail	57
8.3	Connectors	58
8.3.1	Delivery Condition.....	58
8.3.2	WAGO Pluggable Connectors	58
8.3.2.1	Pulling the Female Connector	58
8.3.2.1.1	Pulling with the Unlocking Tool	58
8.3.2.1.2	Pulling with Other Tools.....	59
8.3.2.2	Plugging the Female Connector	59
9	Connection	61
9.1	Connecting the Supply Voltage	61
10	Commissioning	62
10.1	Switching On.....	62
10.2	Setting an IP address	62
10.2.1	IP Connection via USB.....	63
10.2.2	Changing an IP Address in "WAGO Ethernet Settings"	63
10.2.3	Temporarily Setting a Fixed IP Address	64
10.2.4	Setting the IP Address via the WBM	64
10.2.5	Assigning an IP Address Using DHCP	65
10.3	Testing the Network Connection.....	65
10.4	Changing Passwords	66
10.5	Switch Off/Restart.....	67
10.6	Configuration.....	67
10.6.1	Configuration in the Web-Based Management System (WBM)	67
10.6.1.1	User Administration of WBM	68
10.6.1.2	WBM Page Overview and Access Rights	69
10.6.1.3	General Page Information	71
10.6.2	Configuration with "WAGO Ethernet Settings".....	72
10.6.2.1	Identification Tab	74
10.6.2.2	Network Tab.....	75
10.6.2.3	PLC Tab	76
10.6.2.4	Status Tab	76
11	CODESYS V3 Runtime Environment	78
11.1	Basic Information.....	78
11.2	CODESYS V3 Priorities	78
11.3	Memory Spaces under CODESYS V3	79
11.3.1	Program and Data Memory	79
11.3.2	Function Block Limitation.....	79
11.3.3	Remanent Memory	79
12	Diagnostics.....	80
12.1	Diagnostics via Indicators.....	80
12.1.1	Diagnostics via LED Indicators: System.....	80

12.1.2	Diagnostics via Network LED Indicators	81
12.1.3	Diagnostics via LED Indicators: Memory Card Slot	81
12.1.4	Diagnostics via LED Indicators for Digital Inputs and Outputs	81
13	Service	83
13.1	Clearing Reset Functions.....	83
13.1.1	Warmstart Reset	83
13.1.2	Coldstart Reset	83
13.1.3	Software Reset.....	83
13.1.4	Controller Reset	83
13.2	Inserting and Removing a Memory Card	84
13.2.1	Inserting a Memory Card	84
13.2.2	Removing a Memory Card.....	84
13.3	Update Root Certificates	85
13.4	Firmware Updates.....	85
13.4.1	Using WAGOupload to Update/Downgrade Firmware	86
13.4.2	Using a Memory Card and WBM to Update/Downgrade Firmware	86
14	Decommissioning.....	87
14.1	Disposal and Recycling.....	87
15	Appendix	88
15.1	WBM Pages	88
15.1.1	"Information" Tab.....	88
15.1.1.1	"Device Status" Page	88
15.1.1.2	"Vendor Information" Page.....	89
15.1.1.3	"PLC Runtime Information" Page	89
15.1.1.4	"WAGO Software License Agreement" Page	89
15.1.1.5	"Open Source Licenses" Page	89
15.1.1.6	"WBM Third Party License Information" Page	89
15.1.1.7	"Trademarks Information" Page.....	89
15.1.1.8	"WBM Version" Page	89
15.1.2	"Configuration" Tab.....	90
15.1.2.1	"PLC Runtime Configuration" Page	90
15.1.2.2	"TCP/IP Configuration" Page	91
15.1.2.3	"Ethernet Configuration" Page.....	92
15.1.2.4	"Configuration of Host and Domain Name" Page	94
15.1.2.5	"Routing" Page	94
15.1.2.6	"Clock Settings" Page	97
15.1.2.7	"Create bootable Image" Page	97
15.1.2.8	"Firmware Backup" Page	98
15.1.2.9	"Firmware Restore" Page	99
15.1.2.10	"Active System" Page	101
15.1.2.11	"Mass Storage" Page	101
15.1.2.12	"Software Uploads" Page	102
15.1.2.13	WBM "Configuration of Network Services" Page.....	102
15.1.2.14	"Configuration of NTP Client" Page	104
15.1.2.15	"PLC Runtime Services" Page	104
15.1.2.16	"SSH Server Settings" Page	105
15.1.2.17	"Status overview" Page	105
15.1.2.18	"Configuration of Connection <n>" Page.....	106
15.1.2.19	"Configuration of general SNMP parameters" Page.....	109
15.1.2.20	"Configuration of SNMP v1/v2c Parameters" Page.....	110
15.1.2.21	"Configuration of SNMP v3 Parameters" Page	110
15.1.2.22	Docker® Settings Page.....	111
15.1.2.23	"WBM User Configuration" Page	112
15.1.3	"Fieldbus" Tab.....	113
15.1.3.1	"OPC UA Configuration" Page.....	113

15.1.3.2	"BACnet Status" Page	114
15.1.3.3	"BACnet Data Link" Page	115
15.1.3.4	"BACnet Configuration" Page	116
15.1.3.5	"BACnet Storage Location" Page	118
15.1.3.6	"BACnet Info" Page	119
15.1.4	"Security" Tab	120
15.1.4.1	"OpenVPN / IPsec" Page	120
15.1.4.2	"General Firewall Configuration" Page	121
15.1.4.3	"Interface Configuration" Page	121
15.1.4.4	"Configuration of MAC address filter" Page	122
15.1.4.5	"Configuration of User Filter" Page	123
15.1.4.6	"Certificates" Page	124
15.1.4.7	"Boot Mode Configuration" Page	125
15.1.4.8	"Security Settings" Page	125
15.1.4.9	"Advanced Intrusion Detection Environment (AIDE)" Page	126
15.1.4.10	"WAGO Device Access" Page	127
15.1.5	"Diagnostic" Tab	127
15.1.5.1	"Log Message Viewer" Page	127
15.1.5.2	"Download" Page	128
15.1.5.3	"Network Capture" Page	128
15.2	Protected Rights	129
15.3	Technical Data, Approvals, Guidelines and Standards	130
15.3.1	Data Sheet 751-9401	131

1 Provisions

1.1 Scope of Applicability

This document applies to:

751-9402(Compact Controller 100) (Compact Controller 100; 8DI 8DIO 2AI 2AIO 2RTD 2RS 2ETH; SD).

Version Firmware	04.06.xx(28)
Detailed Product Page	www.wago.com/751-9402

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.

1.2 Intended Use

Controllers of WAGO's 751 Series I/O System Compact receive digital and analog signals from sensors and transmit them to the actuators or higher-level control systems. The signals can also be (pre-)processed with the controllers.

The product is an open type device and is designed for installation in an additional enclosure. In order to use it, it is connect to take protective measures suitable for the specific application.

- This product is intended for installation in automation technology systems.
- The product is designed for use in dry indoor rooms.
- Operation of the product is permitted in the industrial sector and in residential and commercial domains, including small businesses.
- 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 in particular 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
- Implementation of a Known Misuse
- 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 provisions of the latest WAGO General Terms and Conditions of Deliveries and Services (GTC) apply as well as the Software License Terms for Standard Software (SW-License) applicable to software products und software embedded in WAGO hardware products, both available at: www.wago.com.

In particular, the warranty is void when:

- The product is improperly used.
- The defect is based on (customer-)specific specifications (hardware and software configurations).
- Modifications of the hardware or software by the user or third parties were made that are not described in this documentation and are at least responsible for the occurrence of the defect.

Individual agreements always take precedence.

Obligations of the installer/operator

Installers and operators bear responsibility for the safety of an installation or a system assembled with the product.

The installer/operator is responsible for the proper installation and the safety of the system. It must comply with the laws, standards, guidelines, local regulations, the state and the rules of technology applicable at the time of installation and must observe the guidelines and instructions described in the operating instructions. The installation requirements of the approvals must also be met.

In the event of non-compliance, operation of product within the scope of the approval is not permitted.

1.3 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 Markups

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

Links

	Link to a topic in a document
---	-------------------------------

	Link to a separate document
	Link to a website
	Link to an email address
Glossary	Link to a glossary entry

Sequence of Action

- ✓ 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.

Warning Messages

DANGER

Type and source of hazard

Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.

- Action step to reduce risk

WARNING

Type and source of hazard

Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

- Action step to reduce risk

CAUTION

Type and source of hazard

Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

- Action step to reduce risk

! NOTICE**Type and source of malfunction (property damage only)**

Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.

- Action step to reduce risk

Information Notices**i Note****Information**

Indicates information, clarifications, recommendations, referrals, etc.

1.4 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 "TM" symbols are omitted hereinafter. The trademarks are listed in the Appendix:  **Protected Rights** [▶ 129](#).

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 product contains open-source software. The requisite license information is saved in the product. This information is also available under www.wago.com.

2 Safety



This section presents hazards that could occur if the product is used. Builders and operators must take all hazards into account when analyzing the risk of their installed systems. Measures to reduce the risk of hazards that are foreseeable from the manufacturer's point of view (i.e., without knowledge of the specific system built) are explained in the respective sections of this documentation (e.g., in "Planning").

Builders and operators must implement explained risk reduction measures and also take their own measures depending on the residual risk.

2.1 General Safety Regulations

- 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.
- Set up permissions management for authorized persons.
 - Physical access may only be made by authorized persons.
 - Digital access may only be made by authorized persons.
- Comply with the laws, standards, guidelines, local regulations and accepted technology standards and practices applicable at the time of installation.

2.2 Electrical Safety

- Hazardous electrical voltage can cause electric shock or burns! Always disconnect all power supplies from the product before mounting, installing, troubleshooting or performing maintenance.
- Make sure the product does not carry any voltage before starting work.

Power Supply

- For non-hazardous live voltages, use SELV/PELV power supplies in accordance with EN/UL/IEC 61010-1.
- Provide a suitable disconnect mechanism and overcurrent protection on the system side. The disconnect mechanism must be located near the product where it can be operated and be clearly associated with the product. The **OFF** position of the disconnect mechanism must be clearly marked.

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.
- Establish sufficient grounding. Make sure there is a flawless electrical connection between the DIN-rail and frame / additional enclosure.

Cables

- To minimize interference (e.g., by electromagnetic interference), maintain a spatial separation between control, signal and data lines and the power supply lines.
- Always design the connection cables for the maximum anticipated current load.

- High currents and the inherent heat generated by the product can cause additional heat generation at the clamping point. Plan for a correspondingly higher temperature range for the connecting cables, or reduce inherent heat by selecting larger conductor cross-sections.
- Only one conductor may be connected to each connection point (e.g., CAGE CLAMP® connection).

Protection

- When working on the system (e.g., during maintenance), protect the facility part in question from accidental or unauthorized restart.

2.3 Mechanical Safety

- 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.
- Do not open the product housing.

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.
- Cooling of the product must not be impaired. Ensure air can flow freely and that the minimum clearances from adjacent products/areas are maintained.
- The temperature inside the additional enclosure must not exceed the ambient 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.
- Do not use any contact spray for cleaning.
- The product is not resistant to materials with seeping and insulating properties, such as aerosols, silicones or triglycerides (found in some hand creams). If these substances occur in the environment of the product, install the product in an additional housing that is resistant to these substances as well.
- Only permit skilled personnel approved by WAGO to perform repair work.
- Replace any defective or damaged devices.
- Observe possible different technical specifications for mounting that does not correspond to the nominal mounting position.
- Only use accessories authorized by WAGO.

3 Overview

The controller is an automation device that can perform PLC control tasks. The controller is suitable for mounting on a DIN-rail and characterized by various interfaces.

The controller can be used for applications in mechanical and systems engineering, in the processing industry and in building technology.

The controller's features include integrated digital and analog inputs and outputs and a serial onboard interface per EIA-485/RS-485.

4 Properties

4.1 View

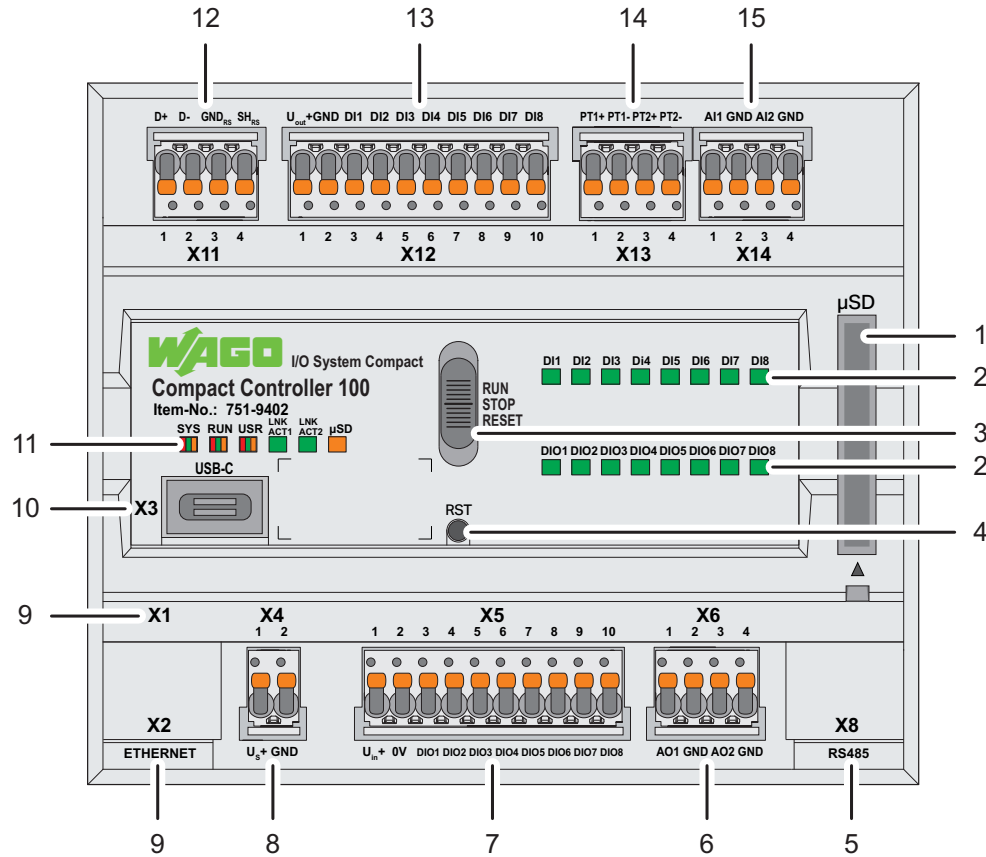


Figure 1: Ansicht

1	Memory Card Slot [23]
2	LEDs Status DI/DIO [24]
3	Operating mode switch [24]
4	Reset Button [24]
5	Communication Interface X8 Communication Interfaces [21]
6	Analog Inputs/Outputs - X6 [20]
7	Digital Inputs/Outputs - X5 [19]
8	Supply Voltage - X4 [18]
9	ETHERNET Interfaces - X1, X2 [17]
10	USB-C Service Interface - X3 [18]
11	System LEDs [23] LNK ACT LEDs [23] Memory Card Slot LED [24]
12	Communication Interface X11 Communication Interfaces [21]
13	Digital Inputs - X12 [18]
14	RTD Inputs - X13 [21]
15	Analog Inputs - X14 [19]

4.2 Product Identification

4.2.1 Marking

The marking is located on the left side of the product.

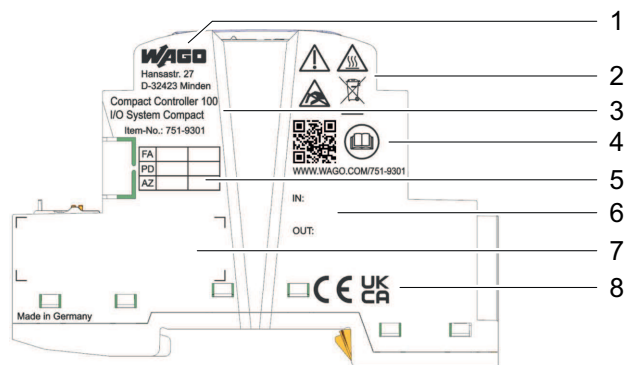


Figure 2: Marking (Example)

Table 1: Marking

1	Company logo and address	
2	Symbols for warning notices	
		Note: Observe the product documentation! Applicable information and documents concerning the product exist which must be observed.
		Warning: Do not touch hot surfaces! The housing surface can become hot during operation. If the product has been used at high ambient temperatures, let it cool down before touching it.
		Note: Avoid electrostatic discharge! The products are equipped with electronic components that may be destroyed by electrostatic discharge when touched. Observe the safety precautions per DIN EN 61340-5-1/-3 to prevent electrostatic discharge.
		Note: Electrical and electronic equipment must not be disposed of with household waste! Electrical and electronic equipment contains materials and substances that can be harmful to the environment and health. Electrical and electronic equipment must be disposed of properly after use. More information about this topic: Disposal and Recycling [► 87].
3		Observe the product documentation! Applicable information and documents concerning the product exist which must be observed. It can be found on the product detail page.
4	QR code with link to website	
5	Update matrix	Update Matrix [► 17]
6	Technical Specifications	Technical Data, Approvals, Guidelines and Standards [► 130]
7	Label	Label [► 17]
8	Field for guidelines, approvals and standards	Technical Data, Approvals, Guidelines and Standards [► 130]

4.2.2 Label

The label is located on the left side of the product.

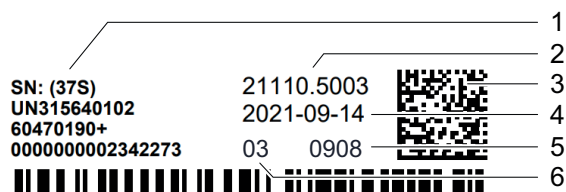


Figure 3: Label (Example)

Table 2: Etikett

1	Product identifier (UII)	
2	Control number	
3	Product identifier (UII) in the form of a Data Matrix code	
4	Date of manufacture (year-month-day)	
5	Production plant identifier	
6	Hardware revision number	

4.2.3 Update Matrix

In the event of a factory update, the updated production data is documented in the update matrix. The initial manufacturing information on the product housing remains unchanged.

Table 3: Update Matrix

FA	XXXXXXXXXX	Production order number, 10-digit
PD	WWYY	WW: production week YY: production year
AZ	FWHWFL	FW: firmware index HW: hardware index FL: firmware loader index

4.3 Connections

4.3.1 ETHERNET Interfaces - X1, X2

The ETHERNET ports are for connecting to a LAN or the Internet for communication with the controller. A crossover cable or category 5e patch cable can be used.

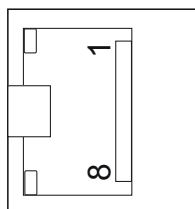


Figure 4: ETHERNET Interface Pin Assignment

Table 4: ETHERNET Interface Pin Assignment

Contact	Signal	Description
1	TD+	Transmit data +
2	TD-	Transmit data -
3	RD+	Receive data +

Contact	Signal	Description
4	NC	Not assigned
5	NC	Not assigned
6	RD–	Receive data –
7	NC	Not assigned
8	NC	Not assigned
Housing	Shield	Shield

4.3.2 USB-C Service Interface - X3

The USB service port is designed as a type C socket.

The service interface is used for communication with WAGO Ethernet Settings.

You can establish an IP connection via this interface for commissioning and service purposes.

4.3.3 Supply Voltage - X4

The connection is made via a 2-pole picoMAX® Pluggable Connector with Push-in CAGE CLAMP®S technology.

Table 5: Pin Assignment Supply Voltage

Contact	Signal	Description
1	U _S +	Supply voltage
2	GND	Ground

4.3.4 Digital Inputs - X12

The controller has 8 digital input channels (24 VDC, type 3).

The input channels receive binary control signals from digital field devices (e.g., sensors, encoders, switches or proximity sensors).

The connection is made via a 10-pole picoMAX® Pluggable Connector with Push-in CAGE CLAMP®S technology.

The sensors are connected according to the following table.

Table 6: Digital Input Pin Assignments

Contact	Signal	Description
1	U _{out} +	Supply voltage output (DI1 ... DI8)
2	GND	Ground
3	DI1	Digital input 1
4	DI2	Digital input 2
5	DI3	Digital input 3
6	DI4	Digital input 4
7	DI5	Digital input 5
8	DI6	Digital input 6
9	DI7	Digital input 7
10	DI8	Digital input 8

The inputs provide high-side switching. If the 24 V potential for the system power (X12, U_{out+}) is switched to an input connection, the signal status of the corresponding input channel is set to "high."

A green status LED for each channel indicates the signal status.

The meaning of the LED indicator is described in the section [🔗 Diagnostics via LED Indicators for Digital Inputs and Outputs \[p. 81\]](#).

4.3.5 Digital Inputs/Outputs - X5

The controller has 8 switchable digital input/output channels (DI: 24 VDC, type 3 / DO: 24 VDC, 0.5 A).

Input channels receive binary control signals from sensors, switches or proximity sensors in the field.

The output channels output binary control signals from the automation device to the connected actuators, e.g., magnetic valves, contactors, relays or other electrical loads.

Configuration is performed using CODESYS or the "WAGO Device Manager" tool.

The sensors and actuators are connected according to the following table.

The connection is made via a 10-pole picoMAX® Pluggable Connector with Push-in CAGE CLAMP®S technology.

Table 7: Digital Input/Output Pin Assignments

Contact	Signal	Description
1	U_{in+}	Supply voltage input (DIO1 ... DIO8)
2	0 V	Ground
3	DIO1	Digital input/output 1
4	DIO2	Digital input/output 2
5	DIO3	Digital input/output 3
6	DIO4	Digital input/output 4
7	DIO5	Digital input/output 5
8	DIO6	Digital input/output 6
9	DIO7	Digital input/output 7
10	DIO8	Digital input/output 8

The inputs provide high-side switching. If the 24 V potential for field power (X5, U_{in+}) is switched to an input connection, the signal status for the corresponding input channel is set to "high."

The outputs provide high-side switching. If the signal status of an output channel is "high," the 24 V potential for the field power supply is switched to the corresponding output connection.

The specifications of the connections corresponding to EN 61010-2-201: DC circuit, general use

A green status LED for each channel indicates the signal status.

The meaning of the LED indicator is described in the section [🔗 Diagnostics via LED Indicators for Digital Inputs and Outputs \[p. 81\]](#).

4.3.6 Analog Inputs - X14

The controller has 2 analog input channels that can be configured channel by channel.

The following measurement ranges can be configured:

- 0 ... 10 V, default setting
- -10 ... +10 V
- 0 ... 20 mA
- 4 ... 20 mA
- 3.6 ... 21 mA

Configuration is performed using CODESYS or the "WAGO Device Manager" tool.

The sensors are connected according to the following table.

The connection is made via a 4-pole picoMAX® Pluggable Connector with Push-in CAGE CLAMP®S technology.

Table 8: Analog Input Pin Assignments

Contact	Signal	Description
1	AI1	Analog input 1
2	GND	Ground
3	AI2	Analog input 2
4	GND	Ground

The internal power supply powers the module.

The ground connections for both channels are at a common 0 V ground potential.

4.3.7 Analog Inputs/Outputs - X6

The controller has 2 configurable analog input/output channels that can be switched channel by channel.

The following measurement ranges can be configured:

- Inputs
 - 0 ... 10 V, default setting
 - -10 ... +10 V
 - 0 ... 20 mA
 - 4 ... 20 mA
 - 3.6 ... 21 mA
- Outputs
 - 0 ... 10 V
 - -10 ... +10 V
 - -12 ... +12 V
 - 0 ... 20 mA
 - 0 ... 22 mA
 - 4 ... 20 mA

Configuration is performed using CODESYS or the "WAGO Device Manager" tool.

The sensors and actuators are connected according to the following table.

The connection is made via a 4-pole picoMAX® Pluggable Connector with Push-in CAGE CLAMP®S technology.

Table 9: Analog Inputs/Outputs Pin Assignments

Contact	Signal	Description
1	AIO1	Analog input/output 1
2	GND	Ground
3	AIO2	Analog input/output 2
4	GND	Ground

The internal power supply powers the module.

The ground connections for both channels are at a common 0 V ground potential.

4.3.8 RTD Inputs - X13

The controller has 2 RTD input channels that can be configured channel by channel.

2-wire resistance sensors can be connected directly.

The following measurement ranges can be configured:

- Pt100 (–200 ... +850 °C)
- Pt200 (–200 ... +850 °C)
- Pt500 (–200 ... +850 °C)
- Pt1000 (–200 ... +850 °C), default setting
- Ni100 (–60 ... +250 °C)
- Ni120 (–80 ... +260 °C)
- Ni1000 (TK6180) (–60 ... +250 °C)
- Ni1000 (TK5000) (–60 ... +250 °C)
- Potentiometer 0 ... 1.2 kOhm
- Potentiometer 0 ... 5 kOhm

Configuration is performed using CODESYS or the "WAGO Device Manager" tool.

The sensors are connected according to the following table.

The connection is made via a 4-pole picoMAX® Pluggable Connector with Push-in CAGE CLAMP®S technology.

Table 10: Analog Temperature Sensor Pin Assignments

Contact	Signal	Description
1	PT1+	Analog temperature sensor 1
2	PT1–	
3	PT2+	Analog temperature sensor 2
4	PT2–	

The controller linearizes the measured resistance values and converts them into a numerical value proportional to the temperature or resistance of the selected sensor.

4.3.9 Communication Interfaces

The communication interfaces integrated into the controller connect devices with an RS-485 interface.

The RS-485 interface guarantees a high level of interference immunity through differential transmission and electrically isolated signals.

The connection to the communication partner is made via connections D+, D–, GND_{RS} and SH_{RS}.

The shield connection is directly connected to the DIN-rail.

The interfaces operate in accordance with TIA/EIA 485.

The connected device can communicate directly via the controller used. The active communication channel works independently of the higher-level bus system in half-duplex mode at up to 250000 baud.

The X8 communication interface is designed as an RJ45 socket.

The X11 communication interface is designed as a picoMAX® Pluggable Connector.

4.3.9.1 Communication Interface - X8

Table 11: Communication Interface X8 Pin Assignment

Contact	Signal	Description
1	---	Not assigned
2	---	Not assigned
3	---	Not assigned
4	D–	Transmit/receive data –
5	D+	Transmit/receive data +
6	---	Not assigned
7	+5V_RS	Supply
8	GND_RS	Ground

4.3.9.2 Communication Interface - X11

The connection is made via a 4-pole picoMAX® Pluggable Connector with Push-in CAGE CLAMP®S technology.

Table 12: Communication Interface X11 Pin Assignment

Contact	Signal	Description
1	D+	Transmit/receive data +
2	D–	Transmit/receive data –
3	GND _{RS}	Ground
4	SH _{RS}	Shield

4.3.9.3 Bus Termination and Biasing

To minimize reflections at the end of the line, the RS-485 line must be terminated at the end with a 120 Ω line terminator. The RS-485 line is already terminated in the Compact Controller 100 with a bus termination resistor (121 Ω). A bias network (pull-up and pull-down resistor) is also integrated in the Compact Controller 100 to keep the bus lines at a specified level when no other subscriber is active.

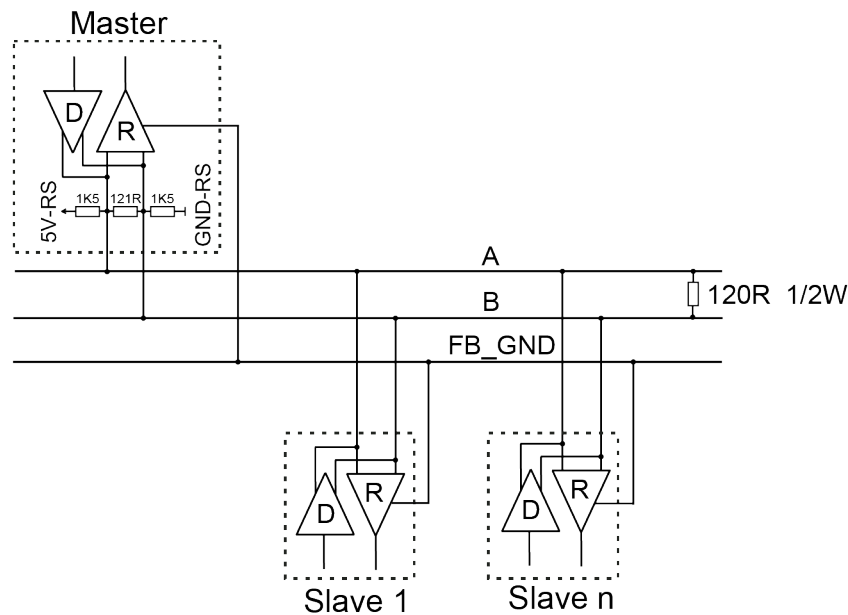


Figure 5: RS-485 Bus Termination

4.4 Memory Card Slot

The slot for the memory card is located on the front of the housing. A push-push mechanism is used to lock the memory card into the housing. The memory card is protected by a cover flap. The cover flap is sealable.

4.5 Indicators

4.5.1 System LEDs

Table 13: System/Fieldbus LED Indicators

Designation	Color	Description
SYS	Red/green/orange/off	System status
RUN	Red/Green/Orange/Off	PLC program status
USR	Red/green/orange/off	User LED; programmable using function blocks from the WAGO libraries to control the LEDs

The meanings of the indicated states are described in [🔗 Diagnostics via LED Indicators: System \[► 80\]](#).

4.5.2 LNK ACT LEDs

Table 14: LNK/ACT LED Indicators

Designation	Color	Description
LNK ACT 1 LNK ACT 2	Green/off	ETHERNET Connection Status/Data Exchange

The meanings of the indicated states are described in [🔗 Diagnostics via Network LED Indicators \[► 81\]](#).

4.5.3 Memory Card Slot LED

Table 15: Memory Card Slot LED Indicator

Designation	Color	Description
μSD	Orange/off	Memory card status

The meanings of the indicated states are described in [🔗 Diagnostics via LED Indicators: Memory Card Slot \[► 81\]](#).

4.5.4 LEDs Status DI/DIO

Table 16: DI/DIO LED indicator

Designation	Color	Description
DI1 ... DI8 DIO1 ... DIO8	Green/off	Status of Digital Inputs and Outputs

The meanings of the indicated states are described in [🔗 Diagnostics via LED Indicators for Digital Inputs and Outputs \[► 81\]](#).

4.6 Control Elements

4.6.1 Operating mode switch

Table 17: Operating mode switch

Pos.	Actuation	Function
RUN	Latching	Normal operation CODESYS V3 applications are running
STOP	Latching	Stop All CODESYS V3 applications have stopped
RESET	Spring-return	Warmstart Reset or Coldstart Reset (depending on how long it is actuated)

Other functions can also be triggered with the reset button.

See also

- 🔗 Warmstart Reset [► 83]
- 🔗 Coldstart Reset [► 83]
- 🔗 Software Reset [► 83]
- 🔗 Controller Reset [► 83]

4.6.2 Reset Button

The reset button is installed within a recess to prevent accidental operation. The button can be pressed with suitable object (e.g., a pen).

See also

- 🔗 Temporarily Setting a Fixed IP Address [► 64]
- 🔗 Software Reset [► 83]

Controller Reset [► 83]

4.7 DIN-Rail Contact

The product transmits electromagnetic interference to the DIN-rail via DIN-rail contacts. The DIN-rail contacts are automatically connected when the product is snapped on to the DIN-rail.

4.8 Circuit Diagram

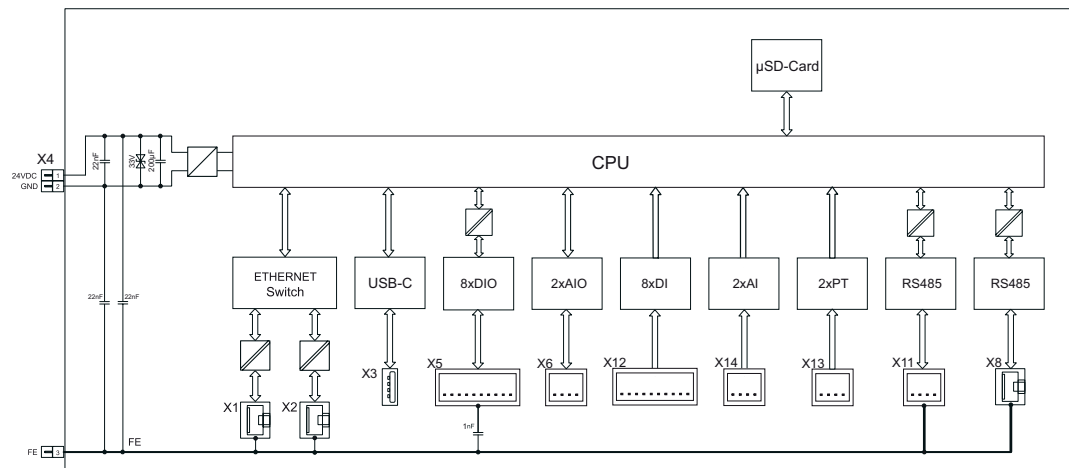


Figure 6: Circuit Diagram

5 Functions

5.1 Function Overview

Automation tasks can be executed in all IEC-61131-3-compatible languages with the CODESYS V3 programming system.

Implementation of task processing in the runtime system is optimized for Linux® with real-time extensions to provide maximal performance for automation tasks. Web visualization is also provided as visualization in addition to the development environment.

The controller provides 32 MB of program memory (flash), 128 MB of data memory (RAM) and 128 kB of remanent memory (retain and flag variables in an integrated NVRAM) for IEC 61131-3 programming in CODESYS applications.

The controller has a slot for a memory card. The memory card can be used to transfer device parameters, boot projects and other files from one controller to another. The memory card can be accessed via FTP as an additional drive.

Two ETHERNET ports and the integrated configurable switch allow wiring in all necessary configurations with a common network and common IP address for both ports, or with two separate networks with a separate IP address for each port.

The physical interfaces (ports) are assigned via logical bridges and can be configured via the WBM, for example.

Both interfaces support:

- 10BASE-T / 100BASE-TX
- Full/half duplex
- Auto-negotiation
- Auto-MDI(X) (automatic uplink and crossover switching)

The following fieldbus interfaces are implemented for exchange of process data:

- Modbus TCP Client/Server
- Modbus RTU Master/Slave (via RS-485)
- Gateway Modbus TCP to Modbus RTU
- EtherCAT Master
- EtherNet/IP Adapter
- EtherNet/IP Scanner

Die Feldbuskonfiguration ist mit CODESYS V3 möglich.

The Web-Based Management (WBM) is also available for configuration. This system includes various dynamic HTML pages from which, among other things, information about configuration and the status of the controller can be called up. The WBM is already stored in the device and is presented and operated using an Web browser. It is also possible to store individual HTML pages in the implemented file system or to launch programs directly.

In the controller's initial state, the installed firmware is based on Linux® with special real-time extensions of the RT-Preempt patch. In addition, the following application programs are also installed on the controller, along with a number of different auxiliary programs:

- An SNMP server/client
- An FTP server
- An FTPS server (explicit connections only)

- An SSH server/client
- A Webserver
- An NTP client
- A BootP client
- A DHCP client
- A DHCP server
- A DNS server
- The CODESYS V3 runtime environment

The following inputs and outputs are implemented for exchange of process signals:

- 8 digital inputs
- 8 digital in-/outputs, switchable
- 2 analog inputs, configurable
- 2 analog in-/outputs, switchable, configurable
- 2 RTD inputs, configurable

Based on IEC-61131-3 programming, data processing takes place on site in the controller. The logical process results can be output directly to the actuators or transmitted via a connected fieldbus to the higher level controller.

5.2 Hardware Functions

5.2.1 Reset Functions

You can initiate various reset functions using the operating mode switch and the Reset button (RST).

See also

- 📖 Warmstart Reset [► 83]
- 📖 Coldstart Reset [► 83]
- 📖 Software Reset [► 83]
- 📖 Controller Reset [► 83]

5.3 Network Functions

5.3.1 Interface Configuration

The X1 and X2 network interfaces of the controller are connected with an integrated configurable 3-port switch, in which the third port is connected to the CPU.

The two interfaces and configurable switch enable wiring for:

- In a common network with a common MAC address and an IP address for both interfaces.
- In two separate networks with a common MAC address and its own IP address for each interface.

The physical interfaces (ports) are assigned via logical bridges and can be e.g., configured via the WBM.

Bridge	Port	
	X1	X2
1		
2		

Figure 7: Example of Interface Assignment

For interface X1, a fixed IP address can be set temporarily ("Fix IP Address" mode). The setting is carried out with the Reset button (see Section "Commissioning" > ... > "Temporarily Setting a Fixed IP Address").

Setting a fixed IP address has no effect on the mode previously set.

See also

 Temporarily Setting a Fixed IP Address [\[► 64\]](#)

5.3.1.1 Operation in Switch Mode

For operation in Switch mode, the TCP/IP settings such as the IP address or subnet mask apply to both X1 and X2.

When switching to Switch mode, the X1 settings are applied as a new common configuration for X1 and X2.

The device is then no longer accessible via the IP address previously set for X2. This must be taken into account for applications that use X2 for communication.

5.3.1.2 Operation with Separate Network Interfaces

When operating with separate network interfaces, both ETHERNET interfaces can be configured and used separately.

When switching to operating with separate interfaces, interface X2 is initialized with the setting values last valid for it. The connections on the X1 interface persist.

When operating with separate interfaces and fixed IP address, the device can still be accessed via the interface X2 via the regular IP address.

5.3.1.3 MAC ID and IP Address Assignment Examples

One common network with one common IP address for both ports

Bridge	Port	
	X1	X2
1		
2		

Figure 8: 1 bridge with 2 ports

Table 18: Assignment of MAC IDs and IP addresses for 1 bridge with 2 ports

Bridge	MAC ID	IP Addr.	Port	MAC ID	Port	MAC ID
1	01	1	X1	02	X2	03

Two separate networks where each port has its own IP address



Figure 9: 2 bridges with 1/1 ports

Table 19: MAC ID and IP address assignment for 2 bridges with 1/1 ports

Bridge	MAC ID	IP Addr.	Port	MAC ID	Port	MAC ID
1	01	1	X1	01		
2	02	2			X2	02

5.3.2 Network Security

5.3.2.1 Users and Passwords

Users and Passwords

There are several user groups that can be used for different services.

A default password is set for all users. We strongly recommend changing these passwords on startup!

Note

Change passwords!

The default passwords are documented in these instructions and therefore do not offer adequate protection.

- Change the passwords to meet your particular needs.

Services and Users

All password-protected services and their associated users are listed in the following table.

Table 20: Services and Users

	User			
Service	Linux®			SNMP
	root	admin	user	
Web-Based Management (WBM)	X	X	X	
Linux® console	X	X	X	
Console-Based Management (CBM)	X			
CODESYS		X		

Service	User			
	Linux®			SNMP
	root	admin	user	
FTP	X	X	X	
FTPS	X	X	X	
SSH	X	X	X	
SNMP				X

Linux® User Group

The Linux® users group includes the actual users of the operating system that most services also use.

Table 21: Linux® user

User	Special Feature	Home Directory	Default password
root	Super user	/root	wago
admin	CODESYS user	/home/admin	wago
user	Normal user	/home/user	user

You can configure passwords for these users via the WBM or a terminal connection.

Note

Change passwords!

The default passwords are documented in these instructions and therefore do not offer adequate protection.

- Change the passwords to meet your particular needs.

Note

Valid characters for passwords

Passwords may contain only the following characters:

lowercase letters (a ... z), uppercase letters (A ... Z), numbers (0 ... 9) and special characters (! " # \$ % & ' () * + , . / : ; < = > ? @ [] ^ _ ` { } | ~ -).

Note

Note password length!

For CODESYS, the password length must be greater than or equal to 1 character and less than 60 characters!

For the logged-in Linux® user, the password can be changed via the WBM "WBM User Configuration" page in the "Change Passwords" group.

Table 22: WBM "WBM User Configuration" Page – "Change Passwords" Group

Parameters	Explanation
Old Password	Enter the current password used for authentication.
New Password	Enter new password.
Confirm Password	Enter new password again to check.

SNMP User Group

The SNMP service manages its own users. When first delivered, no users are stored in the system.

5.3.2.2 Web Server Authentication

WBM pages can be accessed with either the HTTP or the HTTPS Web protocol. Using HTTPS is preferable, since it relies on the TLS protocol.

The TLS protocol ensures secure communication through encryption and authentication.

The default setting for the controller allows strong encryption but uses only simple authentication methods. Since authentication plays a central role for all secure communication channels, using secure authentication is strongly recommended. The security certificate stored on the controller is the basis for authentication. The default location for the security certificate is `/etc/lighttpd/https-cert.pem`.

As delivered, the controller uses a generic security certificate in x509 format. To enable secure authentication, you must replace the generic security certificate with a security certificate specific to the individual device.

5.3.2.2.1 TLS Encryption

When an HTTPS connection is established, the Web browser and Webserver negotiate what TLS version and what cryptographic method is used.

The permitted TLS versions and cryptographic methods can be set ("Standard"/"Strong").

With the "Standard" setting, TLS 1.0, TLS 1.1 and TLS 1.2 are allowed, as well as cryptographic methods that are no longer considered secure. Use is recommended only for backward compatibility with older systems.

With the "Strong" setting, the Webserver only allows TLS version 1.2 and strong algorithms. Older software and older operating systems may not support TLS 1.2 and the encryption algorithms.

Note

BSI TR-02102 Technical Guideline

The rules for the TLS settings are based on the TR-02102 Technical Guideline of the German Federal Office for Information Security.

The Guideline is available from: www.bsi.bund.de.

Note

BSI Guide on Migration to TLS 1.2 or TLS 1.3

The German Federal Office for Information Security guidelines on migration to TLS 1.2 or TLS 1.3 contain "compatibility matrices" that show what software is compatible with TLS 1.2 or TLS 1.3. The guide is available at: www.bsi.bund.de.

5.3.2.3 Root Certificates

For communication encrypted with TLS, root certificates are used to verify the authenticity of the communication partner.

A root certificate, which is signed by a certificate authority, serves to verify the validity of all certificates issued by this certificate authority.

The root certificates stored on the controller (root CA bundle) form the basis for authentication of services hosted on the Internet (e.g., email providers and cloud services).

The standard storage location for the root certificates is `/etc/ssl/certs/ca-certificates.crt`.

This file contains the certificates provided by Mozilla. A list of the included root certificates and their respective validity periods can be requested from the following address:

🔗 <https://hg.mozilla.org/releases/mozilla-release/raw-file/79f079284141/security/nss/lib/ckfw/builtins/certdata.txt>

The root certificates can be updated on the controller by updating the file `/etc/ssl/certs/ca-certificates.crt`.

See also

- 📄 Update Root Certificates [► 85]

5.3.3 Network Configuration

5.3.3.1 Hostname/Domain Name

Without a hostname configuration, the controller is assigned a default name which includes the last three values of the controller's MAC address, e.g., "PFx00-A1A2A3." This name is valid for as long as a hostname was not configured, or hostname was not supplied to the controller via DHCP. See 📖 [Configuration in the Web-Based Management System \(WBM\)](#) [► 67] for configuration.

When the hostname is set, a hostname supplied by a DHCP response is immediately active and displaces the configured or default hostname. If there are multiple network interfaces with DHCP, the last received hostname is valid. If only the configured name is to be valid, the network administrator must adjust the configuration of the active DHCP server so that no hostnames are transferred in the DHCP response.

The default hostname or the configured name is active again if the network interfaces are set to static IP addresses or if a hostname is not received via the DHCP response.

A similar mechanism is used for a domain name as for the hostname. The difference is that a default domain name is not set. As long as a domain name is not configured or supplied by DHCP, the domain name is empty.

5.3.3.2 Routing

As part of the TCP/IP configuration, the controller allows you to configure static routes, IP masquerading and port forwarding. Default gateways are configured via static routes, since default gateways are a special case of static routes.

A network station transmits to a gateway all network data packets for systems outside of its local network. This gateway is responsible for the appropriate routing of the data packets so that they reach the target system. To allow access to different target systems, it may be necessary to configure multiple gateways. This is configured by adding routing entries.

A routing entry consists of the following information:

- Destination address
- Destination mask
- Gateway address
- Gateway metric

On the basis of the target system configuration, consisting of the destination address and destination mask, a decision is made about which gateway a network data packet should be forwarded to. The target system can be specified through an individual IP address or an IP address range. For a network data packet to forward, the routing entry with the most specific destination address and destination mask entries is always selected. The default gateway corresponds to the least specific routing entry. All network data packets such that no specific routing entry exists for their destination address and destination mask are sent to this default gateway.

Default gateway:

If the value "default" is entered in the "Destination Address" field, a default gateway, also called a default route, is defined. The value "0.0.0.0" must then be set in the "Destination Mask" field.

Route:

If an IP address or IP address range is entered in the "Destination Address" field, then all network data packets that are directed to the network address or network address range are sent to the gateway address corresponding to the entry.

If the IP address of the gateway is outside the IP address space that the controller can reach, the associated route is not enabled.

A metric is assigned to each routing entry. If multiple routing entries are configured for the same destination address and destination mask, the metric specifies how the routing entries are prioritized. In this case, routing entries with a lower value for the metric are preferred over routing entries with a higher metric value.

The metric value of the configured routing entries can be specified for the controller. The default value for the metric is 20. Besides the manually configurable routes, default gateways can also be set via DHCP replies. All default gateways transferred via DHCP are assigned a permanent metric value of 10.

Metric example:

A controller obtains its IP configuration via a DHCP server and receives both the IP address and the network mask 192.168.1.10/24. Furthermore, a gateway with IP address 192.168.1.2 and metric value 20 is set up on the controller. Therefore, when no specific routing entry exists for the target address of network data packets, the controller sends them to gateway 192.168.1.2. Besides the IP address and network mask, the DHCP server is now instructed to allocate a default gateway of 192.168.1.1. The controller gives this default gateway a metric value of 10. Therefore, the default gateway received via DHCP is preferred over the manually configured gateway.

The routing entries are used to specify which gateways the network data packets are sent. If the controller is running in switched mode and only has one network interface, all network traffic passes through this network interface. If the controller is running in separated mode or contains a modem, it has more than one network interface. Therefore, it is possible for a

network data packet to arrive at the controller on one network interface and depart on a different network interface. This forwarding between different network interfaces must be explicitly enabled; it is disabled when the controller is delivered. To enable the forwarding, "Routing enabled entirely" must be enabled in the "General Routing Configuration" group. In this case, the controller can function as a router.

For forwarding network communication through a router, it is necessary to note that corresponding routing entries must be provided not only for the router, but also for the respective endpoints of the communication. The routing entries of the endpoints must ensure that the desired network data packets are sent via the router, both when the connection is established and with the replies.

Host route example:

A host route is a route to an individual host. In the following example, a route to a host with IP address 192.168.1.2 is to be specified. The route passes through a gateway that can be reached via address 10.0.1.3. To configure a host route to the destination host on a controller connected to the gateway, the following settings must be made:

Destination address:	192.168.1.2	IP address of the destination host
Destination mask:	255.255.255.255	Subnet mask of an individual host
Gateway address:	10.0.1.3	IP address of the gateway
Gateway metric:	20	Route priority

Network route example:

A network route is a route to a subnet, which can contain multiple hosts. In the following example, a route to a subnet should be specified with network address 192.168.1.0. The route passes through a gateway that can be reached via address 10.0.1.3. To configure a network route to the destination network on a controller connected to the gateway, the following settings must be made:

Destination address:	192.168.1.0	IP address of the destination host
Destination mask:	255.255.255.0	Subnet mask of an individual host
Gateway address:	10.0.1.3	IP address of the gateway
Gateway metric:	20	Route priority

Besides configuration of static routes, the controller also supports IP masquerading. This can be enabled for selected network interfaces of the controller. Network data packets that depart the controller through a network interface for which IP masquerading has been enabled are given the IP address of the network interface as their sender address. If network data packets are forwarded through the controller, the network behind the controller is encapsulated under a single address.

Furthermore, the controller permits configuration of port forwarding entries. For port forwarding, the destination address and, if relevant, destination port of a network data packet that arrived at the controller via a previously configured network interface are overwritten. This makes it possible to forward network data packets through the controller to other addresses and ports. Forwarding can be configured for the TCP or UDP protocols.

5.3.4 Network Services

5.3.4.1 DHCP Client

The controller can get network parameters from an external DHCP master via the DHCP Client service.

The following parameters can be obtained:

- IP Address
- Subnet Mask
- Router/Gateway
- Hostname
- Domain
- DNS Server
- NTP server

For the IP address, SubNet mask and router/gateway parameters, the entries are stored per ETHERNET port (X1, X2).

The Hostname and Domain parameters are stored according to the LIFO principle (Last In First Out). The settings from the last DHCP offer received are always used.

The DNS and NTP Server parameters are stored centrally for global use. All transmitted parameters are saved.

5.3.5 Cloud Connectivity

With the cloud connectivity functionality and an IEC library, the controller is available as a gateway for Internet-of-Things (IoT) applications. This means the controller can collect the data from all the connected devices, access the Internet via the built-in Ethernet interface or the mobile communications module and send the data to the cloud.

You can customize the cloud service to be used; Microsoft Azure and Amazon Web Services are available, among others.

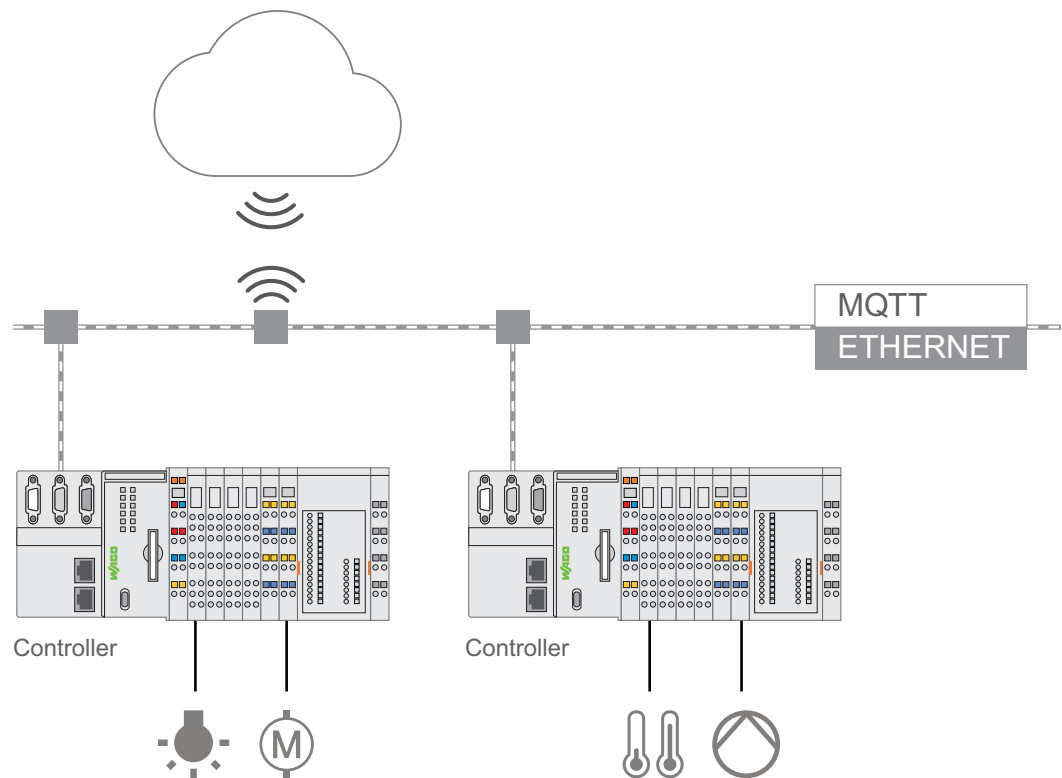


Figure 10: Connecting the Controllers to a Cloud Service (Example)

Data is transmitted from the controller to the cloud service as JSON files. The connection can be encrypted via TLS; see [TLS Encryption](#) [> 31].

You can find the settings that must be made in the controller to use the cloud connectivity functionality in the [Web-Based Management \(WBM\)](#) [> 67].

You can configure the communication parameters in the WBM, for example.

You can configure the data to be exchanged between the cloud and the controller from the IEC application with the corresponding CODESYS V3 library.

Note

Beachten Sie die zusätzlichen Dokumentationen!

Eine detaillierte Beschreibung des Softwarepaketes Cloud Connectivity mit einem Controller und Informationen zur SPS-Programmierung finden Sie im Anwendungshinweis A500920 im Downloadbereich unter www.wago.com.

Note

Observe the necessary data protection and security settings!

Before using the cloud connectivity functionality, please read the information on data protection and security in the corresponding manual in the download area at www.wago.com.

Table 23: Components of the Cloud Connectivity Software Package

Components	Description
CODESYS V3: WagoAppCloud WagoAppSparkplug	IEC libraries to create the PLC application; function blocks make it possible to exchange data between the PLC and cloud service. The data transmission variables are definable.

5.4 Fieldbus Functions

5.4.1 BACnet

BACnet is a license-based extension; licensing can be performed with add-on licensing.

A license key is required for productive use of BACnet without time restriction. Even without a license key, BACnet can be used to its full extent for a limited time. This trial period only includes the amount of time of actual use. Access without a license key is no longer possible after the trial period.

Note

Restriction of BACnet Communication

BACnet communication is only possible via port X1 and the ports assigned to bridge 1 (br0) in the network configuration.

For more information, see the BACnet Protocol Implementation Conformance Statement (PICS) at www.wago.com.

5.5 Memory Functions

The memory card is optional and serves as an additional memory area in addition to the internal memory or drive in the controller. The user program, user data, source code of the project or device settings can be saved to the memory card, and thus already existing project data and programs can be copied to one or more controllers.

If the memory card is inserted, this is incorporated under /media/sd in the directory structure of the file system inside the controller. This means that the memory card can be addressed like a removable medium on a PC.

5.5.1 Formatting

Note

Note the pre-formatting of the memory card!

Please note that memory cards ≤ 2 GB are often formatted with the "FAT16" file system type and can generate up to 512 entries in the root directory. For over 512 entries create these in a subdirectory or format the memory card with "FAT32" or "NTFS."

5.5.2 Data Backup

The controller has a backup function and a restore function.

In the WBM, the required settings can be made in the "Configuration" tab on the "Package Server" > "Firmware Back-up" or "Firmware Restore" pages and the functions can be executed.

The storage medium (internal memory or memory card) and, if applicable, the storage location in the network can be set.

The data to be backed up and restored can also be selected:

- The CODESYS project ("PLC Runtime Project," boot project, CODESYS settings)
- The device settings ("Settings")
- The controller operating system and the root file system ("System")
- All previous ("All"), only visible if not saved in the network

Note

Note the firmware version!

Restoring the operating system ("System" selection) is only permitted and possible if the firmware versions are the same at the time of backup and restore.

If necessary, refrain from restoring the operating system or adjust the firmware version to the firmware version at the time of the backup beforehand.

5.5.2.1 Backup Function

The backup function enables the data of the internal memory and device settings to be saved on the memory card during operation.

The network or the inserted memory card can be selected as the target medium.

The files of the internal drive are stored on the target medium in the media/sd/copy directory and in the corresponding subdirectories. Information that does not exist on the controller in the form of files is saved in XML format in the media/sd/settings directory.

If the memory card is selected as the target medium, the memory card slot LED flashes yellow/orange during the save operation.

The device settings and files of the internal drive are then saved on the target medium.

The controller has an automatic update function. If this function is enabled on a memory card before the data backup and a controller is booted from this memory card, this data is restored automatically on the internal memory of the controller.

Note

Only one package may be copied to the network!

If you have specified "Network" as the storage location, only one package may be selected for each storing operation.

Note

No backup of the memory card!

Backup from the memory card to the internal flash memory is not possible.

Note

Account for backup time

Generation of backup files can take several minutes. Stop the CODESYS program before you start the backup operation to help shorten the time required.

The backup function can be called up via the WBM "Firmware Backup" page in the "Configuration" tab, "Package Server" > "Firmware Backup" selection.

Table 24: WBM "Firmware Backup" Page – "Firmware Backup" Group

Parameters	Explanation	
Boot Device	Storage medium from which the device was booted	
Destination	Storage destination for backup	
	Memory Card	The data is written to the memory card. This selection only appears if a memory card is inserted and the device has not been booted from the memory card.
	USB stick	The data is written to the USB stick. This selection is only available for products with USB connection. This selection is only enabled if a USB stick is inserted and has not been booted from the USB stick.
	Network	The data is saved in the file system and then made available as a download on the PC.
PLC Runtime Project	Save PLC runtime project, boot project and CODESYS settings.	
	☐	PLC runtime project is not saved.
	☒	PLC runtime project is saved.
Settings	Save device settings.	
	☐	Device settings are not saved.
	☒	Device settings are saved.
System	Save device operating system and root file system.	
	☐	The device operating system and root file system are not saved.
	☒	The device operating system and root file system are saved.
Encryption	Save data encrypted.	
	☐	Data is saved unencrypted.
	☒	Data is saved in encrypted form.
Encryption passphrase	Encryption password The input field only appears if the Encryption checkbox is selected.	
Confirm passphrase	Encryption password for confirmation The input field is only displayed if the Encryption checkbox is selected.	

5.5.2.2 Restore Function

The restore function is used to load the data and device settings from the memory card to the internal memory during operation.

The network or, if it is inserted, the memory card can be selected as the source medium.

If the memory card is selected as the source medium, the memory card slot LED flashes yellow/orange during the charging operation.

When loading the data, the files are copied from the directory media/sd/copy/ of the source medium to the appropriate directories on the internal memory.

The device has an enabled and an disabled root partition. The system backup is stored on the disabled partition. Startup is then performed from the newly written partition. If the startup operation can be completed, the new partition is switched to enabled. Otherwise, booting is performed again from the old enabled partition during the next boot operation.

The boot project is loaded automatically and the settings automatically enabled after a restart. The "Home directory on memory card enabled" setting determines whether the boot project of the internal drive or the memory card is loaded. This setting can be called up on the WBM page "PLC Runtime Configuration" in the "Configuration" tab, selection "PLC Runtime".

i Note

File size must not exceed the size of the internal drive!

Note that the amount of data in the media/sd/copy/ directory must not exceed the total size of the internal drive.

i Note

Restoration only possible from internal memory!

If the product was booted from the memory card, the firmware cannot be restored.

i Note

Reset by restore

A reset is performed when the system or settings are restored by CODESYS!

i Note

Connection loss through restore!

If the restore changes the parameters of the ETHERNET connection, the WBM may then no longer be able to open a connection to the product.

Call up the WBM again with the correct IP address of the product in the address line.

i Note

Account for restore time

The restore operation takes about 2 ... 3 minutes.

After the restore operation, the controller is restarted and is then ready for use again.

The restore function can be called up via the WBM "Firmware Restore" page in the "Configuration" tab, "Package Server" > "Firmware Restore" selection.

Table 25: WBM "Firmware Restore" Page – "Firmware Restore" Group

Parameters	Explanation
Source	Data source for restoration

Parameters	Explanation	
	Memory Card	The data is read from the memory card. This selection is only enabled if a memory card is inserted and the device has not been booted from the memory card.
	USB stick	The data is read from the USB stick. This selection is only available for products with USB connection. This selection is only enabled if a USB stick is inserted and has not been booted from the USB stick.
	Network	The data is uploaded from the PC and restored.
Boot Device	Storage medium from which the device was booted	
PLC Runtime Project	Name of the backup file for the CODESYS project; The input field is only enabled if the network is selected as the data source.	
Settings	Name of the backup file for the settings; The input field is only enabled if the network is selected as the data source.	
System	Name of the backup file for the system data and the root file system; The input field is only enabled if the network is selected as the data source.	
Decryption	Data encryption	
	☐	The data has been encrypted and saved.
	☒	The data was saved unencrypted.
Decryption passphrase	Encryption password; The input field is only displayed if the Decryption checkbox is selected.	

5.5.3 Inserting a Memory Card during Operation

The fieldbus nodes and the PLC program are running.

Insert a memory card during ongoing operation.

During normal operation, the memory card is incorporated into the file system of the controller as a drive. No automatic copy operations are triggered.

The LED above the memory card flashes yellow/orange during the access.

The memory card is then ready for operation and available under /media/sd.

5.5.4 Removing the Memory Card during Operation

The fieldbus node and the PLC program are in operation and the memory card is plugged in.

Remove the memory card during ongoing operation.

Note

Data can be lost during writing!

Note that if you pull the memory card out during a write procedure, data will be lost.

The LED above the memory card flashes yellow/orange during the attempted access.

The controller then works without a memory card.

5.5.5 Setting the Home Directory for the Runtime System

The home directory for the runtime system is located in the controller's internal memory by default. An existing boot project may be saved in the home directory.

You can use the WBM to move the home directory for the runtime system to the memory card, e.g., to make more memory available for a large boot project or other files.

Some conditions must be met before moving the directory.

- A running IEC-61131 application must be stopped and the device brought to its initial state by calling the "Reset (Origin)" function. Any boot project is deleted.
- When moving the home directory to the memory card, insert a memory card formatted to support file system. Only the first partition of a memory card can be accessed at /media/sd and can be used as the home directory.

Only when the two conditions are met can the "Home directory on memory card enabled" checkbox be selected from the WBM on the "PLC Runtime" page.

The setting is applied by clicking the **[Submit]** button and takes effect after the next restart. No files are applied from the old to the new home directory.

After moving the directory, a project must be loaded and a boot project created.

It should be noted that the memory card may not be removed under any circumstances as long as the home directory is there. If an application is running, system safety can be endangered by an uncontrolled controller crash.

Switching the home directory has no effect if the controller was booted from a memory card. The configuration state is saved, but only takes effect if the content of the memory card is copied to the internal memory.

5.5.6 Load Boot Project

If a boot project exists, it may be loaded, depending on the home directory setting for the runtime system. The following table shows the possible results:

Table 26: Loading a Boot Project

Boot Project Stored in Internal Flash Memory	Memory Card with Boot Project Inserted	"Home Directory on Memory Card Enabled" Checked	Loading boot project ...
No	No	No	No, no boot project exists
		Yes	No, no boot project exists
	Yes	No	No, no boot project exists in the internal flash memory
		Yes	Yes, from memory card
Yes	No	No	Yes, from internal flash memory
		(Yes) Invalid	No, invalid combination, since no boot project is allowed to exist in the internal flash memory for this setting
	Yes	No	Yes, from internal flash memory
		(Yes) Invalid	No, invalid combination, since no boot project is allowed to exist in the internal flash memory for this setting

5.6 WAGO Device Access

WAGO Device Access (WDA) is an interface that allows uniform access to device configurations and their settings. The service provides a REST API via HTTP, in which the entire configuration of a device can be accessed.

The WDA REST API can be reached at the following address:

```
https://<IP>/wda  
or  
https://<host name of controller>/wda
```

To access the device configuration, use the Postman software or a browser, for example. Access the data via various methods of the rest API.

Example for querying device parameters:

```
https://192.168.1.113/wda/parameters?page[limit]=10000
```

An online English-language documentation for the installed version is available at the following address:

```
https://<IP>/openapi/wda.openapi.html  
or  
https://<host name of controller>/openapi/wda.openapi.html
```

In addition to manual access via API, devices that have a WDA interface can also be configured via the WAGO Device Manager software. The software provides an overview of the device's parameters, allows them to be changed and transferred to the device. The variable channel configuration of devices can also be performed here.

Note

Information on data models and parameter lists

The section **Documentation > WAGO Device Model** of the WAGO Download Center provides descriptions of the data models and parameter lists used (see <https://download-center.wago.com/productgroup/wdm>).

5.7 Process Image

5.7.1 Analog Inputs AI1, AI2

Table 27: Process Image - Analog Inputs AI1, AI2

Input	Pin	I/O Channel	Data Type	Description
AI1	X14.1	X14.AI1	WORD	Analog input 1
AI2	X14.3	X14.AI2	WORD	Analog input 2

The measurement ranges of the analog inputs can be configured channel by channel.

Configuration is performed using CODESYS or the "WAGO Device Manager" tool.

The following measurement ranges can be configured:

- 0 ... 10 V, default setting
- -10 ... +10 V
- 0 ... 20 mA

- 4 ... 20 mA
- 3.6 ... 21 mA

5.7.1.1 AI 0 ... 10 V

Measured values are represented via the data type WORD (16 bit).

Table 28: Process Image – Process Values AI; 0 ... 10 V; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< 0 V	0x0000	0	0000.0000.0000.0000
0 V	0x0000	0	0000.0000.0000.0000
...	...	...	...
10 V	0x7FFF	32767	0111.1111.1111.1111
> 10 V	0x7FFF	32767	0111.1111.1111.1111

5.7.1.2 AI -10 ... +10 V

Measured values are represented via the data type WORD (16 bit).

Table 29: Process Image – Process Values AI; -10 ... +10 V; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< -10 V	0x8000	-32768	1000.0000.0000.0000
-10 V	0x8000	-32768	1000.0000.0000.0000
...	...	...	...
+10 V	0x7FFF	32767	0111.1111.1111.1111
> +10 V	0x7FFF	32767	0111.1111.1111.1111

5.7.1.3 AI 0 ... 20 mA

Measured values are represented via the data type WORD (16 bit).

Table 30: Process Image – Process Values AI; 0 ... 20 mA; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< 0 mA	0x0000	0	0000.0000.0000.0000
0 mA	0x0000	0	0000.0000.0000.0000
...	...	...	...
20 mA	0x7FFF	32767	0111.1111.1111.1111
> 20 mA	0x7FFF	32767	0111.1111.1111.1111

5.7.1.4 AI 4 ... 20 mA

Measured values are represented via the data type WORD (16 bit).

Table 31: Process Image – Process Values AI; 4 ... 20 mA; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< 4 mA	0x0000	0	0000.0000.0000.0000
4 mA	0x0000	0	0000.0000.0000.0000
...	...	...	...
20 mA	0x7FFF	32767	0111.1111.1111.1111
> 20 mA	0x7FFF	32767	0111.1111.1111.1111

5.7.1.5 AI 3.6 ... 21 mA

Measured values are represented via the data type WORD (16 bit).

Table 32: Process Image – Process Values AI; 3.6 ... 21 mA; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< 3.6 mA	0xFD03	-765	1111 1101 0000 0011
3.6 mA	0xFD03	-765	1111 1101 0000 0011
...	...	...	...
21 mA	0x7FFB	32763	0111.1111.1111.1011
> 21 mA	0x7FFB	32763	0111.1111.1111.1011

5.7.2 Analog Inputs/Outputs AIO1, AIO2

Table 33: Process Image – Analog Inputs/Outputs AIO1, AIO2

Input/Output	Pin	I/O Channel	Data Type	Description
AIO1	X6.1	X6.AIO1	WORD	Analog input/output 1
AIO2	X6.3	X6.AIO2	WORD	Analog input/output 2

The measurement ranges of the analog inputs/outputs can be configured channel by channel.

Configuration is performed using CODESYS or the "WAGO Device Manager" tool.

The following measurement ranges can be configured:

- Inputs
 - 0 ... 10 V, default setting
 - -10 ... +10 V
 - 0 ... 20 mA
 - 4 ... 20 mA
 - 3.6 ... 21 mA
- Outputs
 - 0 ... 10 V
 - -10 ... +10 V
 - -12 ... +12 V
 - 0 ... 20 mA
 - 0 ... 22 mA
 - 4 ... 20 mA

5.7.2.1 AI 0 ... 10 V, -10 ... +10 V, 0 ... 20 mA, 4 ... 20 mA, 3.6 ... 21 mA

If an analog input/output AIO1/AIO2 is configured as an input, the tables of the process values of the analog inputs AI1/AI2 apply.

5.7.2.2 AO 0 ... 10 V

Measured values are represented via the data type WORD (16 bit).

Table 34: Process Image – Process Values AO; 0 ... 10 V; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
0 V	0x0000	0	0000.0000.0000.0000
...	...	...	...
10 V	0x7FFF	32767	0111.1111.1111.1111

5.7.2.3 AO –10 ... +10 V

Measured values are represented via the data type WORD (16 bit).

Table 35: Process Image – Process Values AO; –10 ... +10 V; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
–10 V	0x8000	–32768	1000.0000.0000.0000
...	...	...	...
+10 V	0x7FFF	32767	0111.1111.1111.1111

5.7.2.4 AO –12 ... +12 V

Measured values are represented via the data type WORD (16 bit).

Table 36: Process Image – Process Values AO; –12 ... +12 V; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
–12 V	0x8000	–32768	1000.0000.0000.0000
...	...	...	...
+12 V	0x7FFF	32767	0111.1111.1111.1111

5.7.2.5 AO 0 ... 20 mA

Measured values are represented via the data type WORD (16 bit).

Table 37: Process Image – Process Values AO; 0 ... 20 mA; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
0 mA	0x0000	0	0000.0000.0000.0000
...	...	...	...
20 mA	0x8000	32768	1000.0000.0000.0000

5.7.2.6 AO 0 ... 22 mA

Measured values are represented via the data type WORD (16 bit).

Table 38: Process Image – Process Values AO; 0 ... 22 mA; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
0 mA	0x0000	0	0000.0000.0000.0000
...	...	...	...
22 mA	0x7FFF	32767	0111.1111.1111.1111

5.7.2.7 AO 4 ... 20 mA

Measured values are represented via the data type WORD (16 bit).

Table 39: Process Image – Process Values AO; 4 ... 20 mA; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
4 mA	0x0000	0	0000.0000.0000.0000
...	...	...	...
20 mA	0x7FFF	32767	0111.1111.1111.1111

5.7.3 Temperature Inputs PT1+/PT1–, PT2+/PT2–

Table 40: Process Image – Temperature Inputs PT1+/PT1–, PT2+/PT2–

Input	Pin	I/O Channel	Data Type	Description
PT1+	X13.1	X13.PT1+/PT1–	INT	RTD input 1
PT1–	X13.2			
PT2+	X13.3	X13.PT2+/PT2–	INT	RTD input 2
PT2–	X13.4			

The measurement ranges of the RTD inputs can be configured channel by channel.

Configuration is performed using CODESYS or the "WAGO Device Manager" tool.

The following measurement ranges can be configured:

- Pt100 (–200 ... +850 °C)
- Pt200 (–200 ... +850 °C)
- Pt500 (–200 ... +850 °C)
- Pt1000 (–200 ... +850 °C), default setting
- Ni100 (–60 ... +250 °C)
- Ni120 (–80 ... +260 °C)
- Ni1000 (TK6180) (–60 ... +250 °C)
- Ni1000 (TK5000) (–60 ... +250 °C)
- Potentiometer 0 ... 1.2 kOhm
- Potentiometer 0 ... 5 kOhm

On the hardware side, resistance values between 450 and 4400 Ohm can be captured. The representation of resistance values outside this range is undefined.

5.7.3.1 Pt100, Pt200, Pt500, Pt1000

Measured values are represented via data type INT (16 bits).

The resolution is 1 digit per 0.1 °C.

Table 41: Process Image – Process Values RTD; Pt100, Pt200, Pt500, Pt1000; –200 ... +850 °C; 16 Bit; INT

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< –200 °C	0xF830	–2000	1111.1000.0011.0000
–200 °C	0xF830	–2000	1111.1000.0011.0000
...	...	...	...
+850 °C	0x2134	8500	0010.0001.0011.0100
> +850 °C	0x2134	8500	0010.0001.0011.0100

5.7.3.2 Ni100, Ni1000 (TK6180), Ni1000 (TK5000)

Measured values are represented via data type INT (16 bits).

The resolution is 1 digit per 0.1 °C.

Table 42: Process Image – Process Values RTD; Ni100, Ni1000 (TK6180), Ni1000 (TK5000); –60 ... +250 °C; 16 Bit; INT

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< –60 °C	0xFDA8	–600	1111.1101.1010.1000

Measured Value	Value Range		
	Hex.	Dec.	Bin.
–60 °C	0xFDA8	–600	1111.1101.1010.1000
...	...	...	...
+250 °C	0x09C4	2500	0000.1001.1100.0100
> +250 °C	0x09C4	2500	0000.1001.1100.0100

5.7.3.3 Ni120

Measured values are represented via data type INT (16 bits).

The resolution is 1 digit per 0.1 °C.

Table 43: Process Image – Process Values RTD; Ni120; –80 ... +260 °C; 16 Bit; INT

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< –80 °C	0xFCE0	–800	1111.1100.1110.0000
–80 °C	0xFCE0	–800	1111.1100.1110.0000
...	...	...	...
+260 °C	0x0A28	2600	0000.1010.0010.1000
> +260 °C	0x0A28	2600	0000.1010.0010.1000

5.7.3.4 Potentiometer 0 ... 1.2 kOhm

Measured values are represented via data type INT (16 bits).

The resolution is 1 digit per 0.05 Ohm.

Table 44: Process Image – Process Values RTD; Potentiometer; 0 ... 1200 Ohm; 16 Bit; INT

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< 0 Ohm	0x0000	0	0000.0000.0000.0000
0 Ohm	0x0000	0	0000.0000.0000.0000
...	...	...	...
1200 Ohm	0x5DC0	24000	0101.1101.1100.0000
> 1200 Ohm	0x5DC0	24000	0101.1101.1100.0000

5.7.3.5 Potentiometer 0 ... 5 kOhm

Measured values are represented via data type INT (16 bits).

The resolution is 1 digit per 0.2 Ohm.

Table 45: Process Image – Process Values RTD; Potentiometer; 0 ... 5000 Ohm; 16 Bit; INT

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< 0 Ohm	0x0000	0	0000.0000.0000.0000
0 Ohm	0x0000	0	0000.0000.0000.0000
...	...	...	...
5000 Ohm	0x61A8	25000	0110.0001.1010.1000
> 5000 Ohm	0x61A8	25000	0110.0001.1010.1000

5.7.4 Digital Inputs DI

Table 46: Process Image – Digital Inputs DI1 ... DI8

Input	Pin	I/O Channel	Data Type	Description
DI1	X12.3	X12.DI1	BOOL	Digital input 1
DI2	X12.4	X12.DI2	BOOL	Digital input 2
DI3	X12.5	X12.DI3	BOOL	Digital input 3
DI4	X12.6	X12.DI4	BOOL	Digital input 4
DI5	X12.7	X12.DI5	BOOL	Digital input 5
DI6	X12.8	X12.DI6	BOOL	Digital input 6
DI7	X12.9	X12.DI7	BOOL	Digital input 7
DI8	X12.10	X12.DI8	BOOL	Digital input 8

Measured values are represented per channel via the BOOL data type.

Table 47: Process Image – Process Values of Digital Inputs – BOOL

Measured Value	Value Range		
	Hex.	Dec.	Bin.
0 V	---	---	FALSE
+24 V	---	---	TRUE

5.7.5 Digital Inputs/Outputs DIO

Table 48: Process Image – Digital Inputs/Outputs DIO1 ... DIO8

Input/Output	Pin	I/O Channel	Data Type	Description
DIO1	X5.3	X5.DIO1	BOOL	Digital input/output 1
DIO2	X5.4	X5.DIO2	BOOL	Digital input/output 2
DIO3	X5.5	X5.DIO3	BOOL	Digital input/output 3
DIO4	X5.6	X5.DIO4	BOOL	Digital input/output 4
DIO5	X5.7	X5.DIO5	BOOL	Digital input/output 5
DIO6	X5.8	X5.DIO6	BOOL	Digital input/output 6
DIO7	X5.9	X5.DIO7	BOOL	Digital input/output 7
DIO8	X5.10	X5.DIO8	BOOL	Digital input/output 8

Configuration is performed using CODESYS or the “WAGO Device Manager” tool.

5.7.5.1 DI 0/24 V

Measured values are represented per channel via the BOOL data type.

Table 49: Process Image – Process Values of Digital Inputs – BOOL

Measured Value	Value Range		
	Hex.	Dec.	Bin.
0 V	---	---	FALSE
+24 V	---	---	TRUE

5.7.5.2 DO 0/24V

Measured values are represented per channel via the BOOL data type.

Table 50: Process Image – Process Values, Digital Outputs – BOOL

Measured Value	Value Range		
	Hex.	Dec.	Bin.
0 V	---	---	FALSE
+24 V	---	---	TRUE

6 Planning

6.1 Structure Guidelines

6.1.1 Safety Measures at the Installation Location

The product is an open type device.

It must only be installed in suitable enclosures, cabinets or electrical operating rooms that meet the following requirements at a minimum:

- Offer adequate protection against direct or indirect contact.
- Offer adequate protection against UV irradiation.
- Restrict access to authorized personnel and may only be opened with tools.
- Ensure the required pollution degree in the vicinity of the system.
- Prevent fire from spreading outside of the enclosure.
- Guarantee mechanical stability.

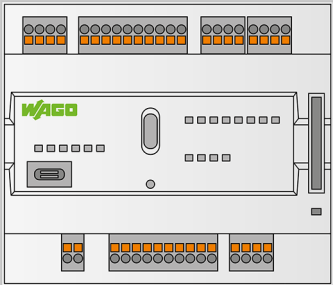
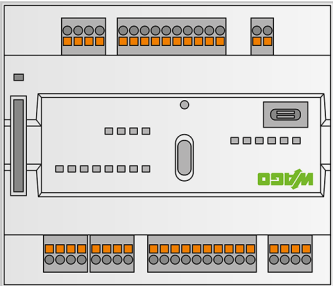
6.1.2 Mounting Position and Distances

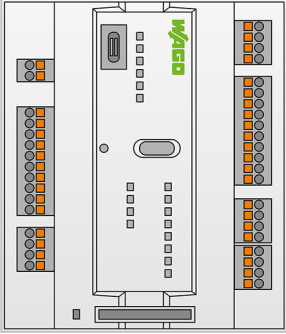
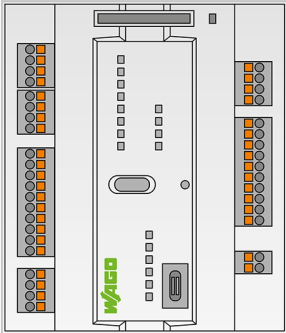
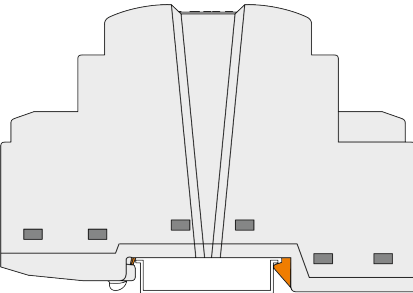
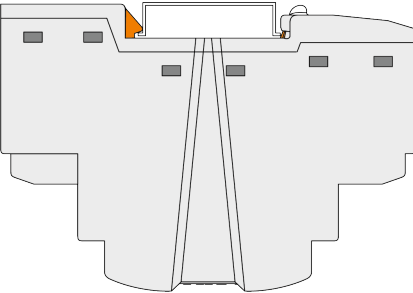
All specifications and handling steps refer to the nominal mounting position. Deviating mounting positions affect, for example:

- The permissible ambient temperature

The following mounting positions are permitted:

Table 51: Mounting Positions and Permissible Ambient Temperatures

Mounting Position	Permissible Ambient Temperature
Horizontal (nominal mounting position) 	D = 10 mm: -25 ... +60 °C D = 0 mm: -25 ... +55 °C
Horizontal 180 ° 	D = 0 mm: -25 ... +55 °C

Mounting Position	Permissible Ambient Temperature
Vertical 	D = 0 mm: -25 ... +55 °C
Vertical 180 ° 	D = 0 mm: -25 ... +50 °C
Floor mounting 	D = 0 mm: -25 ... +50 °C
Overhead mounting 	D = 0 mm: -25 ... +50 °C

Maintain the following distances from adjacent products, cable ducts and the sides of housings and frames for the setup.

The distance (D) from the power supply is 0 ... 10 mm, depending on the mounting position. For adjacent components on a DIN-rail, a distance below this minimum is possible if necessary.

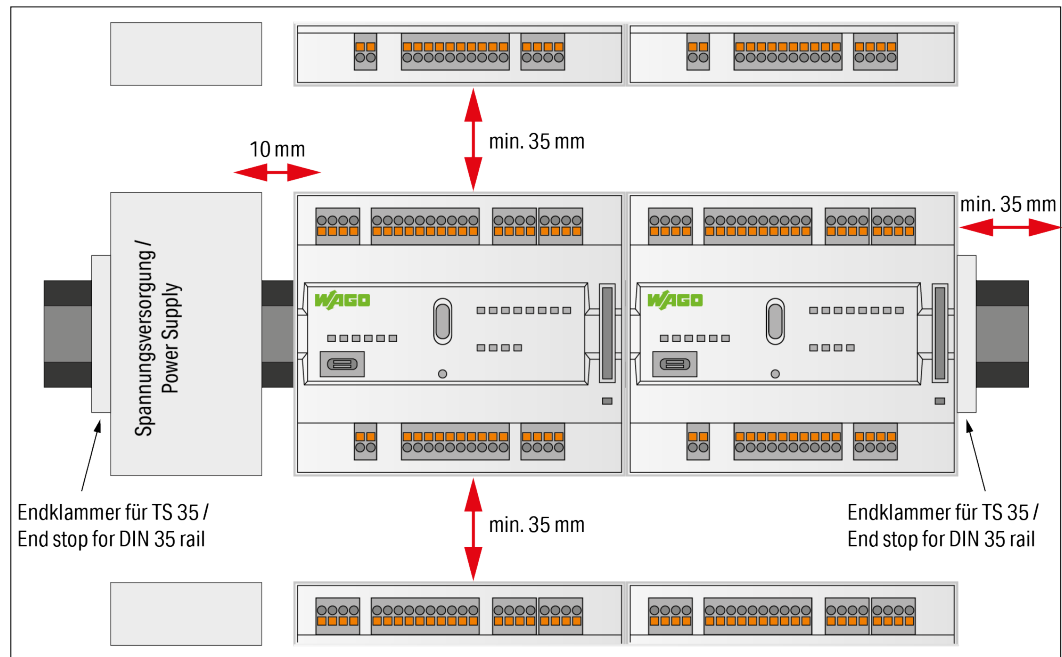


Figure 11: Distances

The distances leave space for heat dissipation and installation/wiring. The distances from cable ducts also prevent conducted electromagnetic interference from affecting operation.

If installation space is limited in the control cabinet or small installation distribution board, use angled network cables or patch cables for the X1 and X2 network connections if necessary.

6.1.3 DIN-Rail Characteristics

- The material must have high corrosion resistance.
- The DIN-rail geometry must not be altered.
- Prevent bending and twisting (torsion) e.g., by using sufficient attachment points.
- Use countersink-head screws, blind rivets, etc., to countersink the attachment points beneath the node structure.
- The component DIN-rail contact (CuSn6) must not form a galvanic element with the DIN-rail that is capable of generating a differential voltage of more than 0.5 V (saline solution of 0.3% at 20°C/68°F).

6.1.4 EMC Installation

▪ Ground DIN-rails.

Ground the DIN-rails to divert electromagnetic interference.

▪ Use shielded cables for data and signal lines.

Electromagnetic interference is reduced and signal quality increased. Measurement errors, data transmission faults and interference due to excessive voltage can be prevented!

▪ Keep data and signal lines separate from interference sources.

Route data and signal lines separately from all power supply cables and other sources of high electromagnetic emissions (e.g., frequency converters or drives).

▪ Connect the cable shielding with the ground potential.

Integrated shielding is mandatory to meet technical specifications regarding measurement accuracy. Establish the connection between the cable shielding and ground potential at the inlet of the cabinet or housing. This grounding allows induced interferences to dissipate and be kept away from devices in the cabinet or housing.

- **Improve shielding performance with a large contact area.**

A low-impedance connection between shielding and ground achieves better shielding performance. For this purpose, connect the shielding over a large surface area, e.g., using the WAGO Series 790 Shield Connection System. This is especially recommended for large-scale systems where equalizing or high impulse currents may occur.

6.1.5 Grounding

Snapping the product onto the grounded DIN-rail grounds it via the spring contacts on the underside.

6.1.6 Data Security

Professional planning and configuration are an important prerequisite for ensuring the confidentiality, availability and integrity of data.

Random Influences

Data transmission and processing can be disrupted by random influences, such as temporary electromagnetic disturbances. Proper setup can significantly reduce the likelihood of corruption or destruction of data.

For additional information see: [🔗 EMC Installation \[► 53\]](#).

Deliberate Influences

Use in ETHERNET Areas

ETHERNET products are designed for use in local networks. Please note the following when using ETHERNET products in your system:

- Do not connect control components and control networks to an open network such as the Internet or an office network.
WAGO recommends putting control components and control networks behind a firewall.
- In the control components, close all ports and services not required by your application to minimize the risk of cyber attacks and to enhance cybersecurity.
Only open the ports and services for the duration of the commissioning/configuration.
- Limit physical and electronic access to all automation components to authorized personnel only.
- To reduce the risk of unauthorized access to your system, change the default passwords during initial commissioning.
- To reduce the risk of unauthorized access to your system, regularly change the passwords used.
- To verify that the measures taken meet your security requirements, regularly perform threat analyses.
- To restrict access to and control of individual products and networks, employ a "defense-in-depth" mechanism in your system's security configuration.

Additional documents

- [📄 White Paper Cybersecurity in Production Facilities](#)

All the documentation and information is available at: [🔗 www.wago.com](http://www.wago.com).

Use of Cloud Services

Note

Please note the risks of using cloud services!

If you use third-party cloud services, sensitive data is transferred to the cloud service provider on your own responsibility. External access may result in manipulated data and/or unwanted control commands affecting the performance of your control system.

- Use encryption methods to protect your data.
- Observe the information provided by the Federal Office for Information Security – “Cloud: Risks and Security Tips.”
- Observe comparable publications of the responsible authorities of your country.

Additional information is available at: www.bsi.bund.de.

6.1.7 Buffering

To compensate for power interruptions per IEC 61131 (PS-1 or PS-2), external buffering is required.

Buffer capacity depends on the node configuration, which is why it is not possible to provide general information on the required capacity.

6.2 CODESYS V3 Compatibility

Table 52: Compatibility Overview

Device Description	Firmware *)	Compiler	Visualization Profile
6.3.1.xx	04.06.xx (28)	3.5.19.7	CODESYS Visualization 4.6.0.0

*) Notes on firmware versions:

- Not every new firmware contains a new version of the runtime environment, which is why the compiler version and visualization profile may remain unchanged.
- As a general rule, the compatibility also extends to hotfix and patch versions of the firmware, assuming only the bugfix point of the firmware version is different (example: “FW:01.02.xx(03)”).

7 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.

8 Installation and Removal

8.1 Mounting on the DIN-Rail

Mount the product per EN 60715 by snapping it onto the DIN-rail without tools:

1. Tilt the product slightly.
2. Place the product, with the DIN-rail guide, on the top edge of the DIN-rail.

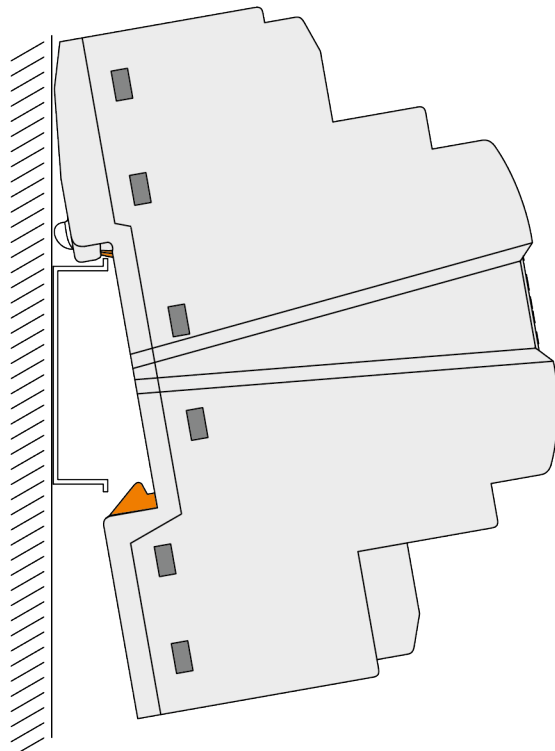


Figure 12: Inserting Controller

3. Press the product onto the DIN-rail.
4. Push down until the product audibly snaps into place.
5. Gently shake the product to ensure that it is correctly locked into place.
6. To ensure secure fastening on the DIN-rail, fit end stops on either side of the product (with a block arrangement: on either side of the products).

8.2 Removal from the DIN-Rail

1. To remove, pull the DIN-rail release tab down.
Use a screwdriver or operating tool for this purpose.
⇒ The product is now unlocked.
2. Tilt the product forward and unhook it from the DIN-rail.

8.3 Connectors

8.3.1 Delivery Condition

When the product is delivered, the female connectors are included but not plugged in.

8.3.2 WAGO Pluggable Connectors

8.3.2.1 Pulling the Female Connector

WAGO recommends using the unlocking tool for WAGO 2092 Series Pluggable Connectors (referred to in the following text as the "unlocking tool"). You can find more information on the unlocking tool in www.wago.com/2092-1630.

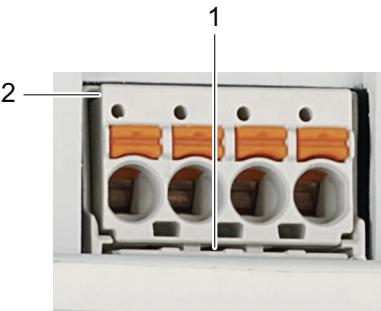


Figure 13: Removing the Female Connector without Wiring (Application Example)

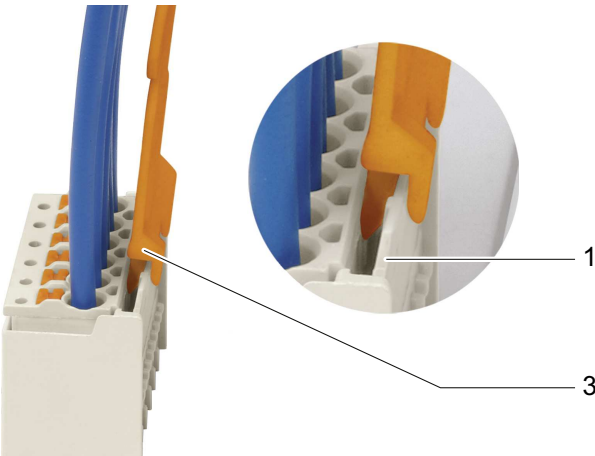


Figure 14: Removing the Female Connector with Wiring (Application Example)

Position	Description
1	Male locking latch
2	Overhanging edge of the female connector
3	Unlocking tool

8.3.2.1.1 Pulling with the Unlocking Tool

Proceed as follows to remove the female connector using the unlocking tool:

Removing the Female Connector without Wiring

1. Place the unlocking tool (3) onto the locking latch (1).
2. Insert the unlocking tool until it hits the stop.
 - ⇒ The wedge opens the locking latch, leasing the locking mechanism.

3. Grasp the underside of the overhanging edge of the female connector (2).
4. Pull out the female connector.

Removing the Female Connector with Wiring

1. Place the unlocking tool (3) onto the locking latch (1).
2. Insert the unlocking tool until it hits the stop.
 - ⇒ The wedge opens the locking latch, leasing the locking mechanism.
3. Pull on the unlocking tool together with the conductors to remove the female connector.

8.3.2.1.2 Pulling with Other Tools

If you do not have an unlocking tool available, you can also remove the female connector with a WAGO operating tool.

Pulling the Female Connector

WARNING

Do not insert the operating tool into the ventilation slots!

Components inside the product may be damaged if the blade of the operating tool enters the ventilation slots. This may lead to serious damage with a risk of injury caused by malfunction, overheating or electric shock!

- When using the operating tool, make sure it is positioned correctly between the locking latch and the female connector!

NOTICE

Do not pull on the conductors when using an operating tool!

Pulling on the conductors can loosen the contact.

1. Do **not** pull on the conductors!
2. Grasp the underside of the overhanging edge of the female connector to pull it out.

1. Use the operating tool to push the locking tab (1) away from the female connector.
2. Grasp the underside of the overhanging edge of the female connector (2).
3. Pull out the female connector.

8.3.2.2 Plugging the Female Connector

DANGER

Be sure to use the correct slot on the female connector!

Mismatching the input female connector into the output connector may lead to a hazardous voltage of 230 V on the output side.

- Make sure the female connector is properly mated to the correct slot!

Proceed as follows to plug the female connector into the corresponding male header:

1. Insert the female connector into the corresponding male header.
2. Push the female connector into the male header until the female connector snaps into position with an audible click.
3. When inserting with wiring: Check that the female connector is seated securely by gently pulling on the wires.

9 Connection

9.1 Connecting the Supply Voltage

- Connect the power supply to connector X4, pin 1 (US+) and pin 2 (GND), as well as to connector X5, pin 1 (Uin+) and pin 2 (0V). Use the connectors included in the delivery (female connector with item number 2091-1122 resp. female connector with item number 2091-1130).

Switch on the power supply for connector X5 before or at least simultaneously with the power supply for connector X4!

10 Commissioning

10.1 Switching On

Before switching the controller on, verify that you have:

- Properly installed the controller
- Connected all the required data cables to the corresponding interfaces and secured the connectors with their attached locking screws
- Connected the electronics and field-side power supply
- Performed appropriate potential equalization on your machine/system
- Implemented the shielding properly

To switch the controller on, switch your power supply unit on.

Brief flashing of the LEDs indicates that the controller is starting up.

After a few seconds, the SYS LED signals a successful controller boot operation.

The CODESYS V3 runtime system starts simultaneously.

If there is an executable IEC 61131-3 program stored and running on the controller, the RUN LED lights up green.

If no executable program is stored on the controller or the mode selector switch is set to STOP, this is also indicated by the RUN LED (see section).

10.2 Setting an IP address

The controller uses the fixed IP address 192.168.42.42 to communicate with a PC.

In the controller's initial state, the following IP addresses are active for the ETHERNET interface (Port X1 and Port X2):

Table 53: Default IP Addresses for ETHERNET Interfaces

ETHERNET Interface	Default Setting
X1/X2 (Switched Mode)	Dynamic assignment of IP address using DHCP ("Dynamic Host Configuration Protocol")

- Adapt IP addressing to your specific system structure to ensure that the PC and the controller can communicate with one another using one of the available configuration tools (e.g., WBM or WAGO ETHERNET Settings – see section [Configuration \[► 67\]](#)).

Example for incorporating the controller (192.168.2.17) into an existing network:

- The IP address of the host PC is **192.168.1.2**.
- The controller and host PC must be in the same subnet (regardless of the IP address of the host PC).
- With a subnet mask of **255.255.255.0**, the first three digits of the IP address of the host PC and controller must match so that they are located in the same subnet.

Table 54: Network Mask 255.255.255.0

Host-PC	Subnet Address Range for the Controller
192.168.1.2	192.168.1.1 oder 192.168.1.3 ... 192.168.1.254

See also

📄 Configuration [▶ 67]

10.2.1 IP Connection via USB

You can establish an IP connection via USB for commissioning and for service purposes.

1. Connect the controller to your PC via the USB service interface and a USB service cable.
2. If you are using Windows® 10, go to step 4.
 - ⇒ In Windows® 7, the controller behaves like an external drive after connection. A driver for the IP connection via USB is stored on the drive.
3. Install this driver.
 - ⇒ Communication is then possible via the IP connection via USB.
4. Call up the fixed IP address 192.168.42.42 in the browser.
 - ➔ The Web-Based Management of the controller opens.
 - ➔ You can use it to make all the necessary settings on the controller.

10.2.2 Changing an IP Address in “WAGO Ethernet Settings”

The Microsoft Windows® application “WAGO Ethernet Settings” is a software used to identify the controller and configure network settings.

For data communication, you can use the WAGO USB service cable or, if applicable, the IP network.

1. Switch off the power supply to the controller.
2. Establish a suitable connection between the controller and your PC.
3. Switch on the power supply to the controller again.
4. Start the “WAGO Ethernet Settings” program.

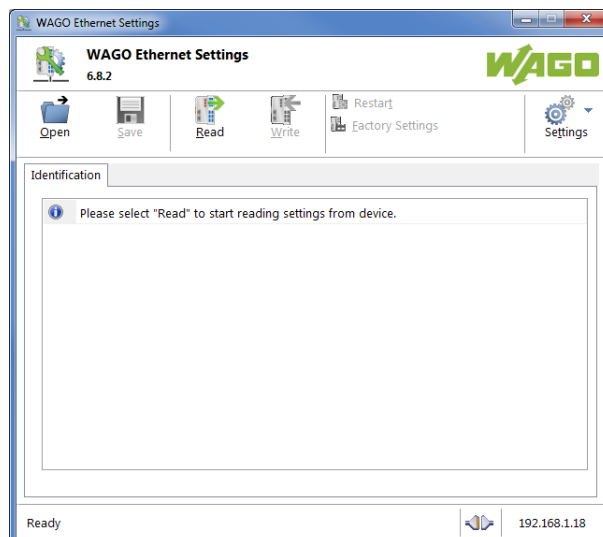


Figure 15: WAGO Ethernet Settings – Start Screen (Example Figure)

5. Click the **[Read]** button to read and identify the connected controller.
6. Select the **“Netzwerk”** tab:

Parameter	Edit	Currently used
Address Source	Static Configuration	Static Configuration
IP address	192.168.1.18	192.168.1.18
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0
Preferred DNS-Server	0.0.0.0	0.0.0.0
Alternative DNS-Server	0.0.0.0	0.0.0.0
Time Server	0.0.0.0	0.0.0.0
Hostname		PFC200-400E6F
Domain name	localdomain.lan	localdomain.lan

Interface X1

Interface X2

Run WBM

Interfaces

☐ Switched

☒ Separated

Figure 16: WAGO Ethernet Settings – Network Tab (Example Figure)

7. To assign a fixed address, select “Static configuration” on the “**Source**” line under “**Input**”. DHCP is normally enabled as the default setting.
8. In the “**Input**” column, enter the required IP address and, if applicable, the address of the subnet mask and gateway.
9. Click the [**Write**] button to apply the address in the controller. (If necessary, “WAGO Ethernet Settings” will restart your controller automatically. This action can take about 30 seconds.)
10. You can now close “WAGO Ethernet Settings” or make other changes directly in the Web-Based Management system as required. To do so, click the [**Start WBM**] button in the right-pane.

10.2.3 Temporarily Setting a Fixed IP Address

This operation temporarily sets the IP address for interface X1 to the fixed address “192.168.1.17.”

If the switch is switched on, the fixed address is also used for interface X2. When the switch is disabled, the original address setting for interface X2 is not changed. No reset is carried out.

To temporarily set a fixed IP address, proceed as follows:

1. Set the operating mode switch to the STOP position.
 2. Press the reset button for more than 8 seconds.
- ➔ Execution of the setting is signaled by the “SYS” LED flashing orange.

To cancel the setting, proceed as follows:

- Perform a software reset or power the product off and on again.

10.2.4 Setting the IP Address via the WBM

You can change the IP address of the controller directly via the built-in Web-Based Management without additional tools.

1. Use a suitable network cable to connect the controller and your PC.
2. Open an internet browser on the PC.
3. Call up the WBM on the controller. To do this, enter the following in the input line of the browser: “https://<IP address>/wbm”.
4. If you do not know the IP address, determine the IP address as described above.
 - ➔ You will then be asked to authenticate.

5. Enter the user name "user" and the corresponding password ("user" by default).
 - ⇒ If you have not already changed the default password, you are asked to change the password now.
6. Open the "Configuration" tab.
7. In the navigation, select the "Networking" item and "TCP/IP Configuration" subitem.
8. In the "TCP/IP Configuration" group, select the "Static IP" entry in the "IP Source" selection field.
9. Enter the required IP address in the "Static IP Address" input field.
10. Enter the required subnet mask in the "Subnet Mask" input field.
11. Click the **[Submit]** button to apply the changes.
 - ⇒ Changing the IP address interrupts the connection to the controller.
12. Establish a new connection with the new IP address.

10.2.5 Assigning an IP Address Using DHCP

The controller can obtain its dynamic IP address from a server (DHCP). In contrast to fixed IP addresses, dynamically assigned addresses are not stored permanently. Therefore, a DHCP server must be available each time the controller is restarted.

If an IP address has been assigned by means of DHCP (default setting), it can be determined through the settings and the output of the specific DHCP server.

In conjunction with the DNS server associated with DHCP, the device can be reached using its hostname. This consists of a prefix and the MAC address or part of it. The MAC address of the product is printed on the label on the side of the product.

The following example shows the corresponding output of "Open DHCP".

```
C:\OpenDHCP>OpenDHCP.exe -v
Open DHCP Server Version 1.75 Windows Build 1052 Starting...
Logging: ALL
Warning: No IP Address for DHCP Static Host 00:ff:a4:0e:ef:99 specified
Warning: No IP Address for DHCP Static Host ff:00:27:78:7b:01 specified
Warning: No IP Address for DHCP Static Host ff:00:27:78:7b:02 specified
Warning: No IP Address for DHCP Static Host ff:00:27:78:7b:03 specified
Default Lease: 36000 (sec)
Server Name: DESKTOP-67MMSRM
Detecting Static Interfaces..
Lease Status URL: http://127.0.0.1:6789
Listening On: 192.168.2.1
Network changed, re-detecting Static Interfaces..
DHCPDISCOVER for 00:30:de:46:68:98 () from interface 192.168.2.1 received
Host 00:30:de:46:68:98 (Host0030de466898) offered 192.168.2.201
Lease Status URL: http://127.0.0.1:6789
Listening On: 192.168.2.1
Network changed, re-detecting Static Interfaces..
DHCPREQUEST for 00:30:de:46:68:98 () from interface 192.168.2.1 received
Host 00:30:de:46:68:98 (Host0030de466898) allotted 192.168.2.201 for 36000 seconds
```

Figure 17: "Open DHCP", Example Figure

In the example shown, the prefix is "Host" and the MAC ID is "00:30:de:46:68:98".

The host name is "Host0030de466898".

10.3 Testing the Network Connection

Carry out a ping network function to check whether you can reach the controller at the IP address you have assigned in the network.

1. Open the command prompt. Enter the command "cmd" in the input field under **Start > Windows System > Run** (Windows® 10) or **Start > Programs/Search Programs** (Windows® 7).

2. Click the **[OK]** button or press **Enter** to confirm the entry.
3. Enter the "ping" command and IP address of the controller (e.g., ping 192.168.1.17) at the command prompt.
4. Press **Enter** to confirm the entry.
 - ⇒ Your PC sends a query that is answered by the controller. The answer appears in the command prompt. If the "Timeout" error message appears, the controller has not responded properly. In this case, check the network settings.

```

C:\WINDOWS\system32\cmd.exe
U:\>ping 192.168.1.17
Ping wird ausgeführt für 192.168.1.17 mit 32 Bytes Daten:
Antwort von 192.168.1.17: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.1.17: Bytes=32 Zeit=1ms TTL=64
Ping-Statistik für 192.168.1.17:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms
U:\>
  
```

Figure 18: Example of a Functional Test

5. Close the command prompt if the test is successful.

10.4 Changing Passwords

Note

Change passwords!

The default passwords are documented in these instructions and therefore do not offer adequate protection.

- Change the passwords to meet your particular needs.

Note

Valid characters for passwords

Passwords may contain only the following characters:

lowercase letters (a ... z), uppercase letters (A ... Z), numbers (0 ... 9) and special characters (! " # \$ % & ' () * + , . / : ; < = > ? @ [] ^ _ ` { } | ~ -).

To increase security, passwords should contain a mix of lowercase letters, uppercase letters, numbers and special characters.

Passwords should not contain generally known names, dates of birth and other information that is easy to guess.

Therefore, change the default passwords before commissioning the controller.

Default passwords are assigned for the "Linux® Users" user group and are listed in the table [Linux® user \[p. 30\]](#).

To change the passwords via WBM, proceed as follows:

1. Connect the controller to a PC via one of the network interfaces (X1, X2).
2. Start a Web browser on the PC and call up the controller WBM.
3. Log on to the controller as user "root", "admin" or "user" with the default password.

4. Change the password for the logged-in user on the WBM "Configuration of the users for the WBM" page.
5. In this way, change the passwords for all users.

To change the passwords using a terminal program, proceed as follows:

1. Connect the controller to a PC via the X1 network interface.
2. Start a terminal program on your PC.
3. Log in on the controller as the "root" user with the default password.
4. Change the password for all users with the "passwd root," "passwd admin" and "passwd user" commands.

10.5 Switch Off/Restart

Switch off the power supply to shut down the controller.

To reset the controller software (reboot), press the reset button. Alternatively, you can switch off the controller and switch it back on again.

Note

Do not power cycle the controller after changing any parameters!

Some parameter changes require a controller restart for the changes to apply. Saving the changes takes some time.

Do not power cycle the controller to perform a restart, i.e., changes may be lost by shutting down the controller too soon.

Only restart using the software reboot function. This ensures that all memory operations are completed correctly and completely.

See also

 Software Reset [► 83]

10.6 Configuration

10.6.1 Configuration in the Web-Based Management System (WBM)

The HTML pages (hereinafter referred to as "pages") of the Web-Based Management are used to configure the controller. To access the WBM via a Web browser, proceed as follows:

1. Connect the controller to your PC via ETHERNET interface X1 and the ETHERNET network or via the USB service port and a USB service cable.
2. Launch a Web browser on your PC.
3. Enter "https://" in the address bar of your Web browser, followed by the IP address of the controller and "/wbm," e.g., "https://192.168.1.17/wbm." Note that the PC and controller must be located in the same subnet; see Setting an IP address.

If you do not know the IP address and cannot determine it, temporarily switch the controller to the fixed preset IP address "192.168.1.17," see Temporarily Setting a Fixed IP Address.

Note**Take usage by the CODESYS program into account!**

If the controller is at capacity due to a CODESYS program, this may result in slower processing in the WBM. As a result, timeout errors are sometimes reported in some circumstances.

- Stop the CODESYS application via the WBM before making extensive configurations.

⇒ When the connection has been established, a login window opens.

Authentication

Hostname: PFC200V3-42E739
Application: Web-based Management

Username

Password

< cancel > Login

Figure 19: Log-in Window

4. Enter the username and password.

5. Click the button [**> Login**].

⇒ The navigation bar and tabs of the WBM are displayed according to the user selected.

If you have disabled cookies in your Web browser, you can continue to use the WBM as long as you move directly inside it. However, if you fully reload the website (e.g., with **[F5]**), you must log in again since the Web browser is then not able to store the data of your login session.

10.6.1.1 User Administration of WBM

To allow settings to be made only by a select group of users, limit access to WBM functions through User Administration.

Note**Change passwords!**

The default passwords are documented in these instructions and therefore do not offer adequate protection.

- Change the passwords to meet your particular needs.

If you do not change these passwords, a warning will appear each time you open a website after logging in.

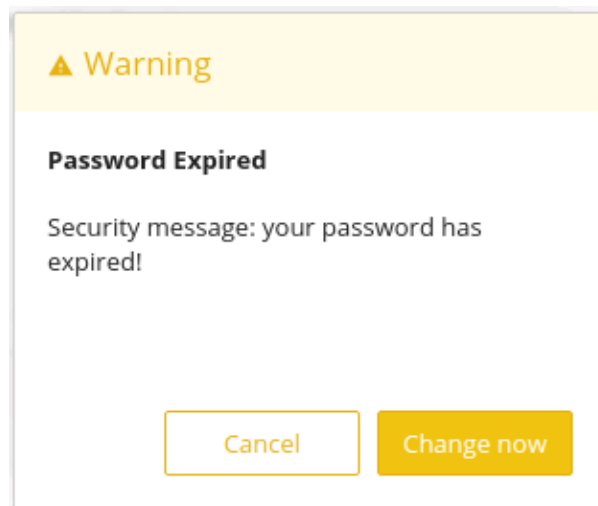


Figure 20: Password Reminder

Clicking the **[[Change now]]** button takes you directly to the WBM page where you can change the password.

Table 55: Default Passwords on Delivery

User	Rights	Password
root	All (administrator)	wago
admin	All (administrator)	wago
user	Limited	user

i Note

General Rights of WBM Users

The WBM users "admin" and "user" have rights beyond the WBM to configure the system and install software.

User administration for controller applications is configured and managed separately.

Access to the WBM pages is as follows.

The "root" user has the same rights as the "admin" user and is therefore not listed separately.

10.6.1.2 WBM Page Overview and Access Rights

The WBM pages require the access rights listed in the table below. Users with lower privileges may not be able to access the pages or may only be able to view them.

Table 56: Access Rights for WBM Pages

Tab	Navigation		WBM Page Title	User
Information	Device Status		Device Status	user
	Vendor Information		Vendor Information	user
	PLC Runtime		PLC Runtime Information	user
	Legal Information	WAGO Licenses	WAGO Software License Agreement	user
		Open Source Licenses	Open Source Licenses	user
		WBM Licenses	WBM Third Party License Information	user

Tab	Navigation		WBM Page Title	User
		Trademarks Information	Trademarks Information	user
	WBM Version		WBM Version Info	user
Configuration	PLC Runtime		PLC Runtime Configuration	user
	Networking	TCP/IP Configuration	TCP/IP Configuration	user
		Ethernet Configuration	Ethernet Configuration	user
		Host/Domain Name	Configuration of Host and Domain Name	user
		Routing	Routing	user
		STP/RSTP	Spanning Tree Protocol	user
	Clock		Clock Settings	user
	Administration	Create Image	Create bootable Image	admin
	Package Server	Firmware Backup	Firmware Backup	admin
		Firmware Restore	Firmware Restore	admin
		Active System	Active System	admin
	Mass Storage		Mass Storage	admin
	Software Uploads		Software Uploads	admin
	Ports and Services	Network Services	Configuration of Network Services	admin
		NTP Client	Configuration of NTP Client	admin
		PLC Runtime Services	PLC Runtime Services	admin
		SSH	SSH Server Settings	admin
		DHCP Server	DHCP Server Configuration	admin
		DNS	Configuration of DNS Server	user
	Cloud Connectivity	Status	Overview	admin
		Connection 1	Configuration	admin
		Connection 2	Configuration	admin
	SNMP	General Configuration	Configuration of general SNMP parameters	admin
		SNMP v1/v2c	Configuration of SNMP v1/v2c parameters	admin
		SNMP v3	Configuration of SNMP v3 Users	admin
	Commissioning		Commissioning Settings	admin
	Docker		Docker Settings	admin
	Users		WBM User Configuration	user
Fieldbus	OPC UA		OPC UA Configuration	admin
	BACnet	Status	BACnet Status	admin
		Configuration	BACnet Configuration	admin
		Data Link	BACnet Data Link	admin
		Storage Location	BACnet Storage Location	admin
		Info	BACnet Info	admin
Security	Open VPN/IPsec		OpenVPN / IPsec Configuration	admin
	Firewall	General Configuration	General Firewall Configuration	admin
		Interface Configuration	Interface Configuration	admin
		MAC Address Filter	Configuration of MAC Address filter	admin
		User Filter	Configuration of User Filter	admin
	Certificates		Certificates	admin

Tab	Navigation	WBM Page Title	User
	Boot Mode	Boot mode configuration	admin
	TLS	Security Settings	admin
	Integrity	Advanced Intrusion Detection Environment (AIDE)	admin
	WAGO Device Access	WAGO Device Access	admin
Diagnostic	Log Message	Log Message Viewer	user
	Download	Download	admin
	Network Capture	Network Capture	admin

10.6.1.3 General Page Information

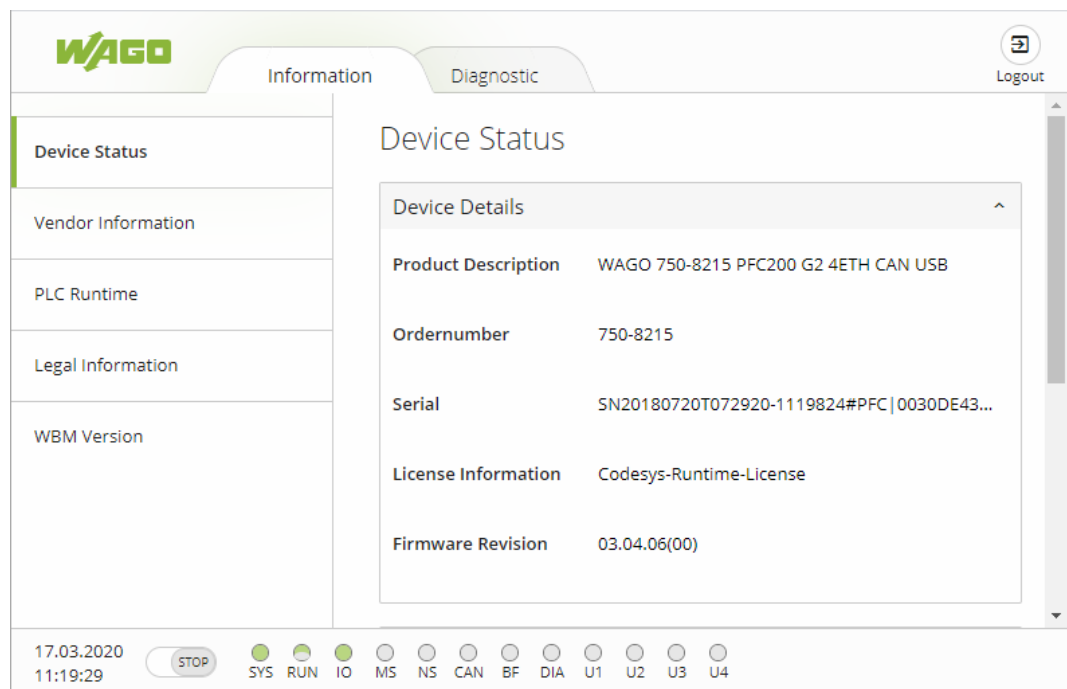


Figure 21: WBM Browser Window (Example)

The tabs for the various WBM areas and the **[Reboot]** and **[Logout]** buttons are displayed in the header of the browser window. The **[Reboot]** button only appears if you are logged in as an administrator. You can use the **[Reboot]** button to reboot the controller. Rebooting may take a few minutes. Use the **[Logout]** button to log the current user out if you do not want to use the interface any longer. You then return to the login prompt.

If not all tabs can be displayed in the selected width of the window, a tab with ellipsis (...) is displayed in place of the tabs that cannot be displayed. This allows you to select the tabs that are not shown using a pull-down menu.

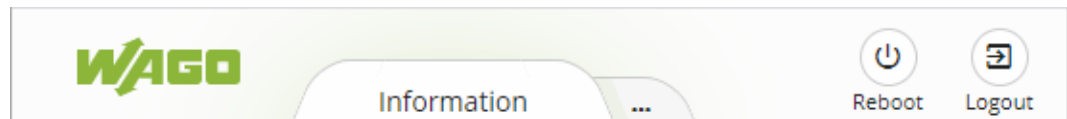


Figure 22: WBM Header with Tabs that Cannot be Displayed (Example)

The navigation tree is shown on the left side of the browser window. The content of the navigation tree depends on the selected tab. You can use this navigation tree to go to the individual pages and, if applicable, their subpages.

The current device status is indicated in the status bar.

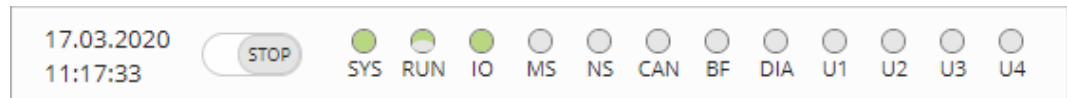


Figure 23: WBM Status Bar (Example)

- Date and time – local time and date on the device
 - Status of the operating mode switch
 - LED status of the device:
The LEDs are labeled with their respective names. The states are symbolized by a graphic. The following representations are possible:
 - Gray: The LED is switched off.
 - Full color: The LED is switched on with the respective color.
 - Half color: The LED is flashing the corresponding color. The other half of the surface is then either gray or also colored. The latter means that the LED is flashing sequentially in different colors.
- A tool tip containing more detailed information opens and remains as long as the cursor is positioned over an LED. The text that is displayed also contains the message that put the LED into its current status. The time of the message is also included.
- The states displayed in the WBM do not always exactly correspond to those on the controller. Data has a runtime during transmission and can only be queried at certain intervals. The time between two queries is 30 seconds.

10.6.2 Configuration with “WAGO Ethernet Settings”

The “WAGO Ethernet Settings” program allows you to read out system information about your controller, make network settings and enable/disable the Webserver.

i Note

Note the software version!

To configure the controller, use at least version 06.15.01, dated 2021-02-08, of “WAGO Ethernet Settings”!

After launching “WAGO ETHERNET Settings,” you must select the corresponding interface.

You can use a suitable USB-C service cable or, if applicable, the IP network for data communication.

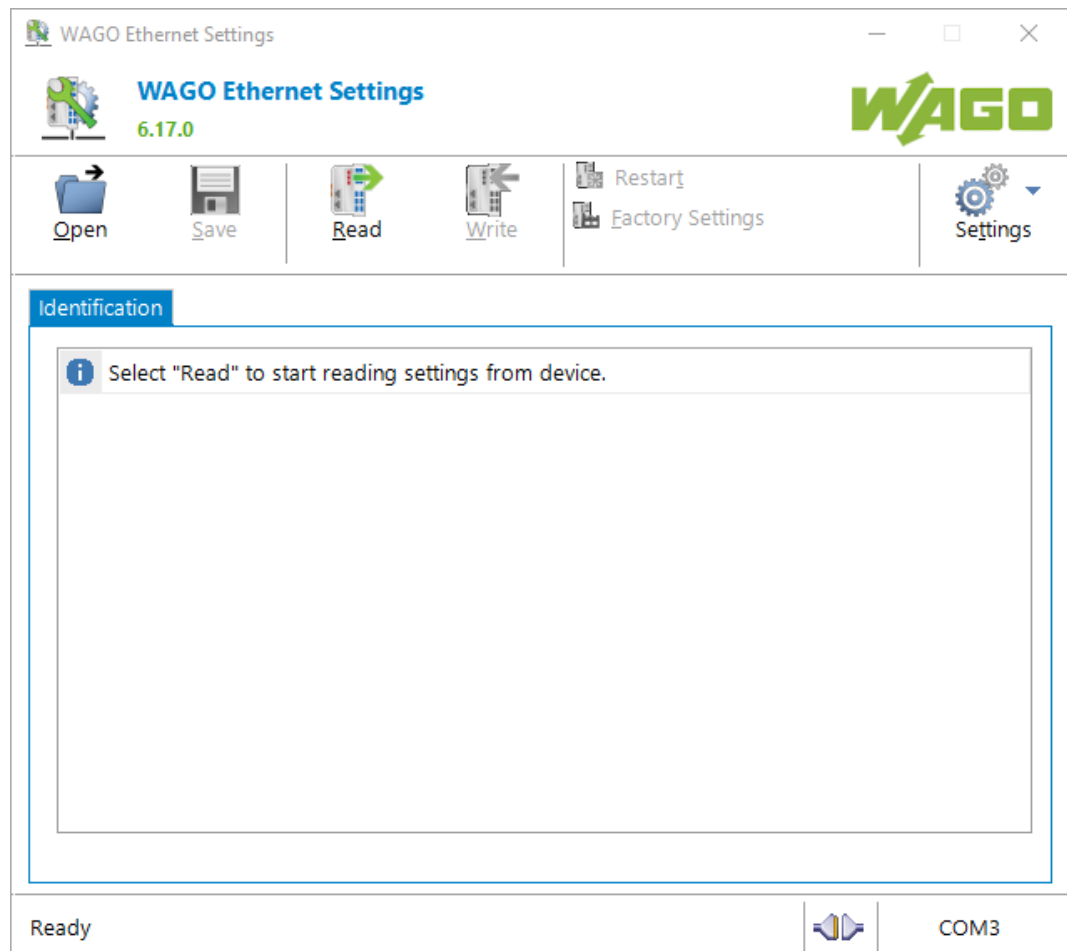
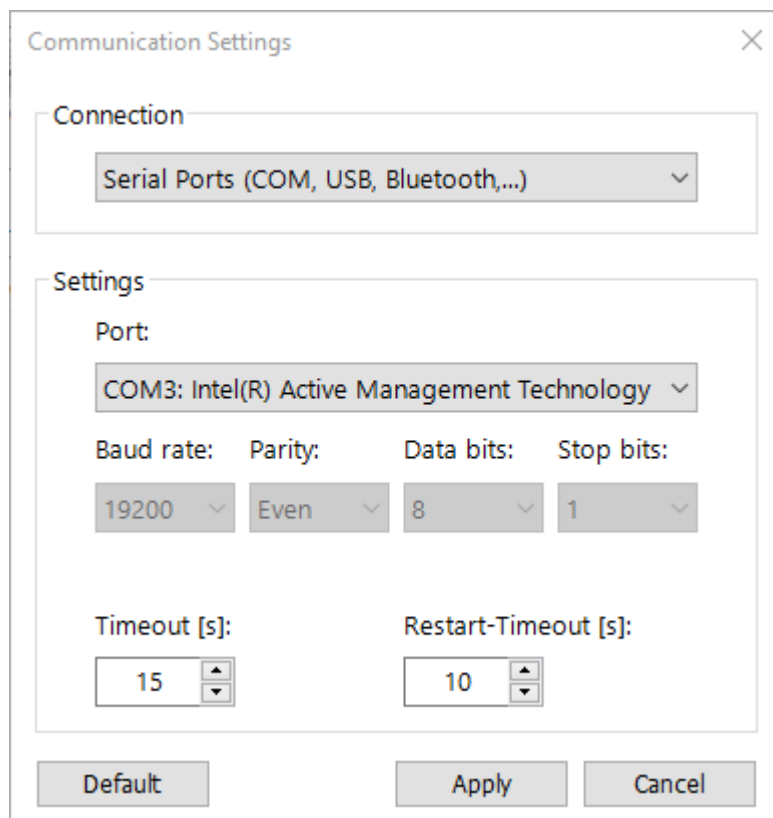


Figure 24: "WAGO Ethernet Settings" – Start Screen (Example)

- To do so, click "Settings" and then "Communication."
- ➔ In the "Communication Settings" window that then opens, modify the settings according to your needs.



Communication Settings

Connection

Serial Ports (COM, USB, Bluetooth,...)

Settings

Port:

COM3: Intel(R) Active Management Technology

Baud rate: 19200 Parity: Even Data bits: 8 Stop bits: 1

Timeout [s]: 15 Restart-Timeout [s]: 10

Default Apply Cancel

Figure 25: "WAGO ETHERNET Settings" – Communication Link (Example)

Once you have configured "WAGO Ethernet Settings" and click **[Apply]**, the connection to the controller is established automatically.

If "WAGO Ethernet Settings" has already been started with the correct parameters, you can establish a connection to the controller by clicking **[Read]**.

10.6.2.1 Identification Tab

An overview of the connected product is given here.

In addition to some fixed values like the item no., MAC address and firmware version, this also indicates the IP address currently in use and the configuration method you used.

Identification	Network	PLC	Status
Item Number	750-8210		
Description	WAGO 750-8210 PFC200 G2 4ETH		
FW Version	04.01.09(00)		
HW Version	01		
FWL Version	2021.10.0w04.00.00 IDX=14		
Serial Number	37SUN31564010260372744+9999999999999999		
MAC address	0030DE46C828		
IP address	192.168.1.10 (Static Configuration)		
Runtime system	CODESYS V3		

Figure 26: "WAGO Ethernet Settings" – Identification Tab (Example)

10.6.2.2 Network Tab

This tab is for configuring network settings.

Values can be changed in the "Input" column, and the parameters actually being used at the time are shown in the "Currently in Use" column.

Identification	Network	PLC	Status																																			
<table> <tr> <th>Parameter</th><th>Edit</th><th>Currently used</th><th>Interface X₁</th></tr> <tr> <td>Address Source</td><td>Static Configuration</td><td>Static Configuration</td><td>Interface X₂</td></tr> <tr> <td>IP address</td><td>192.168.1.10</td><td>192.168.1.10</td><td>Run <u>W</u>BM</td></tr> <tr> <td>Subnet Mask</td><td>255.255.255.0</td><td>255.255.255.0</td><td rowspan="6"> Interfaces ☒ Switched ☐ Separated </td></tr> <tr> <td>Gateway</td><td>0.0.0.0</td><td>0.0.0.0</td></tr> <tr> <td>Preferred DNS-Server</td><td>0.0.0.0</td><td>0.0.0.0</td></tr> <tr> <td>Alternative DNS-Server</td><td>0.0.0.0</td><td>0.0.0.0</td></tr> <tr> <td> Time server</td><td>0.0.0.0</td><td>not available</td></tr> <tr> <td>Hostname</td><td></td><td>PFC200V3-46C828</td></tr> <tr> <td>Domain name</td><td>localdomain.lan</td><td>localdomain.lan</td><td></td></tr> </table>				Parameter	Edit	Currently used	Interface X ₁	Address Source	Static Configuration	Static Configuration	Interface X ₂	IP address	192.168.1.10	192.168.1.10	Run <u>W</u> BM	Subnet Mask	255.255.255.0	255.255.255.0	Interfaces ☒ Switched ☐ Separated	Gateway	0.0.0.0	0.0.0.0	Preferred DNS-Server	0.0.0.0	0.0.0.0	Alternative DNS-Server	0.0.0.0	0.0.0.0	Time server	0.0.0.0	not available	Hostname		PFC200V3-46C828	Domain name	localdomain.lan	localdomain.lan	
Parameter	Edit	Currently used	Interface X ₁																																			
Address Source	Static Configuration	Static Configuration	Interface X ₂																																			
IP address	192.168.1.10	192.168.1.10	Run <u>W</u> BM																																			
Subnet Mask	255.255.255.0	255.255.255.0	Interfaces ☒ Switched ☐ Separated																																			
Gateway	0.0.0.0	0.0.0.0																																				
Preferred DNS-Server	0.0.0.0	0.0.0.0																																				
Alternative DNS-Server	0.0.0.0	0.0.0.0																																				
Time server	0.0.0.0	not available																																				
Hostname		PFC200V3-46C828																																				
Domain name	localdomain.lan	localdomain.lan																																				

Figure 27: "WAGO Ethernet Settings" – Network Tab (Example)

Source

Specify which method the controller should use to determine its IP address: static, via DHCP or via BootP.

IP Address, Subnet Mask, Gateway

Here you can enter the specific network parameters for static configuration.

Note**Restricted setting for default gateways!**

Only default gateway 1 can be set via "WAGO Ethernet Settings." Default gateway 2 can only be set in the WBM!

Preferred DNS Server, Alternative DNS server

Here you can enter the IP address of an accessible DNS server for resolving network names if necessary.

Time Server

Here you can enter the IP address of a time server if the controller is to set its system time via NTP.

Host Name

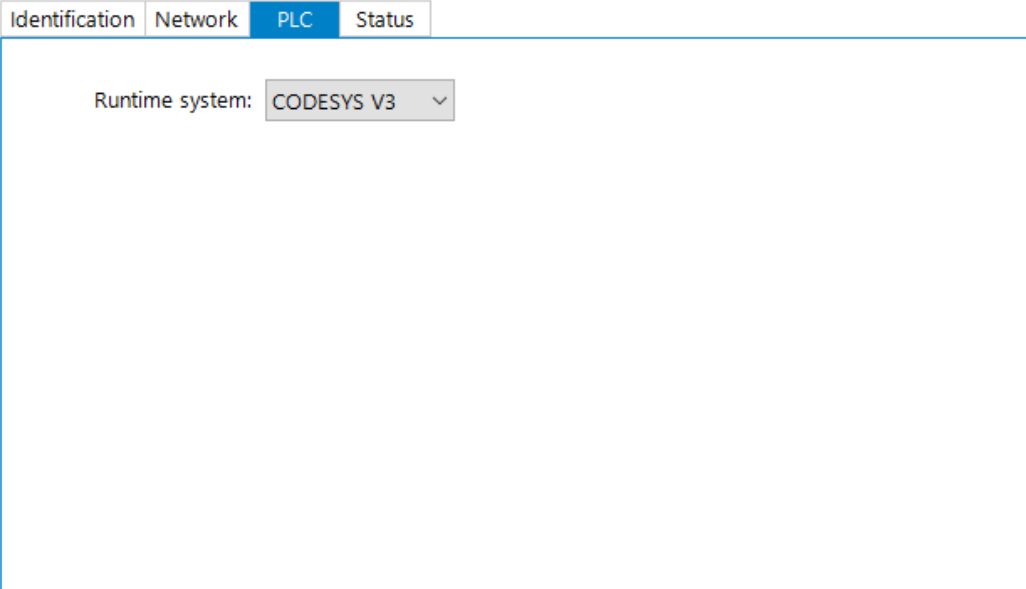
This indicates the controller's host name. Upon delivery, the host name is composed of the string "CC100-" and the last three bytes of the MAC address. This default value is also used whenever the chosen name in the "Input" column is deleted.

Domain Name

This shows the current domain name. This setting can be automatically overwritten with dynamic configurations, e.g., DHCP.

10.6.2.3 PLC Tab

Here you can select the runtime system.



Identification	Network	PLC	Status
Runtime system: CODESYS V3			

Figure 28: "WAGO Ethernet Settings" – Protocol Tab (Example)

10.6.2.4 Status Tab

This shows general information about the controller's status.

Identification

Network

PLC

Status

Status

☐ Field bus active

☐ Write access enabled

☐ Monitor-Mode enabled

☐ Control-Mode enabled

☐ Factory test mode enabled

Blink code

Error code: 0

Argument: 0

No Error

Figure 29: "WAGO Ethernet Settings" – Status Tab (Example)

11 CODESYS V3 Runtime Environment

11.1 Basic Information

Note

Read CODESYS V3 documentation!

Information on installing, commissioning and programming CODESYS V3 is available in the manual for CODESYS V3.

11.2 CODESYS V3 Priorities

A list of priorities implemented for the controller is provided below as supplementary information to the CODESYS V3 documentation.

Table 57: CODESYS V3 Priorities

Scheduler	Task	Linux® Priority	IEC Priority	Comment
Preemptive Scheduling - Real-time area	Local or fieldbus - HIGH	-95 ... -86		Local bus (-88)
	Operating mode switch monitoring	-85		Task registers changes to the mode selector switch and changes the state of the PLC application. (start, stop, reset warm/cold)
	CODESYS Watchdog	-83		Execution of the watchdog functions
	Cyclic and event-controlled IEC task	-55 ... -53	1 ... 3	For real-time tasks which must not be influenced in execution by external interfaces (e.g., fieldbus).
	Local of fieldbus - MID	-52 ... -43		CAN (-52 ... -51) PROFIBUS (-49 ... -45) Modbus slave/master (-43)
	Cyclic and event-controlled IEC task	-42 ... -32	4 ... 14	For real-time tasks which must not influence fieldbus communication during execution.
	Local or fieldbus - LOW	-13 ... -4		
Fair Scheduling - Non-real-time area	CODESYS communication	Background (20)		Communication with the CODESYS development environment
	Cyclic, event-controlled and freewheeling IEC task		15	Incl. standard priority of the visualization task

11.3 Memory Spaces under CODESYS V3

The memory spaces in the controller under CODESYS V3 have the following sizes:

Program memory	32 Mbytes
Data memory	128 Mbytes
Input data	64 kbytes
Output data	64 kbytes
Retain/Persistent	128 kbytes
Function block limitation	12 × 4096 bytes = 48 kbytes

11.3.1 Program and Data Memory

The program memory (also code memory) has a maximum size of 32 MB. The data memory has a maximum size of 128 MB.

Both areas are separate from each other and are requested when downloading to the system depending on the scope of the program. If the size limit is exceeded, it is displayed as an error.

11.3.2 Function Block Limitation

Together with the data memory to be used by the application, memory is required for the individual program function blocks in the system.

The size of the administration space is calculated from the function block limitation * 12 (i.e., 4096 Byte * 12).

The actual size of the main memory required in the system for data is the sum of global program and data memory and function block limitation memory.

11.3.3 Remanent Memory

A total of 128 kbytes of remanent memory is available for the IEC-61131 application.

The remanent area is divided into the retain area and the persistence area. The areas are automatically distributed by CODESYS V3.

12 Diagnostics

12.1 Diagnostics via Indicators

12.1.1 Diagnostics via LED Indicators: System

The "SYS" LED indicates the following diagnostics:

Table 58: "SYS" Diagnostic LED

Status	Explanation	Remedy
Green	Ready for operation; system start completed without errors	---
Orange	Product is in startup/boot process and RST button is not pressed	---
Flashing orange	"Fix IP Address" mode; temporary setting until the next reboot	1. Connect to the product using the default address (192.168.1.17). 2. Restart the product to restore the original value setting.
Flashing green/red	Firmware update mode	---

The "RUN" LED displays the PLC program status with the following diagnostics:

Table 59: "RUN" Diagnostic LED

Status	Explanation	Remedy
Green	Applications loaded and all have status "RUN"	---
Green, flashing	No application and no boot project loaded	▪ Load an application or boot project.
Red	Applications loaded and all have status "STOP"	▪ Set the mode selector switch to "RUN" to start the application.
Green/red, flashing	At least one application with status "RUN" and status "STOP"	▪ Start the stopped application.
Red, one brief off pulse	Warm start reset completed	---
Red, one longer off pulse	Cold start reset completed	---
Red, flashing	At least one application with status "STOP" after exception (e.g., memory access error)	1. Restart the application with a reset via the operating mode switch or in the associated IDE. 2. If the application cannot be started, restart the controller. 3. Contact WAGO Support if the error occurs again.
Orange/green, flashing	Load above threshold value 1	▪ Try to reduce the load on the system: ▪ Change the CODESYS program. ▪ Terminate any fieldbus communication that is not essential, or reconfigure the fieldbuses. ▪ Remove any non-critical tasks from the RT area. ▪ Select a longer cycle time for IEC tasks.

Status	Explanation	Remedy
Orange	Runtime system in debug state (breakpoint, step mode, individual cycle)	1. Resume the application in the associated IDE in step mode or start. If applicable, remove breakpoints. 2. If the connection has been interrupted, set the operating mode switch to "STOP" and then back to "RUN" to allow the application to continue.
Off	No runtime system loaded	• Activate a runtime system, e.g., via the WBM.

The "USR" LED displays the following diagnostics:

Table 60: "USR" Diagnostics LED

Status	Explanation	Remedy
red/green/orange	Programmable status from the user program.	---

12.1.2 Diagnostics via Network LED Indicators

The "LNK|ACT" LED displays the network connection status with the following diagnostics:

Table 61: LNK ACT Diagnostic LED

Status	Explanation	Remedy
Off	No network communication.	• If necessary, check the network connections and network settings.
Green	Existing connection to physical network	---
Flashing green	Network communication occurring.	---

12.1.3 Diagnostics via LED Indicators: Memory Card Slot

The LED for the memory card slot displays the memory card status with the following diagnostics:

Table 62: Memory Card Slot Diagnostic LED

Status	Explanation	Remedy
Off	No read or write access to the memory card	---
Flashing yellow	Read or write access to the memory card	---
Yellow, steady	Read or write access to the memory card	---

12.1.4 Diagnostics via LED Indicators for Digital Inputs and Outputs

The "DI<n>" LEDs display the following diagnostics:

Table 63: Diagnostics LEDs DI<n>

Status	Explanation	Remedy
Off	Digital input <n> is at low potential.	---
Green	Digital input <n> is at high potential.	---

The "DIO<n>" LEDs display the following diagnostics:

Table 64: Diagnostics LEDs DIO<n>

Status	Explanation	Remedy
Off	Digital input/output <n> is at low potential.	---
Green	Digital input/output <n> is at high potential.	---

13 Service

13.1 Clearing Reset Functions

13.1.1 Warmstart Reset

All CODESYS V3 applications are reset during a warm start reset. All global data is set to its initialization values. This corresponds to the CODESYS V3 IDE command "Reset warm."

- To perform a warm start reset, set the mode selector switch to "Reset" and hold it there for two to seven seconds.
- ➔ Execution of the reset is signaled by the red "RUN" LED briefly going out when the mode selector switch is released.

13.1.2 Coldstart Reset

All CODESYS V3 applications are reset during a cold start reset. All global data and the retain variables are set to their initialization values. This corresponds to the CODESYS V3 IDE command "Reset cold."

1. To perform a coldstart reset, set the mode selector switch to "Reset" and hold it there for more than seven seconds.
 - ⇒ Execution of the reset is signaled after seven seconds by the "RUN" LED going out for an extended period.
2. You can then release the mode selector switch.

13.1.3 Software Reset

The product is restarted during a software reset.

- To perform a software reset, set the mode selector switch to the "RUN" or "STOP" position and press the reset button for more than 1 second but less than 8 seconds.
- ➔ All LEDs light up briefly in green to signal reset completion. After a few more seconds, the "SYS" LED signals the successful controller boot operation.

13.1.4 Controller Reset

NOTICE

Do not switch the controller off!

The controller can be damaged by interrupting the factory reset process.

- Do not switch the controller off during the factory reset process and do not disconnect the power supply!

i Note**All parameters and passwords are overwritten!**

With the reset, all parameters and passwords are overwritten.

Saved boot projects, including existing Web visualization data, are deleted.

Post-installed firmware functions are not overwritten.

Software licenses are retained.

- If you have any questions, contact WAGO Support.

To perform a "controller reset," proceed as follows:

1. Press and hold the Reset button.
2. Slide the mode selector switch to the "RESET" position and hold it in this position.
3. Hold both buttons until the "SYS" LED flashes red/green alternately after approx. 8 seconds.
4. If the "SYS" LED flashes red/green alternately, release the mode selector switch and the reset button.

➔ The controller has been reset and restarts automatically.

i Note**Do not interrupt the reset operation!**

If you release the reset button too early, the product restarts without performing the controller reset.

13.2 Inserting and Removing a Memory Card

13.2.1 Inserting a Memory Card

i Note**Note the insertion direction!**

Note the insertion direction when inserting the memory card.

1. Use an operating tool or screwdriver to open the transparent cover flap by folding it upwards. The point where to position the tool is marked with an arrow.
2. Insert the memory card into the slot provided.
3. Push the memory card all the way in. When you let go, the memory card will move back a little and then snap in place (a push-push mechanism).
4. Push the cover flap back in by folding it downwards until it snaps in.
5. You can seal the closed flap through the hole in the enclosure next to the flap.

13.2.2 Removing a Memory Card

1. Remove any seal.

2. Use an operating tool or screwdriver to open the transparent cover flap by folding it upwards. An error indicates where to apply the tool.
3. To remove the memory card, you must first push it slightly into the slot (a push-push mechanism). This releases the mechanical locking mechanism.
4. As soon as you let go of the memory card, the spring pushes the memory card out a bit.
5. Remove the memory card.
6. Push the cover flap back in by folding it downwards until it snaps in.

13.3 Update Root Certificates

If you want to update the root certificates on the controller, proceed as follows:

1. Download the current Root CA bundle from the website <https://curl.haxx.se/ca> to your PC.
2. Rename the file "ca-certificates.crt."
3. Transfer the file to the controller in the /etc/ssl/certs directory using an SFTP or FTP client.
4. Restart the controller. Use the reboot function in the WBM to do this.

13.4 Firmware Updates

! NOTICE

Property damage due to interruption!

Interrupting the update process can damage the product.

- Complete the update/downgrade process!

i Note

Have the matching documentation ready for the target firmware version!

A firmware update can modify, remove or add controller properties and functions. As a result, described properties or functions of the controller may not be available or available properties or functions may not be described in the documentation.

1. Therefore, use only documentation appropriate for the target firmware after an update.
2. If you have any questions, contact WAGO Support.

i Note

Note the firmware version!

The product is compatible with firmware 19 or higher.

Downgrading to a version $\leq$ firmware 19 is not permitted.

You can update the firmware in two different ways using:

- WAGOupload

- Memory card and WBM

13.4.1 Using WAGOupload to Update/Downgrade Firmware

1. Launch WAGOupload.
 2. Click the **[Update Firmware]** action.
 3. In the "Select target controllers" dialog, enter the IP address of your controller in the "Transfer via TCP/IP" option.
 4. Click **[Find Controller]**.
 - ⇒ Your controller is now displayed in the list.
 5. Select the displayed controller and click **[Next]**.
 6. In the "Select Update File" dialog, select the *.wup firmware file for the required firmware.
 7. Click **[Next]**.
 8. Click **[Next]** to confirm the summary.
 9. Wait until the operation ends with a status message and only then click **[Exit]** to close the window.
- ➔ The newly installed firmware is now available on your controller.

13.4.2 Using a Memory Card and WBM to Update/Downgrade Firmware

1. First, copy the firmware image file of the required firmware (*.img) to the memory card using a suitable PC tool.
 2. Save your application and the controller settings.
 3. Switch off the controller.
 4. Insert the memory card with the firmware image to install into the memory card slot.
 5. Switch on the controller.
 - ⇒ The controller is started from the memory card with the firmware image to be installed.
 6. After booting the controller, open the WBM "Administration"> "Create Boot Image" page (you may have to change the IP address temporarily for this).
 7. Create a new boot image on the internal memory. Click the **[Start Copy]** button.
 8. Switch off the controller after completing the operation.
 9. Remove the memory card.
 10. Switch on the controller again.
- ➔ The controller now starts from the internal memory with the newly installed firmware version.

14 Decommissioning

14.1 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.

15 Appendix

15.1 WBM Pages

The following sections contain a description of the parameters and setting options for the Web-Based Management (WBM) pages.

15.1.1 "Information" Tab

15.1.1.1 "Device Status" Page

The "Device Status" page shows information about product identification and the most important network properties.

"Device Details" Group

The product properties are displayed in this group.

Table 65: WBM "Device Status" Page – "Device Details" Group

Parameters	Explanation
Product Description	Product Designation
Order Number	Product Item Number
Unique Item Identifier (UII)	Unique product identification number
License Information	Notification that the CODESYS runtime system is available
Firmware Revision	Firmware Version

"Network TCP/IP Details" Group

The network and interface properties of the product are displayed in this group.

Table 66: WBM "Device Status" Page – "Network TCP/IP" Group

Parameters	Explanation
DIP Switch Status	Status of the address selector switch; this area only appears if an address selector switch is available.
DIP Switch Mode	Address Selector Switch Setting
	Off (0) IP address assignment via e.g., WBM
	static (1 ... 254) Static IP address assignment via address selector switch
	dhcp (255) Dynamic IP address assignment via DHCP
DIP Switch Value	Set value of the address selector switch
Interface <n>	Currently configured interface; the properties are displayed in a separate area for each configured interface.
Mac Address	MAC address used for product identification and addressing
IP Source	Current reference type of the IP address
	none No IP allocation method is selected; this occurs, for example, if a bridge was added due to changes to the bridge configuration. Select a source in the Configuration tab on the TCP/ IP Configuration page.
	static IP Static IP address assignment
	dhcp Dynamic IP address assignment via DHCP
	bootp Dynamic IP address assignment via BootP (if BootP is supported)

Parameters	Explanation	
	external	The IP address may be assigned by the fieldbus application; this occurs e.g., if the IP address is controlled by the application.
IP Address	Current product IP address	
Subnet Mask	Current product subnet mask	

15.1.1.2 "Vendor Information" Page

You can find the manufacturer and address on the "Vendor Information" page.

15.1.1.3 "PLC Runtime Information" Page

The "PLC Runtime Information" page contains information on the enabled runtime system. You will also find a link here to open WebVisu.

"Runtime" Group

Table 67: WBM "PLC Runtime Information" Page – "Runtime" Group

Parameters	Explanation
Version	Currently enabled runtime system If the runtime system is disabled, "None" is displayed.

"WebVisu" Group

You will find a link that you can use to open WebVisu.

15.1.1.4 "WAGO Software License Agreement" Page

The "WAGO Software License Agreement" page lists the license terms for the WAGO software used in the product.

15.1.1.5 "Open Source Licenses" Page

The license conditions for the open source software used for the product are listed in alphabetical order on the "Open Source Licenses" page.

15.1.1.6 "WBM Third Party License Information" Page

On the "WBM Third Party License Information" page, you can find the license text of the open source licenses that apply to the WBM itself.

15.1.1.7 "Trademarks Information" Page

On the "Trademarks Information" page you will find a list of property and trademark rights.

15.1.1.8 "WBM Version" Page

On the "WBM Version" page, you can find the version information for the various sections ("plug-ins") that the WBM contains. This information may be useful for support if an error is found in the WBM.

15.1.2 "Configuration" Tab

15.1.2.1 "PLC Runtime Configuration" Page

On the "PLC Runtime Configuration" page, you will find the settings for the boot project created with the programming software and the settings for the web visualization created in the runtime system.

"General PLC Runtime Configuration" Group

The runtime system change is effective immediately.

The home directory change only takes effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early.

Table 68: WBM "PLC Runtime Configuration" Page – "General PLC Runtime Configuration" Group

Parameters	Explanation	
PLC Runtime Version	Selection of the enabled PLC runtime system	
	None	No runtime system is enabled.
	CODESYS V3	The CODESYS V3 runtime system is enabled.
Home directory on memory card enabled	Selection of the storage location for the home directory of the runtime system	
	☐	The home directory is stored in the internal memory.
	☒	The home directory is moved to the memory card.
[Submit]	Apply change	

Note

All data is deleted when switching the runtime system.

The runtime system's home directory is completely deleted when switching the runtime system!

Note

Insert a memory card before switching the home directory!

Only the first partition of a memory card can be accessed at /media/sd and can be used as the home directory.

- When moving the home directory to the memory card, insert a memory card formatted to support file system.

"Webserver Configuration" Group

The change applies immediately.

Table 69: WBM "PLC Runtime Configuration" Page – "Webserver Configuration" Group

Parameters	Explanation	
CODESYS 3 Webserver State	Status (enabled/disabled) of the CODESYS V3 Webserver	
Default Webserver	Selection of the page display when only entering the IP address of the product	
	Web-Based Management	The Web-Based Management is displayed.
	WebVisu	The web visualization of the runtime system is displayed.
[Submit]	Apply change	

In its default setting, the WBM is called up when only entering the IP address.

To update the display after switching, enter the IP address again in the address line of the Web browser.

To display the web visualization, the Webserver must be enabled (in WBM under "Ports and Services" > "PLC Runtime Services") and there must be a suitably configured application.

Regardless of the default Webserver setting, the WBM can be called up at any time with "https://<IP address>/wbm" and the Web visualization with "https://<IP address>/webvisu".

Note

Possible error messages when calling up the web visualization

The "500 – Internal Server Error" message indicates that the Webserver is not enabled. A page with the header "WebVisu not available" means that no application has been loaded in the product using web visualization.

15.1.2.2 "TCP/IP Configuration" Page

The TCP/IP settings for the ETHERNET interfaces are shown on the "TCP/IP configuration" page.

"Bridge Interfaces" Group

The properties are displayed in a separate area for each configured bridge.

Table 70: WBM "TCP/IP Configuration" Page – "Bridge Interfaces" Group

Parameters	Explanation
Bridge <n>	Settings for the selected bridge
Current IP Address	Current IP address
Current Subnet Mask	Current subnet mask
Current Default Gateway	IP address of the current default gateway
IP Source	Select IP addressing
	Static IP Static IP addressing
	DHCP Dynamic IP addressing
	BootP Dynamic IP addressing (This option is only displayed if BootP is supported)
Static IP Address	Enter static IP address; The IP address is enabled if "Static IP" is enabled in the IP Source selection field.
Subnet Mask	Enter subnet mask; The subnet mask is enabled if "Static IP" is enabled in the selection field IP Source .
Default Gateway	Enter the IP address of the default gateway
[Submit]	Apply change; The change takes effect immediately.

"Dummy Interfaces" Group

The properties are displayed in a separate area for each configured dummy interface.

Table 71: WBM "TCP/IP Configuration" Page – "Dummy Interfaces" Group

Parameters	Explanation
Dummy <n>	Settings for the selected dummy interface

Parameters	Explanation
Current IP Address	Current IP address
Current Subnet Mask	Current subnet mask
IP Source	Select IP addressing. Static IP Static IP addressing
Static IP Address	Enter static IP address; The IP address is enabled if "Static IP" is enabled in the IP Source selection field.
Subnet Mask	Enter subnet mask; The subnet mask is enabled if "Static IP" is enabled in the selection field IP Source .
[Submit]	Apply change; The change takes effect immediately.

"VLAN Interfaces" Group

The properties are displayed in a separate area for each configured VLAN interface.

Table 72: WBM "TCP/IP Configuration" Page – "VLAN Interfaces" Group

Parameters	Explanation
VLAN <n>	Settings for the selected VLAN interface
Current IP Address	Current IP address
Current Subnet Mask	Current subnet mask
IP Source	Select IP addressing. Static IP Static IP addressing DHCP Dynamic IP addressing
Static IP Address	Enter static IP address; The IP address is enabled if "Static IP" is enabled in the IP Source selection field.
Subnet Mask	Enter subnet mask; The subnet mask is enabled if "Static IP" is enabled in the selection field IP Source .
[Submit]	Apply change; The change takes effect immediately.

"DNS Server" Group

Table 73: WBM "TCP/IP Configuration" Page – "DNS Server" Group

Parameters	Explanation
Enabled	Enabled DNS servers; The index reflects the query order.
Assigned by DHCP	DNS servers assigned by DHCP (or BootP); If no DNS server has been assigned by DHCP (or BootP), "no DNS Servers assigned by DHCP" is displayed.
Assigned by user	Addresses of the DNS servers entered by the user; If no server has been entered, "no DNS Servers configured" is displayed.
[Delete]	Delete selected entry; The button is only displayed if there are entries.
New Server IP	Enter additional DNS server addresses; A maximum of 3 addresses are possible.
[Add]	Add new entry.

15.1.2.3 "Ethernet Configuration" Page

The settings for ETHERNET are located on the "Ethernet Configuration" page.

"Bridge Configuration" Group

Table 74: WBM "Ethernet Configuration" Page – "Bridge Configuration" Group

Parameters	Explanation
Bridge 1 ... <n>	Assignment of physical ports X1 ... X<n> to a logical bridge; click the respective option button to do so. The assignment is marked in color. A port can only be assigned to one bridge at a time.
[Submit]	Apply change; The change takes effect immediately.

"Switch Configuration" Group

Table 75: WBM "Ethernet Configuration" Page – "Switch Configuration" Group

Parameters	Explanation
Port Mirror	Switch on/off mirroring of the data traffic between the ports.
	None Both ETHERNET ports are operating normally.
	X1 All data traffic between X1 and the product is mirrored on X2.
	X2 All data traffic between X2 and the product is mirrored on X1.
Broadcast Protection	Set broadcast limit to protect against overload.
	Disabled No broadcast packet limit
	1 ... 5 % Limits incoming broadcast packets to the selected percentage of the total possible data throughput (10/100 Mbit)
Rate Limit	Set the basic limit for incoming data traffic.
	Disabled No limitation of the incoming data traffic
	64 kbps ... 99 mbps Limits the incoming data traffic to the entered value
[Submit]	Apply change; The change takes effect immediately.

"Ethernet Interface Configuration" Group

Table 76: WBM "Ethernet Configuration" Page – "Ethernet Interface Configuration" Groups

Parameters	Explanation
Interface X<n>	For each interface in the controller, a separate area is displayed.
Enabled	Enable/disable interface.
	☐ The interface is disabled
	☒ The interface is enabled
MAC Learning	Enable/disable "MAC Learning" functionality for the interface
	☐ The "MAC Learning" functionality is disabled
	☒ The "MAC Learning" functionality is enabled
Broadcast Protection Enabled	Enables/disables broadcast protection
	☐ Broadcast protection is disabled
	☒ Broadcast protection is enabled
Multicast Protection Enabled	Enables/disables multicast protection
	☐ Multicast protection is disabled
	☒ Multicast protection is enabled

Parameters	Explanation
Current Speed/Duplex	Current transmission rate and current transmission method
Speed/Duplex	Select transmission rate and transmission method; the drop-down menu is generated according to the device and interface. When "Autonegotiation" is selected, the connection modalities are negotiated automatically between the peer devices.
[Submit]	Apply change; The change takes effect immediately.

15.1.2.4 "Configuration of Host and Domain Name" Page

Settings for the hostname and domain name are possible on this page.

"Hostname" Group

Table 77: WBM "Configuration of Host and Domain Name" Page – "Hostname" Group

Parameters	Explanation
Currently used	Hostname currently used
Configured	Enter optional hostname
[Clear]	Delete optional hostname and restore default
[Submit]	Apply change; The change takes effect immediately.

If a hostname is supplied via a DHCP response, this is enabled in the system. If there are several network interfaces with DHCP, the last received hostname is always valid.

If only the hostname configured here is to be valid, the configuration of the DHCP server must be adapted so that no hostnames are transferred in the DHCP response.

"Domain Name" Group

Table 78: WBM "Configuration of Host and Domain Name" Page – "Domain Name" Group

Parameters	Explanation
Currently used	Currently used domain name
Configured	Enter optional domain name
[Clear]	Delete optional domain name
[Submit]	Apply change; The change takes effect immediately.

If a domain name is supplied via a DHCP response, this is enabled in the system. If there are several server network interfaces with DHCP, the last received domain name is always valid.

If only the domain name configured here is to be valid, the configuration of the DHCP server must be adapted so that no domain names are transferred in the DHCP response.

15.1.2.5 "Routing" Page

On the "Routing" page you can find settings and information on the routing between the network interfaces.

"IP Forwarding through multiple interfaces" Group

Table 79: WBM "Routing" Page – "IP Forwarding through multiple interfaces" Group

Parameters	Explanation
Enabled	Allow forwarding of IP data packets between different network interfaces

Parameters	Explanation	
	☐	Settings under "Static Routes" are applied without allowing IP data packets that reach the controller on one network interface to leave the controller on another network interface.
	☒	IP packets may be forwarded between the interfaces. Additional settings may be required.
[Submit]	Apply change; The change takes effect immediately.	

"Custom Routes" Group

Each configured static route has its own area in the display. If no static routes have been entered, "(no custom routes)" is displayed.

Table 80: WBM "Routing" Page – "Custom Routes" Group

Parameters	Explanation	
Enabled	Using the selected route	
	☐	The route is not used.
	☒	The route is used.
Destination Address	Target address of the subscriber	
	Default	Any network devices can be reached.
	Network Address	Only a specific network device or device from the specified address pool can be reached.
Destination Mask	Subscriber subnet mask If "default" is entered for Destination Address, the value "0.0.0.0" must be entered.	
Gateway Address	Address of the gateway If the "Interface" input field is empty, an entry is required here. If a value is entered in the "Interface" input field, the input here is optional.	
Gateway Metric	Metric of the route When there are multiple routes with the same destination address and destination mask, the metric specifies the gateway to which network data packets are first sent. Priority is given to routes with a lower value for the metric. The lowest value is 0. The highest value is $2^{32} - 1 = 4.294.967.295$.	
Interface	Interface through which the packets sent to the destination address are routed Bridges (br0 ... br3), Modem (wwan0) or VPN interface names can be used. If the "Gateway Address" input field is empty, an entry is required here. If a value is entered in the "Gateway Address" input field, the input here is optional.	
[Submit]	Apply change; The change takes effect immediately.	
[Delete]	Delete selected entry; The button is only displayed if there are entries.	
[Add]	Add new entry.	

"Dynamic Routes (assigned by DHCP)" Group

All default gateways received via DHCP are displayed. Default gateways configured via DHCP are given the metric value 10, which means that they are normally used before the statically configured default gateways.

Each dynamic route has its own area in the display. If no dynamic routes are received via DHCP, "(no dynamic route)" appears.

"IP Masquerading" Group

Each entry has its own area in the display.

Table 81: WBM "Routing" Page – "IP Masquerading" Group

Parameters	Explanation
Enabled	Use IP masquerading
☐	IP masquerading is not used.
☒	IP masquerading is used.
Interface	Select one of the specified names of a network interface Any network interface name can be selected by selecting "other."
[Submit]	Apply change; The change takes effect immediately.
[Delete]	Delete selected entry; The button is only displayed if there are entries.
[Add]	Add new entry.

An entry is only transferred to the system if "Enabled" is enabled in the "General Routing Configuration" group. This allows you to configure a default setting that is not applied until the general switch-on.

"Port Forwarding" Group

Each entry has its own area in the display.

Table 82: WBM "Routing" Page – "Port Forwarding" Group

Parameters	Explanation
Enabled	Use Port Forwarding
☐	Port forwarding is not used.
☒	Port forwarding is used.
Interface	Select one of the specified names of a network interface Any network interface name can be selected by selecting "other."
Port	Select the port on which the product receives network data packets to be forwarded.
Protocol	Select the protocol to be used for port forwarding; TCP, UDP or both protocols can be selected.
Destination Address	Select the network address of the target subscriber This address replaces the original destination address of the network data packet.
Destination Port	Select port number of the target subscriber This value replaces the original destination port of the network data packet.
[Submit]	Apply change; The change takes effect immediately.
[Delete]	Delete selected entry; The button is only displayed if there are entries.
[Add]	Add new entry.

An entry is only transferred to the system if "Enabled" is enabled in the "General Routing Configuration" group. This allows you to configure a default setting that is not applied until the general switch-on.

15.1.2.6 "Clock Settings" Page

On this page, date and time settings are possible.

"Timezone and Format" Group

Table 83: WBM "Clock" Page – "Timezone" Group

Parameters	Explanation
Timezone	Select time zone, default setting:
	AST/ADT "Atlantic Standard Time," Halifax
	EST/EDT "Eastern Standard Time," New York, Toronto
	CST/CDT "Central Standard Time," Chicago, Winnipeg
	MST/MDT "Mountain Standard Time," Denver, Edmonton
	PST/PDT "Pacific Standard Time", Los Angeles, Whitehouse
	GMT/BST "Greenwich Mean Time", GB, P, IRL, IS, ...
	CET/CEST "Central European Time," B, DK, D, F, I, CRO, NL, ...
	EET/EEST "Eastern European Time," BUL, FI, GR, TR, ...
	CST "China Standard Time"
	JST "Japan/Korea Standard Time"
TZ string	Time zone not selectable above: Enter the name of the time zone, country and city Determine the valid name of a time zone: http://www.timeanddate.com/time/map/
Time Format	Time format: 12h / 24h
[Submit]	Apply change; The change takes effect immediately.

"UTC Time and Date" Group

Table 84: WBM "Clock" Page – "UTC Time and Date" Group

Parameters	Explanation
UTC Date	Date
UTC Time	GMT Time
[Submit]	Apply change; The change takes effect immediately.

"Local Time and Date" Group

Table 85: WBM "Clock" Page – "Local Time and Date" Group

Parameters	Explanation
Local Date	Local Date
Local Time	Local Time
[Submit]	Apply change; The change takes effect immediately.

15.1.2.7 "Create bootable Image" Page

You can create a bootable image on the "Create Bootable Image" page.

"Create bootable image from boot device" Group

Once the destination has been determined and output, it is then checked and the results of this check are displayed below the settings.

Table 86: WBM "Create bootable Image" – "Create bootable image from boot device" Group

Parameters	Explanation						
Boot Device	Displays the storage medium from which the system was booted						
Destination	Selection of the target of the image to be created; Depending on which medium has been booted, the following destination is available for selection after boot-up for the image to be generated:						
	<table> <tr> <td>Boot system:</td><td>Target partition for "bootable image":</td></tr> <tr> <td>Memory Card</td><td>Internal Flash</td></tr> <tr> <td>Internal Memory</td><td>Memory Card</td></tr> </table>	Boot system:	Target partition for "bootable image":	Memory Card	Internal Flash	Internal Memory	Memory Card
Boot system:	Target partition for "bootable image":						
Memory Card	Internal Flash						
Internal Memory	Memory Card						
[Start Copy]	Start copy operation ▪ If the outcome of the test is positive, copying begins immediately. ▪ If errors have been detected, a corresponding message is displayed and copying is not started. ▪ If warnings have been issued, these are displayed again and you must then confirm that you still wish to continue.						

- Free space on target device:
If the available memory space is less than 5 % a warning is displayed. You can still start the copy operation despite the warning. If the available space is too low, a corresponding message is displayed and copying cannot be started.
- Device being used by CODESYS:
If the device is being used by CODESYS, a warning is displayed. Although it is not recommended, you can still start the copy operation despite this warning.

15.1.2.8 "Firmware Backup" Page

You can find the controller data backup settings on the "Firmware Backup" page.

"Firmware Backup" Group

Table 87: WBM "Firmware Backup" Page – "Firmware Backup" Group

Parameters	Explanation						
Boot Device	Storage medium from which the device was booted						
Destination	Storage destination for backup						
	<table> <tr> <td>Memory Card</td><td>The data is written to the memory card. This selection only appears if a memory card is inserted and the device has not been booted from the memory card.</td></tr> <tr> <td>USB stick</td><td>The data is written to the USB stick. This selection is only available for products with USB connection. This selection is only enabled if a USB stick is inserted and has not been booted from the USB stick.</td></tr> <tr> <td>Network</td><td>The data is saved in the file system and then made available as a download on the PC.</td></tr> </table>	Memory Card	The data is written to the memory card. This selection only appears if a memory card is inserted and the device has not been booted from the memory card.	USB stick	The data is written to the USB stick. This selection is only available for products with USB connection. This selection is only enabled if a USB stick is inserted and has not been booted from the USB stick.	Network	The data is saved in the file system and then made available as a download on the PC.
Memory Card	The data is written to the memory card. This selection only appears if a memory card is inserted and the device has not been booted from the memory card.						
USB stick	The data is written to the USB stick. This selection is only available for products with USB connection. This selection is only enabled if a USB stick is inserted and has not been booted from the USB stick.						
Network	The data is saved in the file system and then made available as a download on the PC.						
PLC Runtime Project	Save PLC runtime project, boot project and CODESYS settings.						
	<table> <tr> <td>☐</td><td>PLC runtime project is not saved.</td></tr> <tr> <td>☒</td><td>PLC runtime project is saved.</td></tr> </table>	☐	PLC runtime project is not saved.	☒	PLC runtime project is saved.		
☐	PLC runtime project is not saved.						
☒	PLC runtime project is saved.						
Settings	Save device settings.						
	<table> <tr> <td>☐</td><td>Device settings are not saved.</td></tr> <tr> <td>☒</td><td>Device settings are saved.</td></tr> </table>	☐	Device settings are not saved.	☒	Device settings are saved.		
☐	Device settings are not saved.						
☒	Device settings are saved.						

Parameters	Explanation	
System	Save device operating system and root file system.	
	☐	The device operating system and root file system are not saved.
	☒	The device operating system and root file system are saved.
Encryption	Save data encrypted.	
	☐	Data is saved unencrypted.
	☒	Data is saved in encrypted form.
Encryption passphrase	Encryption password The input field only appears if the Encryption checkbox is selected.	
Confirm passphrase	Encryption password for confirmation The input field is only displayed if the Encryption checkbox is selected.	
[Create Backup]	Start backup operation	

Note

Note the firmware version!

Restoring the operating system ("System" selection) is only permitted and possible if the firmware versions are the same at the time of backup and restore.

If necessary, refrain from restoring the operating system or adjust the firmware version to the firmware version at the time of the backup beforehand.

Note

Only one package may be copied to the network!

If you have specified "Network" as the storage location, only one package may be selected for each storing operation.

Note

No backup of the memory card!

Backup from the memory card to the internal flash memory is not possible.

Note

Account for backup time

Generation of backup files can take several minutes. Stop the CODESYS program before you start the backup operation to help shorten the time required.

15.1.2.9 "Firmware Restore" Page

The settings for restoring the controller data are shown on the "Firmware Restore" page.

"Firmware Restore" Group

Table 88: WBM "Firmware Restore" Page – "Firmware Restore" Group

Parameters	Explanation	
Source	Data source for restoration	
	Memory Card	The data is read from the memory card. This selection is only enabled if a memory card is inserted and the device has not been booted from the memory card.
	USB stick	The data is read from the USB stick. This selection is only available for products with USB connection. This selection is only enabled if a USB stick is inserted and has not been booted from the USB stick.
	Network	The data is uploaded from the PC and restored.
Boot Device	Storage medium from which the device was booted	
PLC Runtime Project	Name of the backup file for the CODESYS project; The input field is only enabled if the network is selected as the data source.	
Settings	Name of the backup file for the settings; The input field is only enabled if the network is selected as the data source.	
System	Name of the backup file for the system data and the root file system; The input field is only enabled if the network is selected as the data source.	
Decryption	Data encryption	
	☐	The data has been encrypted and saved.
	☒	The data was saved unencrypted.
Decryption passphrase	Encryption password; The input field is only displayed if the Decryption checkbox is selected.	
[Restore]	Start restore operation	

i Note**Note the firmware version!**

Restoring the operating system ("System" selection) is only permitted and possible if the firmware versions are the same at the time of backup and restore.

If necessary, refrain from restoring the operating system or adjust the firmware version to the firmware version at the time of the backup beforehand.

i Note**File size must not exceed the size of the internal drive!**

Note that the amount of data in the media/sd/copy/ directory must not exceed the total size of the internal drive.

i Note**Restoration only possible from internal memory!**

If the product was booted from the memory card, the firmware cannot be restored.

Note**Reset by restore**

A reset is performed when the system or settings are restored by CODESYS!

Note**Connection loss through restore!**

If the restore changes the parameters of the ETHERNET connection, the WBM may then no longer be able to open a connection to the product.

Call up the WBM again with the correct IP address of the product in the address line.

Note**Account for restore time**

The restore operation takes about 2 ... 3 minutes.

After the restore operation, the controller is restarted and is then ready for use again.

15.1.2.10 "Active System" Page

This page contains settings for selecting the partition from which the system is to be started.

"Boot Device" Group

Table 89: WBM "Active System" Page – "Boot Device" Group

Parameters	Explanation
Booted from	Storage medium from which the system was booted

"System <n> (Internal Flash)" Group

Table 90: WBM "Active System" Page – "System n (Internal Flash)" Group

Parameters	Explanation
Enabled	System activity
Configured	System activity after the next reboot
State	System status
	good Valid system
	bad Invalid system, use for test purposes only
[Activate]	Start the system at the next reboot.

Note**Provide a bootable system!**

A functional firmware backup must be available on the boot system!

15.1.2.11 "Mass Storage" Page

The "Mass Storage" page displays information and settings for the storage media.

The group title contains the designation for the storage media ("Memory Card" or "Internal Flash") and, if this storage medium is also the enabled partition, the text "Active Partition".

"Devices" Group

An area with information on the storage medium is displayed for each storage medium found.

Table 91: WBM "Mass Storage" Page – "Devices" Group

Parameters	Explanation
<Device>	Storage medium
Boot device	This shows whether the device has booted from this storage medium.
Volume name	Name of the storage medium

"Create new Filesystem on Memory Card" Group

Note

Data are deleted!

Any data stored in the storage medium is deleted during formatting.

Table 92: WBM "Mass Storage" Page – "Create new Filesystem on Memory Card" Group

Parameters	Explanation
IP Source	Select the format to be used to recreate the file system on the memory card
	Ext4 The filesystem is created in Ext4 format. The files are not readable under Windows!
	FAT The filesystem is created in FAT format.
Label	Enter the name that the storage medium should receive when formatting
[Start]	Format storage medium

15.1.2.12 "Software Uploads" Page

On "Software Upload" page, you can install software packages on the product from your PC.

Table 93: WBM "Software Uploads" Page – "Upload New Software" Group

Parameters	Explanation
Software File	File name of the selected software package as long as it has not yet been transferred to the product; If you have not yet selected a package, "Choose ipk file ..." appears. In this case, click the input field and select a file with a software package on your PC.
Force install	
[Install]	Installed selected package; The file with the software package is deleted from the product again after the installation process. If this is not possible due to a processing error, it is deleted no later than the next time the product restarts.

15.1.2.13 WBM "Configuration of Network Services" Page

The settings for various services are shown on the "Configuration of Network Services" page.

Note

Close any ports and services that you do not need!

Unauthorized persons may gain access to your automation system through open ports.

1. To reduce the risk of cyber attacks and, thus, enhance your cyber security, close all ports and services in the control components (e.g., port 6626 for WAGO-I/O-CHECK and port 11740 for CODESYS V3) not required by your application.
2. Only open ports and services during commissioning and/or configuration.

"FTP" Group

Table 94: WBM "Configuration of Network Services" Page – "FTP" Group

Parameters	Explanation	
Service enabled	Enable/disable FTP service;	
	☐	The FTP service is disabled; factory setting
	☒	The FTP service is enabled.
[Submit]	Apply change; The change takes effect immediately.	

"FTPES (explicit FTPS)" Group

Table 95: WBM "Configuration of Network Services" Page – "FTPES (explicit FTPS)" Group

Parameters	Explanation	
Service enabled	Enable/disable FTPES (explicit FTPS) service;	
	☐	The FTPES service is disabled; factory setting
	☒	The FTPES service is enabled.
[Submit]	Apply change; The change takes effect immediately.	

"HTTP" Group

Table 96: WBM "Configuration of Network Services" Page – "HTTP" Group

Parameters	Explanation	
Service enabled	Enable/disable HTTP service;	
	☐	The HTTP service is disabled; default setting
	☒	The HTTP service is enabled.
[Submit]	Apply change; The change takes effect immediately.	

Note

Disconnection abort on disabling

If the service is disabled, the connection to the product may be interrupted.

- Open the page again.

"HTTPS" Group

Table 97: WBM "Configuration of Network Services" Page – "HTTPS" Group

Parameters	Explanation	
Service enabled	Status of the HTTPS service	
	☐	The HTTPS service is disabled.
	☒	The HTTPS service is enabled.

"I/O-CHECK" Group

Table 98: WBM "Configuration of Network Services" Page – "I/O-CHECK" Group

Parameters	Explanation	
Service enabled	Enable/disable WAGO I/O-CHECK service;	
	☐	The WAGO I/O-CHECK service is disabled; factory setting
	☒	The WAGO I/O-CHECK service is enabled.
[Submit]	Apply change; The change takes effect immediately.	

15.1.2.14 "Configuration of NTP Client" Page

The settings for the NTP service are shown on the "Configuration of NTP Client" page.

"NTP Client Configuration" Group

Table 99: WBM "Configuration of NTP Client" Page – "NTP Client Configuration" Group

Parameters	Explanation
Service enabled	Enable/disable time update.
Update Interval (sec)	Specify the update interval of the time server.
Time Server <n>	Enter here the IP addresses of up to 4 time servers. Time server No. 1 is requested first of all. If no data is accessible via this server, time server No. 2 is queried, etc.
Additionally assigned (DHCP)	The time servers assigned by DHCP are displayed. If no time server has been assigned by DHCP, "no additional servers assigned" is displayed.

1. Click the **[Update Time]** button to update the time.
 2. Click the **[Submit]** button to apply the change.
- ➔ The change applies immediately.

15.1.2.15 "PLC Runtime Services" Page

The settings for various services of the runtime system are shown on the "PLC Runtime Services" page.

"CODESYS V3" Group

Table 100: WBM "PLC Runtime Services" Page – "CODESYS V3" Group

Parameters	Explanation	
CODESYS V3 State	Status of the runtime system	
	disabled	The runtime system is disabled.

Parameters	Explanation	
	enabled	The runtime system is enabled.
Webserver Enabled	Enable/disable Webserver for Web visualization.	
	☐	The Webserver is disabled.
	☒	The Webserver is enabled.
Separated WebVisu Ports (8080/8081)	Set CODESYS WebVisu ports for HTTP/HTTPS.	
	☐	CODESYS WebVisu is provided on ports 80/443 (standard like WBM).
	☒	The CODESYS WebVisu is provided on ports 8080/8081.
Port Authentication Enabled	Enable/disable log-in for the connection to the device.	
	☐	No log-in is required for the connection.
	☒	A login is required for the connection. The default user name is admin and the password is the password specified under "General Configuration".
Webserver Port Authentication Enabled	Enable/disable log-in for calling up the web visualization of a CODESYS application.	
	☐	No log-in is required to access the web visualization.
	☒	A log-in is required to access the web visualization. The default user name is admin and the password is the password specified under "General Configuration".
[Submit]	Apply change; The change takes effect immediately.	

15.1.2.16 "SSH Server Settings" Page

The settings for the SSH service are shown on the "SSH Server Settings" page.

"SSH Server" Group

Table 101: WBM "SSH Server Settings" Page – "SSH Server" Group

Parameters	Explanation	
Service enabled	Enable/disable SSH Server service.	
	☐	The SSH Server service is disabled.
	☒	The SSH Server service is enabled.
Port Number	Enter the port number.	
Allow root login	Block or allow root access.	
Allow password login	Enable or disable password request.	
[Submit]	Apply change; The change takes effect immediately.	

15.1.2.17 "Status overview" Page

On the "Status overview" page, you can find information about cloud access.

"Connection <n>" Group

A group is displayed for each cloud access.

Table 102: WBM "Overview" Page – "Connection <n>" Group

Parameters	Explanation
Operation	Status of the Cloud Connectivity Application
Data from PLC Runtime	Number of data collections registered by the IEC application for transfer to the cloud
Cloud Connection	Status of the connection to the cloud service
Heartbeat	Currently configured heartbeat interval in seconds
Telemetry Data Transmission	Status of the data transmission
Cache fill level (QoS 1 and 2)	Percentage of the storage level for outgoing messages

15.1.2.18 "Configuration of Connection <n>" Page

Settings and information on cloud access are possible on this page.

A page is displayed for each cloud access.

"Configuration" Group

The parameters indicated depend on the cloud platform setting and, if applicable, on other settings in this group.

The dependencies are shown in a separate table.

Table 103: WBM "Configuration of Connection <n>" Page – "Configuration" Group

Parameters	Explanation
Enabled	Enable/disable cloud connectivity functionality
Cloud platform	Cloud Platform
Hostname	Hostname or IP address for the selected cloud platform
ID Scope	Endpoint for Azure Device Provisioning Service (DPS)
Registration ID	Registration ID for Azure Device Provisioning Service (DPS)
Port number	Port number to which a connection should be established Typical values: 8883 for encrypted connections 1883 for unencrypted connections
Device ID	Device ID for the selected cloud platform
Client ID	Client ID for the selected cloud platform
Authentication	Authentication method, e.g., "Shared Key Access," "X.509 Certificate"
Activation Key	Activation key for the selected cloud platform
Clean Session	Enable clean session when connecting to the cloud service Clean session enabled: Information and messages about this connection are not persistently stored by the cloud service
TLS	Enable/disable use of TLS encryption for the connection to the cloud platform Amazon Web Services (AWS) uses TLS
CA file	Path to the file encoded in PEM format that contains the trusted CA certificate to use to establish an encrypted connection Default: CA certificate /etc/ssl/certs/ca-certificates.crt
User	Username
Password	Password
Certification file	Path to the file encoded in PEM format that is used for cloud service authentication
Key file	Path to the file encoded in PEM format that contains the private key for cloud service authentication

Parameters	Explanation
Use websockets	Enable/disable connection to the cloud platform using the WebSocket protocol via port 443 If disabled: Establishes a connection to the cloud platform using the MQTT protocol via port 8883
HTTP Proxy Host	Hostname or IP address of the proxy
HTTP Proxy Port	Proxy port number
HTTP Proxy User	Name of the proxy user
HTTP Proxy Password	Password of the proxy user
Use compression	Enable/disable data compression via GZIP compression
Data Protocol	Data protocol
Cache mode	Cache location for the data telegrams Only enabled if a correctly formatted SD card is inserted Additional Information: Application Note A500920
Last Will	Enable/disable last will message After enabled, additional input fields appear below
(Last Will) Topic	Topic under which the last will message is to be sent
(Last Will) Message	Message to be sent as last will message
(Last Will) QoS	"Quality of Service" (QoS) of the last will message
(Last Will) Retain	Enable/disable the last will message sent under a topic by the broker as a saved message (retained message)
Device info	Enable/disable device info message that informs the cloud service about the basic configuration of the controller Additional Information: Application Note A500920
Device status	Enable/disable device-status messages that inform the cloud service of changes to the mode selector switch and LEDs Additional Information: Application Note A500920
Standard commands	Enable/disable integrated standard commands Additional Information: Application Note A500920 If disabled: Only supported commands defined in the IEC program
Application property template	Create your own property for the individual MQTT messages to the Azure cloud Parameter optional, i.e., if the field is left blank, this property is not sent Placeholder to create: <m>: Message type <p>: Protocol version <d>: DeviceId Examples: - MyKey=HelloWorld_<m> - TestKey=<m>/<p>/<d> - DeviceId=<d>
[Submit]	Apply change; The change only takes effect after the next restart.

The following tables show the dependencies of the selection and input fields as well as the possible settings.

Table 104: Displays the selection and input fields depending on the cloud platform selected

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT Any-Cloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
Enabled	X	X	X	X	X	X
Cloud platform	X	X	X	X	X	X
Hostname	X	X	X	X	X	
Port Number			X	(X)	X	
Device ID	X	X				
Client ID			X	X	X	
Authentication		X				X
Activation Key	X	X2				X2
Clean Session			X	(X)	X	
TLS			X	(X)	X	
CA file			X	X	X	X
User			X			
Password			X			
Certification file		X2	X	X	X	
Key file		X2	X	X	X	
Use websockets	X	X1				X
Proxy Type	X4	X4				X4
HTTP Proxy Host	X5	X5				X5
HTTP Proxy Port	X5	X5				X5
HTTP Proxy User	X5	X5				X5
HTTP Proxy Password	X5	X5				X5
Data Protocol		X	X	X	(X)	X
Use compression	X	X1	X1			X1
Cache mode	X	X	X	X	X	X
Last Will			X	X	X	
Last Will Topic			X3	X3	X3	
Last Will Message			X3	X3	X3	
Last Will QoS			X3	X3	X3	
Last Will Retain			X3	(X3)	X3	
Device info		X1	X1	X1		X1
Device status		X1	X1	X1		X1
Standard commands		X1	X1	X1		X1
Application property template		X1				X1
X: Visible and enabled						
(X): Visible, but not enabled						
X1: Visible and enabled, depending on the selected data protocol						
X2: Visible and enabled, depending on the selected authentication						
X3: Visible and enabled when "Last Will" is switched on						
(X3): Visible but not enabled when "Last Will" is switched on						
X4: Enabled when "Use websockets" is switched on						
X5: Visible and enabled when "Use websockets" is switched on and when "HTTP" is set as "Proxy Type"						

Table 105: Option for selecting the data protocol depending on the cloud platform selected

Data Protocol	Cloud Platform					
	WAGO Cloud	Azure	MQTT Any-Cloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
WAGO Protocol		X	X	X		X
WAGO Protocol 1.5		X	X	X		X
Native MQTT			X	X	(X)	
Sparkplug payload B		X	X	X		
X: Selection possible						
(X): Fixed setting						

Table 106: Displays the selection and input fields depending on the selected data protocol

Selection or Input Field	Data Protocol			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
Client ID	X	X	X	X
Use compression	X	X	X	
Device info	X	X		
Device status	X	X		
Standard commands	X	X		
Application property template	X	X		
X: Visible and enabled				

Table 107: Option for selecting the cache mode depending on the selected data protocol

Cache mode	Data Protocol			
	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B
RAM	X	X	X	(X)
SD Card	X1	X1	X1	
X: Selection possible				
X1: Selection only possible when "Compression" is not switched on				
(X): Fixed setting				

Table 108: Display of input fields depending on the selected authentication

Selection or Input Field	Authentication	
	Shared Access Key	X.509 Certificate
Activation Key	X	
Certification file		X
Key file		X
X: Visible and enabled		

15.1.2.19 "Configuration of general SNMP parameters" Page

Settings for general settings for SNMP are possible on this page.

"General SNMP Configuration" Group

Table 109: WBM "Configuration of general SNMP parameters" Page – "General SNMP Configuration" Group

Parameters	Explanation	
Service enabled	Enable/disable SNMP service;	
	☐	The SNMP service is disabled.
	☒	The SNMP service is enabled.
Name of Device	Enter product name (sysName).	
Description	Enter product description (sysDescription).	
Physical location	Enter the product location (sysLocation).	
Contact	Enter email contact address (sysContact).	
ObjectID	Enter Object ID.	
[Submit]	Apply change; The change only takes effect after the next restart.	

15.1.2.20 "Configuration of SNMP v1/v2c Parameters" Page

The settings for SNMP v1/v2c are shown on the "Configuration of SNMP v1/v2c Parameters" page.

"Communities" Group

Table 110: WBM "Configuration of SNMP v1/v2c Parameters" Page – "Communities" Group

Parameters	Explanation
Name	Community name for the SNMP manager configuration
Access	Access rights for the community; possible values are: • ReadOnly • ReadWrite
[Delete]	Delete selected entry; The button is only displayed if there are entries.
[Add]	Add new entry.

"Trap Receivers" Group

Table 111: WBM "Configuration of SNMP v1/v2cparameters" Page – "Trap Receivers" Group

Parameters	Explanation
Host	Hostname or IP address of the trap receiver (management station)
Community Name	Community name for the trap receiver configuration
Version	SNMP version via which the traps are to be sent; possible values are: • v1 • v2c
[Delete]	Delete selected entry; The button is only displayed if there are entries.
[Add]	Add new entry.

15.1.2.21 "Configuration of SNMP v3 Parameters" Page

The settings for SNMP v3 are shown on the "Configuration of SNMP v3 Parameters" page.

"Users" Group

Table 112: WBM "Configuration of SNMP v3 Parameters" Page – "Users" Group

Parameters	Explanation
Security Authentication Name	Username
Authentication Type	Authentication type for the SNMP v3 packets; possible values are: - No authentication ("None") - Message Digest 5 ("MD5") - Secure Hash Algorithm ("SHA," "SHA224," "SHA256," "SHA384," "SHA512")
Authentication Key	Password for authentication
Privacy	Encryption algorithm for the SNMP message; possible values are: - No encryption ("None") - Data Encryption Standard ("DES") - Advanced Encryption Standard ("AES," "AES128," "AES192," "AES192C," "AES256," "AES256C")
Privacy Key	Encryption Code
Access	Access rights for the v3 user; possible values are: - ReadOnly - ReadWrite
[Delete]	Delete selected entry; The button is only displayed if there are entries.
[Add]	Add new entry.

"Trap Receivers" Group

Table 113: WBM "Configuration of SNMP v3 Parameters" Page – "Trap Receivers" Group

Parameters	Explanation
Security Authentication Name	Username
Authentication Type	Authentication type for the SNMP v3 packets; possible values are: - No authentication ("None") - Message Digest 5 ("MD5") - Secure Hash Algorithm ("SHA," "SHA224," "SHA256," "SHA384," "SHA512")
Authentication Key	Password for authentication
Privacy	Encryption algorithm for the SNMP message; possible values are: - No encryption ("None") - Data Encryption Standard ("DES") - Advanced Encryption Standard ("AES," "AES128," "AES192," "AES192C," "AES256," "AES256C")
Privacy Key	Encryption Code
Host	Hostname or IP address of the v3 trap receiver
[Delete]	Delete selected entry; The button is only displayed if there are entries.
[Add]	Add new entry.

15.1.2.22 Docker® Settings Page

The settings for the "Docker®" service are shown on the "Docker Settings" page.

"Docker® Status" Group

Table 114: WBM "Docker Settings" Page – "Docker Status" Group

Parameters	Explanation	
Current State	Current status of the "Docker®" service.	
	stopped	The "Docker®" service is stopped.
	running	The "Docker®" service is running.
Service Enabled	Enable/disable "Docker®" service;	
	☐	The "Docker®" is disabled.
	☒	The "Docker®" is enabled.
[Submit]	Apply change; The change takes effect immediately.	

15.1.2.23 "WBM User Configuration" Page

The settings for user administration are displayed on the "WBM User Configuration" page.

"Change Passwords" Group

Note

Change passwords!

The default passwords are documented in these instructions and therefore do not offer adequate protection.

- Change the passwords to meet your particular needs.

Note

Valid characters for passwords

Passwords may contain only the following characters:

lowercase letters (a ... z), uppercase letters (A ... Z), numbers (0 ... 9) and special characters (! " # \$ % & ' () * + , . / : ; < = > ? @ [] ^ _ ` { } | ~ -).

Note

Note the permitted characters for WBM passwords!

If WBM passwords with invalid characters are set outside the WBM system (e.g. via CBM), then accessing the WBM pages is no longer possible.

Table 115: WBM "WBM User Configuration" Page – "Change Passwords" Group

Parameters	Explanation
Old Password	Enter the current password used for authentication.
New Password	Enter new password.
Confirm Password	Enter new password again to check.
[Set Password]	Apply new password

Note

General Rights of WBM Users

The WBM users "admin" and "user" have rights beyond the WBM to configure the system and install software.

15.1.3 "Fieldbus" Tab

15.1.3.1 "OPC UA Configuration" Page

The settings for the OPC UA service are shown on the "OPC UA Configuration" page.

"OPC UA Server Configuration" Group

Table 116: WBM "OPC UA Configuration" Page – "OPC UA Server Configuration" Group

Parameters	Explanation	
Enabled	Enable or disable OPC UA server.	
	☐	The OPC UA server is disabled.
	☒	The OPC UA server is enabled.
Log Level	Select log levels; Selecting the log level affects the response time of the server. Therefore, select only the minimum level required, e.g., "Debug" only for in-depth analyzes. The following values can be set:	
	Error	Only error messages are output.
	Warning	Error messages and warnings are output.
	Info	Error messages, warning messages and status messages are output.
	Debug	Error messages, warning messages, status messages and also debug messages are output.
Ctrl Configuration Name	Enter the configuration name that the controller receives within the PLC Open Device Set.	
[Submit]	Apply change; The change only takes effect after the next restart.	

"OPC UA Server Security Settings" Group

Table 117: WBM "OPC UA Configuration" Page – "OPC UA Server Security Settings" Group

Parameters	Explanation	
Anonymous Access	Block/allow anonymous access to the server.	
	☐	Anonymous access is not permitted.
	☒	Anonymous access is permitted; this requires that port authentication of the runtime is also disabled.
Allow Password In Plain Text	Transfer of password in readable format	
	☐	
	☒	
Security Modes	Security mode of the OPC UA server; depending on the operating mode selected, various OPC UA endpoints are available for establishing a connection.	

Parameters	Explanation	
	None	Only the OPC UA endpoint None is enabled. This allows an unsecured connection to the OPC UA server to be established.
	None + Sign + SignAndEncrypt	The endpoints None , Sign and SignAndEncrypt are available. Sign provides an endpoint that is password protected. SignAndEncrypt provides an endpoint that allows encryption in addition to a password.
	Sign + SignAndEncrypt	The endpoints Sign and SignAndEncrypt are available.
	SignAndEncrypt	Only the endpoint SignAndEncrypt is available.
Security Policies	Selects the security policies; this sets the encryption strength of the OPC UA server. The following options are available: Aes128Sha256RsaOaep and better, Basic256Sha256 and better, Aes256Sha256RsaPss.	
[Submit]	Apply change; The change only takes effect after the next restart.	

15.1.3.2 "BACnet Status" Page

The "BACnet Status" page displays specific information about your product for the BACnet fieldbus and the BACnet license.

"BACnet Information" Group

Table 118: WBM "BACnet Status" Page – "BACnet Information" Group

Parameters	Explanation	
State	BACnet Fieldbus Status	
	☐	Fieldbus BACnet is disabled
	☒	Fieldbus BACnet is enabled
Mode	BACnet operating mode	
	ip	Communication via BACnet/IP
	sc	Communication via BACnet/SC
Version	Installed BACnet version	
Status Info	BACnet Fieldbus Status	
Device-ID	Current product device ID	

"BACnet License" Group

Table 119: WBM "BACnet Status" Page – "BACnet License" Group

Parameters	Explanation
Type	Display of BACnet licenses
User Objects	Display of the number of existing and possible BACnet objects with the license

"BACnet Data Link" Group

Table 120: WBM "BACnet Status" Page – "BACnet Data Link" Group

Parameters	Explanation
Connection Info	Display of the connection status

15.1.3.3 "BACnet Data Link" Page

"Restart" Group

Table 121: WBM "BACnet Data Link" Page – "BACnet Restart" Group

Parameters	Explanation
[Restart]	Restart the BACnet service

"BACnet/IP" Group

Table 122: WBM "BACnet Data Link" Page – "BACnet/IP" Group

Parameters	Explanation
Port Number	Input of the port for BACnet/IP communication
[Submit]	Apply change; The change is only applied after the controller is restarted or after a BACnet restart.

"BACnet/SC" Group

Table 123: WBM "BACnet Data Link" Page – "BACnet/SC" Group

Parameters	Explanation
Mode	Selection of the BACnet/SC operating mode
	regular The device is operated as a BACnet/SC node.
	primary The device is operated as a BACnet/SC Primary HUB.
	failover The device is operated as a BACnet/SC Failover HUB.
Port Number	Input of the port for BACnet/SC communication
Primary Hub URI	Input of the URI for the primary HUB; wss://<IP address>:<port of the HUB> or wss://<domain name>:<port of the HUB> (e.g., wss://192.168.178.19:47808 or wss://PFC200V3-XXXXXX.localdomain.lan:47808)
Failover Hub URI	Enter the URI for the failover HUB; wss://<IP address>:<port of the HUB> or wss://<domain name>:<port of the HUB> (e.g., wss://192.168.178.19:47808 or wss://PFC200V3-XXXXXX.localdomain.lan:47808)
Allow self-signed certificates	Enable/disable whether communication can be established via self-signed certificates.
Allow expired Certificates	Enable/disable whether communication via expired certificates can be established.
Allow any Certificates	Enable/disable whether communication can be established via any certificates.
[Submit]	Apply change; The change is only applied after the controller is restarted or after a BACnet restart.

"BACnet/SC Certificate Authority (CA)" Group

Table 124: WBM "BACnet Data Link" Page – "BACnet/SC Certificate Authority (CA)" Group

Parameters	Explanation
Chose file ...	Select the CA certificate on the computer for transfer to the device
[Upload]	Transfer of the selected CA certificate to the device; after restart, this certificate is used as the CA certificate for BACnet/SC communication.

"BACnet/SC Certificate" Group

Table 125: WBM "BACnet Data Link" Page – "BACnet/SC Certificate" Group

Parameters	Explanation
Chose file ...	Select the device certificate on the computer for transfer to the device
[Upload]	Transfer of the selected device certificate to the device; after restart, this certificate is used for BACnet/SC communication.

"BACnet/SC Certificate Signing Request (CSR)" Group

Table 126: WBM "BACnet Configuration" Page – "BACnet/SC Certificate Signing Request (CSR)" Group

Parameters	Explanation
Country	Enter the country for the CSR or device certificate (two letters)
State	State entry for the CSR or device certificate
Locality	Enter the location for the CSR or device certificate
Organization	Entering the company or organization for the CSR or for the device certificate
Organizational Unit	Entering the department for the CSR or for the device certificate
Common Name	Enter the device name for the CSR or for the device certificate
[Generate]	Generate a CSR and a new private key on the device
[Download]	Download CSR from device

"BACnet/SC Default Certificates" Group

Table 127: WBM "BACnet Data Link" Page – "BACnet/SC Default Certificates" Group

Parameters	Explanation
[Generate]	Generation of a new certificate

15.1.3.4 "BACnet Configuration" Page

You can make special settings for the BACnet fieldbus on this page.

"Restart" Group

Table 128: WBM "BACnet Data Link" Page – "BACnet Restart" Group

Parameters	Explanation
[Restart]	Restart the BACnet service

"BACnet Service" Group

Table 129: WBM "BACnet Configuration" Page – "BACnet Service" Group

Parameters	Explanation
Service enabled	Enable/disable fieldbus BACnet.
	☐ BACnet is disabled.
	☒ BACnet is enabled.
Mode	Select the BACnet operating mode here.
	ip Communication via BACnet/IP
	sc Communication via BACnet/SC
Who-Is online interval time (sec)	Time interval between controller requests to the fieldbus and which other subscribers are online (minimum: 60 sec).
Broadcast I-Am answer	Enable/disable the device's I-Am messages to be sent to the BACnet broadcast address.
	☐ I-Am messages are not sent to the BACnet broadcast address.

Parameters	Explanation	
	☒	I-Am messages are sent to the BACnet broadcast address.
[Submit]	Apply change; The change is only applied after the controller is restarted or after a BACnet restart.	

"BACnet Data" Group

Table 130: WBM "BACnet Configuration" Page – "BACnet Data" Group

Parameters	Explanation	
Delete Persistence Data	Persistent BACnet data is deleted on the next restart.	
Reset all BACnet Data and Settings to Default	BACnet-specific settings and data are reset to factory settings the next time you restart.	
[Submit]	Apply change; The change is only applied after the controller is restarted or after a BACnet restart.	
override.xml Chose file ...	Select the required file on the PC	
[Upload]	Transfer the selected file from the PC to the controller	

"BACnet Log Level" Group

Table 131: WBM "BACnet Configuration" Page – "BACnet Log Level" Group

Parameters	Explanation	
Error	Enable/disable error log outputs.	
	☐	Error log entries are not output.
	☒	Error log entries are output.
Warning	Enable/disable warning log outputs.	
	☐	Warning log entries are not output.
	☒	Warning log entries are output.
Info	Enable/disable info log output.	
	☐	Info log entries are not output.
	☒	Info log entries are output.
Debug	Enable/disable debug log output.	
	☐	Debug log entries are not output.
	☒	Debug log entries are output.
[Submit]	Apply change; The change is only applied after the controller is restarted or after a BACnet restart.	

"BACnet Network Capture" Group

Table 132: WBM "BACnet Configuration" Page – "BACnet Network Capture" Group

Parameters	Explanation	
Enable	Enable/disable logging of network traffic with the corresponding BACnet filters.	
	☐	Network traffic is not logged.

Parameters	Explanation	
	☒	Network traffic is being logged.
Log pre-master secrets	Enable/disable saving of secrets for decryption of BACnet/SC network traffic.	
	☐	Secrets are not saved.
	☒	Secrets are saved.
[Submit]	Apply change; The change is only applied after the controller is restarted or after a BACnet restart.	
BACnet Network Capture Archive [Download]	Click the [Download] button to download the logged network traffic, including the secrets, from the device if the option is enabled.	

15.1.3.5 "BACnet Storage Location" Page

You can make settings for saving the BACnet-specific parameters on the "BACnet Storage Location" page.

"BACnet Persistence" Group

Table 133: WBM "BACnet Storage Location" Page – "BACnet Persistence" Group

Parameters	Explanation	
Storage Location	Select the storage location for the persistence data; selection is only possible if both storage locations are available.	
	Internal Flash	Data will be stored in the controller's internal memory.
	SD Card	The data is saved to the memory card. If "SD card" is selected, but the memory card is no longer inserted, this option is no longer enabled and only "Internal Flash" can be selected.
[Submit]	Apply change; The change takes effect immediately.	

"BACnet Trendlog" Group

Table 134: WBM "BACnet Storage Location" Page – "BACnet Trendlog" Group

Parameters	Explanation	
Storage Location	Select the storage location for the trend log data; selection is only possible if both storage locations are available.	
	Internal Flash	Data will be stored in the controller's internal memory.
	SD Card	The data is saved to the memory card. If "SD card" is selected, but the memory card is no longer inserted, this option is no longer enabled and only "Internal Flash" can be selected.
[Submit]	Apply change; The change takes effect immediately.	

"BACnet Eventlog" Group

Table 135: WBM "BACnet Storage Location" Page – "BACnet Eventlog" Group

Parameters	Explanation	
Storage Location	Select the storage location for the event log data; selection is only possible if both storage locations are available.	
	Internal Flash	Data will be stored in the controller's internal memory.

Parameters	Explanation	
	SD Card	The data is saved to the memory card. If "SD card" is selected, but the memory card is no longer inserted, this option is no longer enabled and only "Internal Flash" can be selected.
[Submit]	Apply change; The change takes effect immediately.	

15.1.3.6 "BACnet Info" Page

The settings for displaying BACnet specific information are shown on the "BACnet Info" page.

"Refresh Options" Group

Table 136: WBM "BACnet Info" Page – "Refresh Options" Group

Parameters	Explanation
Automatic refresh interval (sec)	Switch cyclic refresh on/off; Enter the cycle time in seconds at which a cyclic refresh is performed; Depending on the status, the button label changes ("Refresh"/"Start"/"Stop").
[Refresh]	Refresh display; The button is only displayed if cyclic refresh is not enabled.
[Start]	Start cyclic refresh; The button is only displayed if cyclic refresh is enabled and has not yet started.
[Stop]	Stop cyclical update; The button is only displayed if cyclic update is enabled.

The cyclical refresh is performed for as long as the "BACnet Info" page is open. If you change the WBM page, the update is stopped until you call up the "BACnet Info" page again.

"BACnet/IP Statistics" Group

Table 137: WBM "BACnet Info" Page – "BACnet/IP Statistics" Group

Parameters	Explanation
BACnet/IP Statistics	BACnet/IP Statistics If no data is available, "no data available or retrieved" is displayed.

"BACnet/SC Statistics" Group

Table 138: WBM "BACnet Info" Page – "BACnet/SC Statistics" Group

Parameters	Explanation
BACnet/SC Statistics	BACnet/SC Statistics If no data is available, "no data available or retrieved" is displayed.

"BACnet/SC Connections" Group

Table 139: WBM "BACnet Info" Page – "BACnet/SC Connections" Group

Parameters	Explanation
BACnet/SC Connections	BACnet/SC Connections If no data is available, "no data available or retrieved" is displayed.

15.1.4 "Security" Tab

15.1.4.1 "OpenVPN / IPsec" Page

Note

Potential security vulnerability with VPN protocols!

By default, VPN protocols offer the option of executing hook scripts. This represents a potential security vulnerability.

1. If you are not making use of the hook protocol option, switch it off in the configuration. To do this, edit the corresponding configuration file.
2. To disable the use of hook commands in OpenVPN, use the command `--script-security level 1` in the "openvpn.conf" configuration file.
For more information, see www.openvpn.net/community-resources/reference-manual-for-openvpn-2-5/#scripting-integration.
3. To disable the use of hook commands in IPsec, use the command `--disable-updown` in the "ipsec.conf" configuration file.
For more information, see www.wiki.strongswan.org/projects/strongswan/wiki/Updown/.

The "OpenVPN / IPsec" page displays the settings for OpenVPN and IPsec.

"OpenVPN" Group

Table 140: WBM "OpenVPN / IPsec" Page – "OpenVPN" Group

Parameters	Explanation
Current State	Current status of the OpenVPN service
	stopped The service is disabled.
	running The service is enabled.
OpenVPN enabled	Enable/disable OpenVPN service
openvpn.conf	Select the OpenVPN configuration file to be transferred from the PC to the product or vice versa
[Submit]	Apply change; The change only takes effect after the next restart.
Choose file ...	Select file on product or PC
[Upload]	Transfer selected file from PC to product
[Download]	Transfer selected file from product to PC

"IPsec" Group

Table 141: WBM "OpenVPN / IPsec" Page – "IPsec" Group

Parameters	Explanation
Current State	Current status of the IPsec service
	stopped The service is disabled.
	running The service is enabled.
IPsec enabled	Enable/disable IPsec service
ipsec.conf	Select the IPsec configuration file to be transferred from the PC to the product or vice versa
ipsec.secrets	Select the IPsec secrets file to be transferred from the PC to the product or vice versa

Parameters	Explanation
[Submit]	Apply change; The change only takes effect after the next restart.
Choose file ...	Select file on product or PC
[Upload]	Transfer selected file from PC to product
[Download]	Transfer selected file from product to PC

15.1.4.2 "General Firewall Configuration" Page

The "General Firewall Configuration" page displays the global firewall settings.

"Global Firewall Parameter" Group

Table 142: WBM "General Firewall Configuration" Page – "Global Firewall Parameter" Group

Parameters	Explanation
Firewall enabled entirely	Enable/disable all firewall functionality This setting is the highest priority. If the firewall is disabled, all other settings have no direct effect. It is still possible to configure the other parameters so that the firewall parameters can be set correctly before the firewall is enabled. This setting is independent of the "Filter enabled" setting in the "MAC address filter state bridge <n>" group on the "MAC address filter state bridge <n>" page.
ICMP echo broadcast protection	Enable/disable "ICMP echo broadcast" protection
Max. UDP connections per second	Enter the maximum number of UDP connections per second
Max. TCP connections per second	Enter the maximum number of TCP connections per second
[Submit]	Apply change; The change takes effect immediately.

Note

CODESYS services are rejected when the firewall is switched on without a user filter!

If CODESYS services (e.g., Modbus, OPC-UA, SNMP or IIOT) are used, user filters for these services must be set up in the firewall configuration. The user filters must be configured to accept the corresponding ports.

15.1.4.3 "Interface Configuration" Page

The individual interfaces for the firewall settings are displayed on the "Interface Configuration" page.

"Firewall Configuration Bridge <n> / VPN" Group

A separate group is displayed for each configured bridge.

The settings in this group are based on the firewall configuration on the IP level.

Table 143: WBM "Interface Configuration" Page – "Firewall Configuration Bridge <n> / VPN / WAN" Group

Parameters	Explanation
Firewall enabled for Interface	Enable/disable firewall for the respective interface
ICMP echo protection	Enable/disable "ICMP echo" protection for the respective interface
ICMP echo limit per second	Enter the maximum number of "ICMP pings" per second. "0" = "Disabled"
ICMP burst limit (0=disabled)	Enter the maximum number of "ICMP echo burst" per second

Parameters	Explanation
Service Configuration	Enable/disable firewall for the respective service
FTP/FTPS	Not every service shown here is available for every product. The services themselves must be enabled or disabled separately on the "Ports and Services" page.
FTPS (implicit)	
HTTP	
HTTPS	
I/O Check	
PLC Runtime	
WebVisu - HTTP (port 8080)	
WebVisu - HTTPS (port 8081)	
SSH	
SNMP	
OPC UA (port 4840)	
BACnet (port 47808)	
PROFINET IO	
DNP3 (port 20000)	
IEC60870-5-104 (port 2404)	
IEC61850 (port 102)	
[Submit]	Apply change; The change takes effect immediately.

The firewall ports listed in the following table are open by default on controllers with telecontrol functionality. The corresponding telecontrol services can be executed via these ports without the firewall blocking their communication.

Table 144: Ports for Telecontrol Functionality

Protocol	Port
DNP3	20000
IEC60870-5-104	2404
IEC61850	102

15.1.4.4 "Configuration of MAC address filter" Page

You set the firewall configuration at ETHERNET level on this page.

The "MAC Address Filter Whitelist" contains two default entries with the following values:

- Description: All WAGO devices
MAC address: 00:30:DE:00:00:00
MAC mask: ff:ff:ff:00:00:00
- Description: Enable docker bridges
MAC address: 02:42:00:00:00:00
MAC mask: ff:ff:00:00:00:00

If you enable the first default entry, this already allows communication between different WAGO products in the network.

Note

Enable the MAC address filter before activation!

Before activating the MAC address filter, you must enter and activate your own MAC address in the "MAC Address Filter Whitelist." Otherwise you cannot access the product via the ETHERNET. This also applies to other services used by your product, e.g., IP configuration via

DHCP.

If the MAC address of your DHCP server is not included in the "MAC Address Filter Whitelist", your product will lose its IP settings after the next update cycle and will then also no longer be accessible.

As long as there is no entry in the "MAC Address Filter Whitelist", switching on the filter is prevented.

If at least one enabled address is active, you will receive a corresponding warning before activation, which you have to confirm.

The check described above is only carried out in the WBM, not in the CBM!

"Global MAC address filter state" Group

Table 145: WBM "Configuration of MAC address filter" Page – "Global MAC address filter state" Group

Parameters	Explanation
Filter enabled	Enable/disable global MAC address filter
[Submit]	Apply change; The change takes effect immediately.

"MAC address filter state Bridge <n>" Group

A separate group is displayed for each configured bridge.

Table 146: WBM "Configuration of MAC address filter" Page – "MAC address filter state Bridge <n>" Group

Parameters	Explanation
Filter enabled	Enable/disable MAC address filter for the respective bridge; This setting is independent of the "Firewall enabled entirely" setting in the "Global Firewall Parameters" group on the "General Firewall Configuration" page.
[Submit]	Apply change; The change takes effect immediately.

"MAC address filter whitelist" Group

Table 147: WBM "Configuration of MAC address filter" Page – "MAC address filter whitelist" Group

Parameters	Explanation
Description	Description of the devices or areas that can be enabled by enabling the filter when the firewall is generally enabled. The description is only displayed for entries initially available in the factory default settings.
MAC address	MAC address of the list entry
MAC mask	MAC mask of the list entry
Filter enabled	Enable/disable filter for the list entry
[Submit]	Apply change; The change takes effect immediately.
[Delete]	Delete selected entry; The button is only displayed if there are entries.
[Add]	Add new entry.

15.1.4.5 "Configuration of User Filter" Page

The "Configuration of User Filter" page displays the settings for user-specific firewall filters.

"User Filter" Group

Each configured filter has its own area in the display.

Table 148: WBM "Configuration of User Filter" Page – "User Filter" Group

Parameters	Explanation	
Policy	Allow/exclude network subscribers through the filter	
	Allow	The network device is permitted.
	Drop	The network device is excluded.
Source IP address	Source IP address for the filter	
Source Netmask	Source network mask for the filter	
Source Port	Source port number for the filter	
Destination IP address	Destination IP address for the filter	
Destination Netmask	Target network mask for the filter	
Destination Port	Destination port number for the filter	
Protocol	Protocols for the filter	
	TCP/UDP	The TCP service and UDP service are filtered.
	TCP	The TCP service is filtered.
	UDP	The UDP service is filtered.
Input Interface	Interfaces for the filter	
	Any	All interfaces are filtered.
	Bridge <n>	The interfaces assigned for bridge <n> are filtered. Only the configured bridges are displayed.
	VPN	The VPN interface is filtered.
[Submit]	Apply change; The change takes effect immediately.	

Note

CODESYS services are rejected when the firewall is switched on without a user filter!

If CODESYS services (e.g., Modbus, OPC-UA, SNMP or IIOT) are used, user filters for these services must be set up in the firewall configuration. The user filters must be configured to accept the corresponding ports.

15.1.4.6 "Certificates" Page

You find certificate settings on this page.

"Installed Certificates" Group

Table 149: WBM "Certificates" Page – "Installed Certificates" Group

Parameters	Explanation
<certificate name>	Loaded certificates; If no certificate has been loaded, "No certificates existing" is displayed.
[Delete]	Delete selected entry; The button is only displayed if there are entries.
Choose file ...	Select file on the PC
[Upload]	Transfer selected file from PC to product

The certificates are stored in the `"/etc/certificates/"` directory.

"Installed Private Keys" Group

Table 150: WBM "Certificates" Page – "Installed Private Keys" Group

Parameters	Explanation
<private key name>	Loaded key; If no key has been loaded, "No private keys existing" is displayed.
[Delete]	Delete selected entry; The button is only displayed if there are entries.
Choose file ...	Select file on the PC
[Upload]	Transfer selected file from PC to product

The keys are stored in the "/etc/certificates/keys/" directory.

15.1.4.7 "Boot Mode Configuration" Page

See the "Boot mode configuration" page for boot option settings.

i Note

If you force booting from the internal flash, the device can no longer be booted from the memory card!

If a connection via ETHERNET is no longer possible due to problems or incorrect configuration, you have the option of making the product accessible again via the service interface and "WAGO Ethernet Settings".

"Force internal boot" Group

Table 151: WBM "Boot Mode Configuration" Page – "Force Internal Boot" Group

Parameters	Explanation
Boot mode	Set the boot option for the product
	Memory card or internal flash You can boot from the internal flash or from the memory card.
	Internal flash only You can only boot from the internal flash.
[Submit]	Apply change; The change takes effect immediately.

15.1.4.8 "Security Settings" Page

This page displays the network security settings.

"TLS Configuration" Group

Table 152: WBM "Security Settings" Page – "TLS Configuration" Group

Parameters	Explanation
TLS Configuration	Set permitted TLS versions and cryptographic procedures for HTTPS
	Extended Compatibility The Webserver allows TLS 1.3, as well as TLS 1.2 with less powerful cryptographic methods.
	Strong The Webserver only allows TLS 1.3 and strong algorithms.
[Submit]	Apply change; The change takes effect immediately.

Note

BSI TR-02102 Technical Guideline

The rules for the TLS settings are based on the TR-02102 Technical Guideline of the German Federal Office for Information Security.

The Guideline is available from: www.bsi.bund.de.

15.1.4.9 "Advanced Intrusion Detection Environment (AIDE)" Page

The network security settings are available on the "Advanced Intrusion Detection Environment (AIDE)" page.

"Run AIDE check at startup" Group

Table 153: WBM "Advanced Intrusion Detection Environment (AIDE)" Page – "Run AIDE check at startup" Group

Parameters	Explanation	
Service enabled	Enable/disable "AIDE check" when starting the controller.	
	☐	"AIDE check" is not enabled at startup.
	☒	"AIDE check" is enabled at startup.
[Submit]	Apply change; The change takes effect immediately.	

"Control AIDE and show log" Group

Table 154: WBM "Advanced Intrusion Detection Environment (AIDE)" Page – "Control AIDE and show log" Group

Parameters	Explanation	
Select Action	Select the action to be executed.	
	readlog	The log data are displayed.
	init	The database is initialized and filled with the current values.
	check	The current values are compared against the values stored in the database.
	update	The current values are compared with the values stored in the database and the database then updated.
Read only the last n	Switch display of the last n messages on/off; enter the number of messages displayed.	
Automatic refresh interval (sec)	Switch cyclic refresh on/off; Enter the cycle time in seconds at which a cyclic refresh is performed; Depending on the status, the button label changes ("Refresh"/"Start"/"Stop").	
[Refresh]	Refresh display; The button is only displayed if cyclic refresh is not enabled.	
[Start]	Start cyclic refresh; The button is only displayed if cyclic refresh is enabled and has not yet started.	
[Stop]	Stop cyclical update; The button is only displayed if cyclic update is enabled.	

The cyclical refresh is performed for as long as the "Advanced Intrusion Detection Environment (AIDE)" page is open. If you change the WBM page, the refresh is stopped until you call up the "Advanced Intrusion Detection Environment (AIDE)" page again.

The messages are displayed below the settings.

15.1.4.10 "WAGO Device Access" Page

On the "WAGO Device Access" page, you can find settings for authentication during node scanning.

Note

Beta Status

In the present firmware version, the "WAGO Device Access" functionality is still in beta status!

"Unauthenticated Requests" Group

Table 155: WBM "WAGO Device Access" Page – "Unauthenticated Requests" Group

Parameters	Explanation
Allow unauthenticated device scan	Here you can specify whether the node can be scanned without authentication. In the default setting, authentication is switched off. To increase the security level, you can force authentication for node scanning. In the current beta version, scanning only discovers head stations, not I/O modules!
[Submit]	Apply change; The change takes effect immediately.

"CORS Configuration" Group

Table 156: WBM "WAGO Device Access" Page – "CORS Configuration" Group

Parameters	Explanation
CORS Policy	Select the origins from which "Cross Origin" access to the REST API is permitted.
	Allow all "Cross Origin" access to the REST API is permitted from all origins.
	Allow all origins and null In addition to all normal origins, a value of "null" is also allowed, which some browsers use to indicate that the Web page is hosted by a local file system.
	Allow origins from whitelist The REST API should only be accessed by the origins in the whitelist. Note: With this setting, it is essential to enter your application's origin in the whitelist; otherwise, the browser will block access to the REST API.
	None The Webserver instructs the browser not to perform any cross-origin access at all.
CORS Whitelist	Enter the origins of the applications that can perform cross-origin access to the REST API. This input field is only effective if the "CORS Policy" value is set to "Allow origins from whitelist."
[Submit]	Apply change; The change takes effect immediately.

15.1.5 "Diagnostic" Tab

15.1.5.1 "Log Message Viewer" Page

The settings for displaying the diagnostic messages are shown on the "Log Message Viewer" page.

Table 157: WBM "Log Message Viewer" Page – "Refresh Options" Group

Parameters	Explanation
Read only the last	Switch display of the last n messages on/off; enter the number of messages displayed.
Automatic refresh interval (sec)	Switch cyclic refresh on/off; Enter the cycle time in seconds at which a cyclic refresh is performed; Depending on the status, the button label changes ("Refresh"/"Start"/"Stop").
Source	Select the source of the diagnostic messages; The drop-down list depends on the user logged in.
user	Only standard diagnostic messages
admin	Standard diagnostic messages and all log files in the folder /var/log/ *
[Refresh]	Refresh display; The button is only displayed if cyclic refresh is not enabled.
[Start]	Start cyclic refresh; The button is only displayed if cyclic refresh is enabled and has not yet started.
[Stop]	Stop cyclical update; The button is only displayed if cyclic update is enabled.

The cyclical refresh is performed for as long as the "Diagnostic Information" page is open. If you change the WBM page, the update is stopped until you call up the "Diagnostic" page again.

The messages are displayed below the settings.

15.1.5.2 "Download" Page

On the "Download" page, you have the option of downloading diagnostic data from the product.

Table 158: WBM "Download" Page – "Diagnostic Information" Group

Parameters	Explanation
[Download]	Download diagnostic information from device

The archive file created contains the log messages, the firmware version and a list of the installed packages.

15.1.5.3 "Network Capture" Page

All the settings required for logging the network traffic on the device and downloading these logs are available on the "Network Capture" page. The current status of the network logging is displayed.

"State" Group

Table 159: WBM "Network Capture" Page – "State" Group

Parameters	Explanation
Current State	Current status of network logging
Last Captured Package Count	Network packets already logged
Last Refresh Time	Time of the last update of "Current State" and "Last Captured Package Count"

"Configuration" Group

Table 160: WBM "Network Capture" Page – "Configuration" Group

Parameters	Explanation
Enable	Switch logging on/off
Rotate Log Files	Switch rotary logging on/off; If this option is enabled, the network traffic is stored in up to three files with the set maximum file size. When the maximum file size for the first file is reached, the data is logged in a second file and then to a third file when the second file is full. When the maximum size of the third file is reached, the data in the first file is then overwritten.
Max. File Size	Enter maximum file size for data logging
Storage Location	Select the storage location for the logged data
	Internal Flash The data is stored in the internal memory.
	SD Card The data is saved to the memory card. If "SD card" is selected, but the memory card is no longer inserted, this option is no longer enabled and only "Internal Flash" can be selected.
Lists On Network Interface	Select the network interface from which network traffic is to be logged; The available network interfaces of the device area available for selection.
[Submit]	Apply change; The change takes effect immediately.

"Filter Configuration" Group

Table 161: WBM "Network Capture" Page – "Filter Configuration" Group

Parameters	Explanation
Capture Filter	Logging filters are entered; These are used to log only the relevant or required data traffic. For example, it is possible to log the communication of only one port or from a specific IP address. More information on the possible filter settings is available in the explanations of the "Capture Filter" in the "Wireshark" documentation.
[Check]	Check entered "Capture Filter" for correctness
[Submit]	Apply change; The change takes effect immediately.

"Log Download" Group

Table 162: WBM "Network Capture" Page – "Log Download" Group

Parameters	Explanation
Select Log File	Select the recording to be downloaded from the product.
[Download]	Download selected recording from the product
[Download All]	Download all available recordings from the product

15.2 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.
- DeviceNet® is a registered trademark of the Open DeviceNet Vendor Association, Inc (ODVA).
- DALI is a registered trademark of the Digital Illumination Interface Alliance (DiiA).
- Docker® and the Docker® logo are trademarks or registered trademarks of Docker, Inc. in the USA and/or other countries. Docker, Inc. and other parties may also have trademark rights to other terms used herein.
- 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.
- **flexROOM**® is a registered trademark of WAGO Verwaltungsgesellschaft mbH.
- 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.

15.3 Technical Data, Approvals, Guidelines and Standards

Note

Subject to changes!

Please also observe the further product documentation! You can generate the current datasheet at any time at: [www.wago.com /<item number>](https://www.wago.com/<item number>).

See also

- 📄 Data Sheet 751-9401 [► 131]

Data Sheet | Item Number: 751-9402

Compact Controller 100; 8DI 8DIO 2AI 2AIO 2NI/PT 2RS485; 2 x ETHERNET; SD

<https://www.wago.com/751-9402>



Technical data

Communications	Modbus (TCP, UDP) EtherCAT® Master EtherNet/IP™ Adapter (slave) EtherNet/IP™ Scanner Modbus RTU OPC UA Server/Client OPC UA Pub/Sub (can be installed later) MQTT RS-485 interface BACnet/IP, requires an additional license Telecontrol protocols, requires an additional license
ETHERNET protocols	DHCP DNS NTP FTP FTPS SNMP HTTP HTTPS SSH
Telecontrol protocols	IEC 60870 (additional license as slave or master) IEC 61850 (additional license as Client or Server) DNP3 (additional license as Slave or Master)
Visualization	Web-Visu
Operating system	Real-time Linux (with PREEMPT_RT patch)
CPU	2 x Cortex A7; 650 MHz
Programming languages per IEC 61131-3	Instruction List (IL) Ladder Diagram (LD) Continuous Function Chart (CFC) Structured Text (ST) Sequential Function Chart (SFC)
Programming environment	CODESYS V3.5 Node RED
Configuration options	CODESYS V3.5 Ethernet Settings Web-Based Management WAGOupload WAGO Solution Builder
Transmission rate	10/100 Mbit/s
Transmission medium (communication/fieldbus)	Twisted pair S-UTP; 100 Ω; Cat. 5; 100 m maximum cable length
Main memory (RAM)	512 MB
Internal memory (flash)	4096 MB
Non-volatile hardware memory	128 KB
Program memory	32 MB
Data memory	128 MB
Non-volatile software memory	128 KB
Type of memory card	microSD up to 32 GB (all guaranteed properties only valid with WAGO's memory card)
Memory Card Slot	Push-push mechanism
Indicators	LED (SYS, RUN), red/green: System status; LED (USR), red/green: User-programmable status (accessible via CODESYS library); LED (μSD), orange: microSD card status; LED (LNK/ACT), green: Network connection status via ports 1 ... 2; LED (DI1 ... 8), green: Status of inputs; LED (DO1 ... 8) green: Status of inputs and outputs
Control Elements	Operating mode switch (RUN, STOP, RESET); reset button
Interfaces (USB)	1 × USB Type-C interface
Supply voltage (system)	24 VDC (-15 ... +20 %); Via wiring interface (<i>picoMAX</i> ® 3.5; Push-in CAGE CLAMP® connection)
Current consumption (system) max.	600 mA
Supply voltage (field)	24 VDC (-15 ... +20 %); Via wiring interface (<i>picoMAX</i> ® 3.5; Push-in CAGE CLAMP® connection)
Field current consumption max. (digital outputs) U_{in+}	4000 mA

Digital inputs/outputs	
Number of configurable digital inputs/outputs	8
Signal type	Voltage
Output current (per channel)	500 mA (DC)
Input characteristic	Type 3 (per EN 61131-2)

Digital inputs	
Number of digital inputs	8
Input characteristic	Type 3 (per EN 61131-2)

Output current (per channel)	500 mA (DC)
------------------------------	-------------

Number of analog inputs/outputs (configurable)	2
Resolution of analog inputs	16 bits
Input signal (current)	0 ... 20 mA 4 ... 20 mA 3.6 ... 21 mA
Input signal (voltage)	0 ... 10 V ±10 V
Resolution of analog outputs	12 bits
Output signal (current)	0 ... 20 mA 4 ... 20 mA 0 ... 22 mA
Output signal (voltage)	0 ... 10 V ±12 V ±10 V
Load impedance (voltage output)	≥ 1 kΩ
Load impedance (current output)	≤ 500 Ω

Number of analog inputs	2
Resolution of analog inputs	16 bits
Input signal (current)	0 ... 20 mA 4 ... 20 mA 3.6 ... 21 mA
Input signal (voltage)	0 ... 10 V ±10 V

Number of measurement inputs	2
Sensor types	Pt100 (-200 ... +850 °C); Pt200 (-200 ... +850 °C); Pt500 (-200 ... +850 °C); Pt1000 (-200 ... +850 °C); Ni100 (-60 ... +250 °C); Ni1000, TK6180 (-60 ... +250 °C); Ni1000, TK5000 (-60 ... +250 °C); Ni120 (-80 ... +260 °C); Potentiometer 0 Ohm ... 1.2 kOhm; Potentiometer 0 Ohm ... 4 kOhm

Connection technology: communication/fieldbus	Modbus (TCP, UDP): 2 x RJ-45; RS-485 interface: 1 x RJ-45; RS-485 interface: 1 x Female connector, 4-pole; Push-in CAGE CLAMP®
Connection technology: system supply	1 x Female connector, 2-pole; Push-in CAGE CLAMP®
Connection technology: field supply	2 x Female connector, 10-pole; Push-in CAGE CLAMP®
Connectable conductor materials	Copper
Solid conductor	0.2 ... 1.5 mm² / 24 ... 14 AWG
Fine-stranded conductor	0.2 ... 1.5 mm² / 24 ... 14 AWG
Strip length	8 ... 9 mm / 0.31 ... 0.35 inches

Physical data		
Width		108 mm / 4.252 inches
Height		90 mm / 3.543 inches
Depth from upper-edge of DIN-rail		55 mm / 2.165 inches

Mechanical data		
Mounting type		DIN-35 rail

Material data		
Housing material		Polycarbonate, polyamid
Fire load		0 MJ
Weight		205 g
Conformity marking		CE; UKCA

Environmental requirements		
Ambient temperature (operation)		-25 ... +60 °C
Ambient temperature (storage)		-25 ... +85 °C
Protection type		IP20
Pollution degree		2 per IEC 61131-2
Operating altitude		0 ... 2000 m / 0 ... 6562 ft
Mounting position		any
Relative humidity (without condensation)		95 %
Vibration resistance		1g per IEC 60068-2-6
Shock resistance		15g per IEC 60068-2-27
EMC immunity to interference		per EN 61000-6-2
EMC emission of interference		per EN 61000-6-3

Product Classification		
UNSPSC		32151705
ETIM 9.0		EC000236
ETIM 10.0		EC000236
ECCN		NO US CLASSIFICATION

Environmental Product Compliance		
RoHS Compliance Status		Compliant, No Exemption

Approvals / Certificates

General approvals			Declarations of conformity and manufacturer's declarations		
 			Approval	Standard	Certificate Name
KC	Article 58-2, Clause 3	R-R-W43-CC751	EU-Declaration of Conformity WAGO GmbH & Co. KG	-	-
National Radio Research Agency					
UL	UL 61010-2-201	E175199			
Underwriters Laboratories Inc. (ORDINARY LOCATIONS)					



Approvals for marine applications



Approval	Standard	Certificate Name
DNV DNV GL SE	DNV-CG-0339,Aug.2021	DNV TAA00003G6

1 Compatible Products

1.1 Product Expansions

1.1.1 Runtime software



Item No.: 2759-2283/211-1000
Runtime; BACnet; 300; M; Single License;
Online activation



Item No.: 2759-2273/211-1000
Runtime; BACnet; 300; S; Single License;
Online activation



Item No.: 2759-283/211-1000
Runtime; BACnet; 300; Single License; On-
line activation



Item No.: 2759-2293/211-1000
Runtime; DNP3 Master; M; Single License;
Online activation



Item No.: 2759-2290/211-1000
Runtime; DNP3 Slave; Single License; Online
activation



Item No.: 2759-293/211-1000
Runtime; IEC60870 Master; M; Single Li-
cense; Online activation



Item No.: 2759-290/211-1000
Runtime; IEC60870 Slave; Single License;
Online activation



Item No.: 2759-2243/211-1000
Runtime; IEC61850 Client; M; Single License;
Online activation



Item No.: 2759-2240/211-1000
Runtime; IEC61850 Server; Single License;
Online activation



Item No.: 2759-248/211-1000
Runtime; Multi Cloud Connectivity; Single Li-
cense; Online activation



Item No.: 2759-247/211-1000
Runtime; Sparkplug; Single License; Online
activation



List of Tables

Table 1	Marking	16
Table 2	Etikett.....	17
Table 3	Update Matrix.....	17
Table 4	ETHERNET Interface Pin Assignment.....	17
Table 5	Pin Assignment Supply Voltage	18
Table 6	Digital Input Pin Assignments	18
Table 7	Digital Input/Output Pin Assignments.....	19
Table 8	Analog Input Pin Assignments	20
Table 9	Analog Inputs/Outputs Pin Assignments.....	20
Table 10	Analog Temperature Sensor Pin Assignments.....	21
Table 11	Communication Interface X8 Pin Assignment	22
Table 12	Communication Interface X11 Pin Assignment.....	22
Table 13	System/Fieldbus LED Indicators.....	23
Table 14	LNK/ACT LED Indicators.....	23
Table 15	Memory Card Slot LED Indicator.....	24
Table 16	DI/DIO LED indicator.....	24
Table 17	Operating mode switch	24
Table 18	Assignment of MAC IDs and IP addresses for 1 bridge with 2 ports	29
Table 19	MAC ID and IP address assignment for 2 bridges with 1/1 ports.....	29
Table 20	Services and Users	29
Table 21	Linux® user	30
Table 22	WBM "WBM User Configuration" Page – "Change Passwords" Group	30
Table 23	Components of the Cloud Connectivity Software Package.....	36
Table 24	WBM "Firmware Backup" Page – "Firmware Backup" Group	39
Table 25	WBM "Firmware Restore" Page – "Firmware Restore" Group.....	40
Table 26	Loading a Boot Project.....	42
Table 27	Process Image - Analog Inputs AI1, AI2.....	43
Table 28	Process Image – Process Values AI; 0 ... 10 V; 16 Bit, WORD	44
Table 29	Process Image – Process Values AI; –10 ... +10 V; 16 Bit; WORD	44
Table 30	Process Image – Process Values AI; 0 ... 20 mA; 16 Bit; WORD	44
Table 31	Process Image – Process Values AI; 4 ... 20 mA; 16 Bit; WORD	44
Table 32	Process Image – Process Values AI; 3.6 ... 21 mA; 16 Bit; WORD	45
Table 33	Process Image – Analog Inputs/Outputs AIO1, AIO2.....	45
Table 34	Process Image – Process Values AO; 0 ... 10 V; 16 Bit; WORD	45
Table 35	Process Image – Process Values AO; –10 ... +10 V; 16 Bit; WORD.....	46
Table 36	Process Image – Process Values AO; –12 ... +12 V; 16 Bit; WORD.....	46

Table 37	Process Image – Process Values AO; 0 ... 20 mA; 16 Bit; WORD	46
Table 38	Process Image – Process Values AO; 0 ... 22 mA; 16 Bit; WORD	46
Table 39	Process Image – Process Values AO; 4 ... 20 mA; 16 Bit; WORD	46
Table 40	Process Image – Temperature Inputs PT1+/PT1–, PT2+/PT2–	47
Table 41	Process Image – Process Values RTD; Pt100, Pt200, Pt500, Pt1000; –200 ... +850 °C; 16 Bit; INT	47
Table 42	Process Image – Process Values RTD; Ni100, Ni1000 (Tk6180), Ni1000 (TK5000); –60 ... +250 °C; 16 Bit; INT	47
Table 43	Process Image – Process Values RTD; Ni120; –80 ... +260 °C; 16 Bit; INT	48
Table 44	Process Image – Process Values RTD; Potentiometer; 0 ... 1200 Ohm; 16 Bit; INT	48
Table 45	Process Image – Process Values RTD; Potentiometer; 0 ... 5000 Ohm; 16 Bit; INT	48
Table 46	Process Image – Digital Inputs DI1 ... DI8	49
Table 47	Process Image – Process Values of Digital Inputs – BOOL	49
Table 48	Process Image – Digital Inputs/Outputs DIO1 ... DIO8	49
Table 49	Process Image – Process Values of Digital Inputs – BOOL	49
Table 50	Process Image – Process Values, Digital Outputs – BOOL	50
Table 51	Mounting Positions and Permissible Ambient Temperatures	51
Table 52	Compatibility Overview	55
Table 53	Default IP Addresses for ETHERNET Interfaces	62
Table 54	Network Mask 255.255.255.0	62
Table 55	Default Passwords on Delivery	69
Table 56	Access Rights for WBM Pages	69
Table 57	CODESYS V3 Priorities	78
Table 58	"SYS" Diagnostic LED	80
Table 59	"RUN" Diagnostic LED	80
Table 60	"USR" Diagnostics LED	81
Table 61	LNK ACT Diagnostic LED	81
Table 62	Memory Card Slot Diagnostic LED	81
Table 63	Diagnostics LEDs DI<n>	81
Table 64	Diagnostics LEDs DIO<n>	82
Table 65	WBM "Device Status" Page – "Device Details" Group	88
Table 66	WBM "Device Status" Page – "Network TCP/IP" Group	88
Table 67	WBM "PLC Runtime Information" Page – "Runtime" Group	89
Table 68	WBM "PLC Runtime Configuration" Page – "General PLC Runtime Configuration" Group	90
Table 69	WBM "PLC Runtime Configuration" Page – "Webserver Configuration" Group	90
Table 70	WBM "TCP/IP Configuration" Page – "Bridge Interfaces" Group	91
Table 71	WBM "TCP/IP Configuration" Page – "Dummy Interfaces" Group	91
Table 72	WBM "TCP/IP Configuration" Page – "VLAN Interfaces" Group	92

Table 73	WBM "TCP/IP Configuration" Page – "DNS Server" Group	92
Table 74	WBM "Ethernet Configuration" Page – "Bridge Configuration" Group	93
Table 75	WBM "Ethernet Configuration" Page – "Switch Configuration" Group	93
Table 76	WBM "Ethernet Configuration" Page – "Ethernet Interface Configuration" Groups	93
Table 77	WBM "Configuration of Host and Domain Name" Page – "Hostname" Group	94
Table 78	WBM "Configuration of Host and Domain Name" Page – "Domain Name" Group	94
Table 79	WBM "Routing" Page – "IP Forwarding through multiple interfaces" Group	94
Table 80	WBM "Routing" Page – "Custom Routes" Group	95
Table 81	WBM "Routing" Page – "IP Masquerading" Group	96
Table 82	WBM "Routing" Page – "Port Forwarding" Group	96
Table 83	WBM "Clock" Page – "Timezone" Group	97
Table 84	WBM "Clock" Page – "UTC Time and Date" Group	97
Table 85	WBM "Clock" Page – "Local Time and Date" Group	97
Table 86	WBM "Create bootable Image" – "Create bootable image from boot device" Group	98
Table 87	WBM "Firmware Backup" Page – "Firmware Backup" Group	98
Table 88	WBM "Firmware Restore" Page – "Firmware Restore" Group	100
Table 89	WBM "Active System" Page – "Boot Device" Group	101
Table 90	WBM "Active System" Page – "System n (Internal Flash)" Group	101
Table 91	WBM "Mass Storage" Page – "Devices" Group	102
Table 92	WBM "Mass Storage" Page – "Create new Filesystem on Memory Card" Group	102
Table 93	WBM "Software Uploads" Page – "Upload New Software" Group	102
Table 94	WBM "Configuration of Network Services" Page – "FTP" Group	103
Table 95	WBM "Configuration of Network Services" Page – "FTPES (explicit FTPS)" Group	103
Table 96	WBM "Configuration of Network Services" Page – "HTTP" Group	103
Table 97	WBM "Configuration of Network Services" Page – "HTTPS" Group	104
Table 98	WBM "Configuration of Network Services" Page – "I/O-CHECK" Group	104
Table 99	WBM "Configuration of NTP Client" Page – "NTP Client Configuration" Group	104
Table 100	WBM "PLC Runtime Services" Page – "CODESYS V3" Group	104
Table 101	WBM "SSH Server Settings" Page – "SSH Server" Group	105
Table 102	WBM "Overview" Page – "Connection <n>" Group	106
Table 103	WBM "Configuration of Connection <n>" Page – "Configuration" Group	106
Table 104	Displays the selection and input fields depending on the cloud platform selected	108
Table 105	Option for selecting the data protocol depending on the cloud platform selected	109
Table 106	Displays the selection and input fields depending on the selected data protocol	109
Table 107	Option for selecting the cache mode depending on the selected data protocol	109
Table 108	Display of input fields depending on the selected authentication	109
Table 109	WBM "Configuration of general SNMP parameters" Page – "General SNMP Configuration" Group	110

Table 110	WBM "Configuration of SNMP v1/v2c Parameters" Page – "Communities" Group	110
Table 111	WBM "Configuration of SNMP v1/v2cparameters" Page – "Trap Receivers" Group	110
Table 112	WBM "Configuration of SNMP v3 Parameters" Page – "Users" Group.....	111
Table 113	WBM "Configuration of SNMP v3 Parameters" Page – "Trap Receivers" Group.....	111
Table 114	WBM "Docke Settings" Page – "Docke Status" Group.....	112
Table 115	WBM "WBM User Configuration" Page – "Change Passwords" Group	112
Table 116	WBM "OPC UA Configuration" Page – "OPC UA Server Configuration" Group.....	113
Table 117	WBM "OPC UA Configuration" Page – "OPC UA Server Security Settings" Group.....	113
Table 118	WBM "BACnet Status" Page – "BACnet Information" Group.....	114
Table 119	WBM "BACnet Status" Page – "BACnet License" Group.....	114
Table 120	WBM "BACnet Status" Page – "BACnet Data Link" Group.....	114
Table 121	WBM "BACnet Data Link" Page – "BACnet Restart" Group	115
Table 122	WBM "BACnet Data Link" Page – "BACnet/IP" Group.....	115
Table 123	WBM "BACnet Data Link" Page – "BACnet/SC" Group.....	115
Table 124	WBM "BACnet Data Link" Page – "BACnet/SC Certificate Authority (CA)" Group	115
Table 125	WBM "BACnet Data Link" Page – "BACnet/SC Certificate" Group	116
Table 126	WBM "BACnet Configuration" Page – "BACnet/SC Certificate Signing Request (CSR)" Group	116
Table 127	WBM "BACnet Data Link" Page – "BACnet/SC Default Certificates" Group	116
Table 128	WBM "BACnet Data Link" Page – "BACnet Restart" Group	116
Table 129	WBM "BACnet Configuration" Page – "BACnet Service" Group	116
Table 130	WBM "BACnet Configuration" Page – "BACnet Data" Group.....	117
Table 131	WBM "BACnet Configuration" Page – "BACnet Log Level" Group.....	117
Table 132	WBM "BACnet Configuration" Page – "BACnet Network Capture" Group	117
Table 133	WBM "BACnet Storage Location" Page – "BACnet Persistence" Group	118
Table 134	WBM "BACnet Storage Location" Page – "BACnet Trendlog" Group.....	118
Table 135	WBM "BACnet Storage Location" Page – "BACnet Eventlog" Group	118
Table 136	WBM "BACnet Info" Page – "Refresh Options" Group.....	119
Table 137	WBM "BACnet Info" Page – "BACnet/IP Statistics" Group	119
Table 138	WBM "BACnet Info" Page – "BACnet/SC Statistics" Group	119
Table 139	WBM "BACnet Info" Page – "BACnet/SC Connections" Group	119
Table 140	WBM "OpenVPN / IPsec" Page – "OpenVPN" Group.....	120
Table 141	WBM "OpenVPN / IPsec" Page – "IPsec" Group	120
Table 142	WBM "General Firewall Configuration" Page – "Global Firewall Parameter" Group.....	121
Table 143	WBM "Interface Configuration" Page – "Firewall Configuration Bridge <n> / VPN / WAN" Group	121
Table 144	Ports for Telecontrol Functionality.....	122
Table 145	WBM "Configuration of MAC address filter" Page – "Global MAC address filter state" Group	123

Table 146	WBM "Configuration of MAC address filter" Page – "MAC address filter state Bridge <n>" Group	123
Table 147	WBM "Configuration of MAC address filter" Page – "MAC address filter whitelist" Group.....	123
Table 148	WBM "Configuration of User Filter" Page – "User Filter" Group	124
Table 149	WBM "Certificates" Page – "Installed Certificates" Group	124
Table 150	WBM "Certificates" Page – "Installed Private Keys" Group	125
Table 151	WBM "Boot Mode Configuration" Page – "Force Internal Boot" Group	125
Table 152	WBM "Security Settings" Page – "TLS Configuration" Group.....	125
Table 153	WBM "Advanced Intrusion Detection Environment (AIDE)" Page – "Run AIDE check at startup" Group	126
Table 154	WBM "Advanced Intrusion Detection Environment (AIDE)" Page – "Control AIDE and show log" Group	126
Table 155	WBM "WAGO Device Access" Page – "Unauthenticated Requests" Group.....	127
Table 156	WBM "WAGO Device Access" Page – "CORS Configuration" Group	127
Table 157	WBM "Log Message Viewer" Page – "Refresh Options" Group.....	128
Table 158	WBM "Download" Page – "Diagnostic Information" Group.....	128
Table 159	WBM "Network Capture" Page – "State" Group	128
Table 160	WBM "Network Capture" Page – "Configuration" Group	129
Table 161	WBM "Network Capture" Page – "Filter Configuration" Group.....	129
Table 162	WBM "Network Capture" Page – "Log Download" Group	129

List of Figures

Figure 1	Ansicht	15
Figure 2	Marking (Example).....	16
Figure 3	Label (Example)	17
Figure 4	ETHERNET Interface Pin Assignment.....	17
Figure 5	RS-485 Bus Termination.....	23
Figure 6	Circuit Diagram	25
Figure 7	Example of Interface Assignment	28
Figure 8	1 bridge with 2 ports.....	28
Figure 9	2 bridges with 1/1 ports	29
Figure 10	Connecting the Controllers to a Cloud Service (Example).....	36
Figure 11	Distances	53
Figure 12	Inserting Controller	57
Figure 13	Removing the Female Connector without Wiring (Application Example)	58
Figure 14	Removing the Female Connector with Wiring (Application Example).....	58
Figure 15	WAGO Ethernet Settings – Start Screen (Example Figure)	63
Figure 16	WAGO Ethernet Settings – Network Tab (Example Figure).....	64
Figure 17	“Open DHCP”, Example Figure	65
Figure 18	Example of a Functional Test	66
Figure 19	Log-in Window	68
Figure 20	Password Reminder	69
Figure 21	WBM Browser Window (Example)	71
Figure 22	WBM Header with Tabs that Cannot be Displayed (Example)	71
Figure 23	WBM Status Bar (Example).....	72
Figure 24	“WAGO Ethernet Settings” – Start Screen (Example).....	73
Figure 25	“WAGO ETHERNET Settings” – Communication Link (Example)	74
Figure 26	“WAGO Ethernet Settings” – Identification Tab (Example).....	75
Figure 27	“WAGO Ethernet Settings” – Network Tab (Example)	75
Figure 28	“WAGO Ethernet Settings” – Protocol Tab (Example).....	76
Figure 29	“WAGO Ethernet Settings” – Status Tab (Example).....	77

WAGO GmbH & Co. KG

Postfach 2880 · D - 32385 Minden
Hansastraße 27 · D - 32423 Minden

✉ info@wago.com
🌐 www.wago.com

Headquarters	+49 571/887 – 0
Sales	+49 (0) 571/887 – 44 222
Order Service	+49 (0) 571/887 – 44 333

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Copyright – WAGO GmbH & Co. KG – All rights reserved. The content and structure of the WAGO websites, catalogs, videos and other WAGO media are subject to copyright. Distribution or modification of the contents of these pages and videos is prohibited. Furthermore, the content may neither be copied nor made available to third parties for commercial purposes. Also subject to copyright are the images and videos that were made available to WAGO GmbH & Co. KG by third parties.