TECHDOCS

WAGO I/O System 750/753

Controller PFC100 2nd Generation, PFC200 2nd Generation and PFC300

750-811x, 750-821x, 750-8302

Control manual
FW version 04.08.xx(30)
3621366155 | 5 | en-US | 2026-02-03 07:08

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

Technical Support
Phone: +49 571/887 – 44555
E-Mail: support@wago.com
Internet: 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

Table of Contents

1 Provisions ... 7

1.1 Scope of Applicability ... 7

2 Overview ... 12

3 Functions ... 13

3.1 Function Overview ... 13

3.2 System Functions ... 14
3.2.1 Product and system status ... 14
3.2.2 Real-Time Clock ... 15
3.2.2.1 Display/Manual Setting ... 15
3.2.2.2 Automatic Setting ... 15
3.2.3 CODESYS V3 Runtime Environment ... 16
3.2.3.1 Memory Areas under CODESYS V3 ... 16
3.2.3.1.1 Program and Data Memory ... 16
3.2.3.1.2 Function Block Limitation ... 16
3.2.3.1.3 Flag Area (Memory) and Retain Area ... 16
3.2.3.2 CODESYS V3 Priorities ... 17
3.2.3.3 CODESYS V3 Service and Port Settings ... 17

3.3 Hardware Functions ... 18
3.3.1 Address Selector Switch ... 18
3.3.2 Mode Selector Switch/Reset Button ... 18
3.3.2.1 Activating/Deactivating the Mode Selector Switch / Reset Button ... 18
3.3.2.2 Temporarily Set Fixed IP Addresses ... 19
3.3.2.3 Software Reset (Restart) ... 20
3.3.2.4 Controller Reset ... 20
3.3.3 Communication Interface ... 20
3.3.3.1 PFC100/PFC200 ... 20
3.3.3.2 PFC300 ... 21
3.3.4 Service Interface ... 23

3.4 Configuration Functions ... 23
3.4.1 Web-based Management (WBM) ... 23

3.5 Network Functions ... 24
3.5.1 Network Configuration ... 24
3.5.1.1 Interface Configration ... 24
3.5.1.1.1 Bridge Configuration ... 24
3.5.1.1.2 Dummy Interfaces ... 24
3.5.1.1.3 VLAN Interfaces ... 24
3.5.1.1.4 Port Mirror Configuration (PFC100 G2, PFC200 G2 – 2-Port, PFC300) ... 24
3.5.1.1.5 Storm Control Configuration (PFC100 G2, PFC200 G2 – 2-Port) ... 24
3.5.1.1.6 Storm Control Configuration (PFC200 G2 – 4-Port) ... 25
3.5.1.1.7 Storm Control Configuration (PFC300) ... 25
3.5.1.1.8 Ethernet Interface Configuration (PFC100 G2, PFC200 G2 – 2-Port) ... 25
3.5.1.1.9 Ethernet Interface Configuration (PFC200 G2 – 4-Port, PFC300) ... 26
3.5.1.2 TCP/IP Configuration ... 26
3.5.1.2.1 Bridge Interfaces ... 26
3.5.1.2.2 Dummy-Interfaces ... 27
3.5.1.2.3 VLAN Interfaces ... 27
3.5.1.2.4 DNS Server ... 27
3.5.1.3 Hostname/Domain Name ... 28
3.5.1.3.1 Hostname ... 28

3.5.1.3.2 Domain name ... 28
3.5.1.4 Routing ... 28
3.5.1.4.1 Static routes ... 29
3.5.1.4.2 Dynamic Routes ... 31
3.5.1.4.3 IP masquerading ... 32
3.5.1.4.4 Port forwarding ... 32
3.5.2 Network Security ... 33
3.5.2.1 Users and Passwords ... 33
3.5.2.2 Web Server Authentication ... 35
3.5.2.2.1 TLS Encryption ... 35
3.5.2.3 Root Certificates ... 36
3.5.2.4 Firewall ... 36
3.5.2.4.1 Global Firewall Settings ... 36
3.5.2.4.2 Interface-Related Firewall Settings ... 36
3.5.2.4.3 MAC Address Filter ... 37
3.5.2.4.4 User Filter ... 38
3.5.3 Network Services ... 39
3.5.3.1 DHCP Client ... 39
3.5.3.2 DHCP Server ... 39
3.5.3.3 DNS Server ... 41
3.5.3.4 SNMP ... 41
3.5.3.4.1 SNMP v1/v2c ... 42
3.5.3.4.2 SNMP v3 ... 43
3.5.3.5 FTP/FTPS ... 44
3.5.3.6 HTTP/HTTPS ... 45
3.5.3.7 I/O-CHECK ... 45
3.5.3.8 SSH Server ... 45
3.5.3.9 Docker® ... 46
3.6 Cloud Connectivity ... 46
3.7 Fieldbus Functions ... 51
3.7.1 OPC UA ... 51
3.7.2 BACnet ... 52
3.7.3 CANopen Master and Slave ... 56
3.7.3.1 Object Dictionary ... 57
3.7.3.2 Communication Profile ... 57
3.7.3.2.1 Master Configuration ... 60
3.7.3.3 Data Exchange ... 61
3.7.3.3.1 Controller Communication Objects ... 61
3.7.3.3.2 Fieldbus-Specific Addressing ... 61
3.7.3.3.3 Examples of PFC Fieldbus Variable Definitions ... 63
3.7.3.3.4 Using the CANopen Slave (Device) under CODESYS V3 ... 65
3.7.3.3.5 Use as a CAN Layer 2 Device ... 65
3.8 Memory Functions ... 65
3.8.1 Data Backup ... 65
3.8.1.1 Backup Function ... 66
3.8.1.2 Restore Function ... 67
3.8.2 Memory Card Function ... 69
3.8.2.1 Inserting a Memory Card during Operation ... 69
3.8.2.2 Removing the Memory Card during Operation ... 69
3.8.2.3 Setting the Home Directory for the Runtime System ... 69
3.8.2.4 Load Boot Project ... 70
3.9 Diagnostic Functions ... 70
3.9.1 Diagnostics via Indicators ... 70
3.9.1.1 Diagnostics via Blink Sequences ... 71
3.9.1.1.1 I/O LED Error Codes ... 71
3.9.1.1.2 MS LED Error Codes ... 74
3.9.2 Diagnostics via WBM ... 75

4 Commissioning ... 77

4.1 Switching On the Controller ... 77
4.2 Determining the IP Address of the Host PC ... 77
4.3 Setting an IP Address ... 77
4.3.1 IP Connection via USB (PFC300) ... 78
4.3.2 Setting an IP Address via the WBM ... 78
4.3.3 Assigning an IP Address with DHCP ... 79
4.3.4 Changing an IP Address with "WAGO Ethernet Settings" ... 79
4.3.5 Setting the IP Address with the Address selector switch ... 80
4.3.6 Temporarily Set Fixed IP Addresses ... 82
4.4 Testing the Network Connection ... 82
4.5 Changing Passwords ... 83
4.6 Switch Off/Restart ... 84

5 Configuration ... 85

5.1 Configuration in the WBM ... 85
5.1.1 General Page Information ... 86
5.1.2 WBM Page Overview and Access Rights ... 87
5.2 Configuration with "WAGO Ethernet Settings" ... 88
5.2.1 Identification Tab ... 90
5.2.2 Network Tab ... 91
5.2.3 PLC Tab ... 92
5.2.4 Status Tab ... 92

6 Service ... 94

6.1 Firmware Updates ... 94
6.1.1 Using WAGOupload to Update/Downgrade Firmware ... 94
6.1.2 Using a Memory Card and WBM to Update/Downgrade Firmware ... 95
6.2 Clearing Reset Functions ... 95
6.2.1 Warmstart Reset ... 95
6.2.2 Coldstart Reset ... 95
6.2.3 Software Reset (Restart) ... 96
6.2.4 Controller Reset ... 96
6.3 Update Root Certificates ... 97

7 Appendix ... 98

7.1 Configuration Dialog ... 98
7.1.1 WBM Pages ... 98
7.1.1.1 WBM Page Overview and Access Rights ... 98
7.1.1.2 "Information" Tab ... 99
7.1.1.2.1 "Device Status" Page ... 99
7.1.1.2.2 "Vendor Information" Page ... 100
7.1.1.2.3 "PLC Runtime Information" Page ... 100
7.1.1.2.4 "WAGO Software License Agreement" Page ... 101
7.1.1.2.5 "Open Source Licenses" Page ... 101
7.1.1.2.6 "WBM Third Party License Information" Page ... 101
7.1.1.2.7 "Trademarks Information" Page ... 101
7.1.1.2.8 "WBM Version" Page ... 101
7.1.1.3 "Configuration" Tab ... 101
7.1.1.3.1 "PLC Runtime Configuration" Page ... 101
7.1.1.3.2 "TCP/IP Configuration" Page ... 103
7.1.1.3.3 "Ethernet Configuration" Page ... 104
7.1.1.3.4 "Configuration of Host and Domain Name" Page ... 107
7.1.1.3.5 "Routing" Page ... 108
7.1.1.3.6 "Spanning Tree Protocol" Page ... 110
7.1.1.3.7 "Clock Settings" Page ... 112
7.1.1.3.8 Seite „Configuration of Serial Interface" ... 113
7.1.1.3.9 "Configuration of Service Interface" Page ... 115

7.1.1.3.10 “Create bootable Image” Page ... 115
7.1.1.3.11 “Firmware Backup” Page ... 116
7.1.1.3.12 “Firmware Restore” Page ... 117
7.1.1.3.13 “Active System” Page ... 119
7.1.1.3.14 “Mass Storage” Page ... 119
7.1.1.3.15 “Software Uploads” Page ... 120
7.1.1.3.16 “Configuration of Network Services” Page ... 120
7.1.1.3.17 “Configuration of NTP Client” Page ... 122
7.1.1.3.18 “PLC Runtime Services” Page ... 122
7.1.1.3.19 “SSH Server Settings” Page ... 123
7.1.1.3.20 “DHCP Server Configuration” Page ... 123
7.1.1.3.21 “Configuration of DNS Server” Page ... 124
7.1.1.3.22 “Status overview” Page ... 125
7.1.1.3.23 “Configuration of Connection <n>” Page ... 125
7.1.1.3.24 “Controls Settings” Page ... 128
7.1.1.3.25 “Configuration of general SNMP parameters” Page ... 129
7.1.1.3.26 “Configuration of SNMP v1/v2c Parameters” Page ... 129
7.1.1.3.27 “Configuration of SNMP v3 Parameters” Page ... 130
7.1.1.3.28 “Commissioning Settings” Page ... 131
7.1.1.3.29 Docker® Settings Page ... 132
7.1.1.3.30 “WBM User Configuration” Page ... 132
7.1.1.4 “Fieldbus” Tab ... 133
7.1.1.4.1 “OPC UA Configuration” Page ... 133
7.1.1.4.2 “BACnet Status” Page ... 134
7.1.1.4.3 “BACnet Configuration” Page ... 135
7.1.1.4.4 “BACnet Data Link” Page ... 136
7.1.1.4.5 “BACnet Storage Location” Page ... 138
7.1.1.4.6 “BACnet Info” Page ... 139
7.1.1.5 “Security” Tab ... 140
7.1.1.5.1 “OpenVPN / IPsec” Page ... 140
7.1.1.5.2 “General Firewall Configuration” Page ... 141
7.1.1.5.3 “Interface Configuration” Page ... 141
7.1.1.5.4 “Configuration of MAC address filter” Page ... 142
7.1.1.5.5 “Configuration of User Filter” Page ... 143
7.1.1.5.6 “Certificates” Page ... 144
7.1.1.5.7 “Boot Mode Configuration” Page ... 145
7.1.1.5.8 “Security Settings” Page ... 145
7.1.1.5.9 “Advanced Intrusion Detection Environment (AIDE)” Page ... 146
7.1.1.5.10 “WAGO Device Access” Page ... 147
7.1.1.6 “Diagnostic” Tab ... 147
7.1.1.6.1 “Log Message Viewer” Page ... 147
7.1.1.6.2 “Download” Page ... 148
7.1.1.6.3 “Network Capture” Page ... 148

1 Provisions

1.1 Scope of Applicability

This document applies to the following products:

750-8110 (PFC100; G2; 2ETH; ECO)
PFC100 Controller; 2nd Generation; 2 × ETHERNET; ECO

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8110

750-8111 (PFC100; G2; 2ETH)
Controller PFC100; 2nd Generation; 2 × ETHERNET

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8111

750-8112 (PFC100; G2; 2ETH; RS)
PFC100 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8112

750-8112/025-000 (PFC100; G2; 2ETH; RS; T)
PFC100 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485; Ext. Temperature

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8112/025-000

750-8210 (PFC200; G2; 4ETH)
PFC200 Controller; 2nd Generation; 4 × ETHERNET

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8210

750-8210/025-000 (PFC200; G2; 4ETH; T)
PFC200 Controller; 2nd Generation; 4 × ETHERNET; Ext.Temperature

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8210/025-000

750-8210/040-000 (PFC200; G2; 4ETH; XTR)
PFC200 Controller; 2nd Generation; 4 × ETHERNET; Extreme

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8210/040-000

750-8211 (PFC200; G2; 2ETH 2SFP)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, 2 × SFP

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8211

750-8211/040-000 (PFC200; G2; 2ETH 2SFP; XTR)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, 2 × 100Base-FX; Extreme

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8211/040-000

750-8211/040-001 (PFC200; G2; 2ETH 2SFP; Tele; XTR)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, 2 × 100Base-FX; Telecontrol Technology; Extreme

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8211/040-001

750-8212 (PFC200; G2; 2ETH RS)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8212

750-8212/025-000 (PFC200; G2; 2ETH RS; T)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485; Ext. Temperature

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8212/025-000

750-8212/025-001 (PFC200; G2; 2ETH RS; Tele; T)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485; Telecontrol Technology; Ext. Temperature

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8212/025-001

750-8212/025-002 (PFC200; G2; 2ETH RS; Tele; T; ECO)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485; Telecontrol Technology; Ext. Temperature; ECO

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8212/025-002

750-8212/000-100 (PFC200; G2; 2ETH RS BACnet/IP)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485; BACnet/IP

Version Firmware	04.08.xx(30)

Product Detail Page	http://www.wago.com/750-8212/000-100

750-8212/040-000 (PFC200 G2 2ETH RS XTR)
PFC200 Controller G2; 2 × ETHERNET; RS-232/485; Extreme

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8212/040-000

750-8212/040-001 (PFC200 G2 2ETH RS TELE XTR)
PFC200 Controller G2; 2 × ETHERNET; RS-232/485; Telecontrol; Extreme

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8212/040-001

750-8212/040-010 (PFC200 G2 2ETH M12 RS XTR)
PFC200 Controller G2; 2 × ETHERNET M12, RS-232/485; Extreme

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8212/040-010

750-8213 (PFC200; G2; 2ETH CAN)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, CAN, CANopen

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8213

750-8213/040-010 (PFC200 G2 2ETH M12 CAN XTR)
PFC200 Controller G2; 2 × ETHERNET M12, CAN, CANopen; Extreme

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8213/040-010

750-8214 (PFC200; G2; 2ETH RS CAN)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485, CAN, CANopen

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8214

750-8215 (PFC200; G2; 4ETH CAN USB)
PFC200 Controller; 2nd Generation; 4 × ETHERNET, CAN, CANopen, USB-A

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8215

750-8216 (PFC200; G2; 2ETH RS CAN DPS)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485, CAN, CANopen, PROFIBUS Slave

Version Firmware	04.08.xx(30)

Product Detail Page	http://www.wago.com/750-8216

750-8216/025-000 (PFC200; G2; 2ETH RS CAN DPS; T)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485, CAN, CANopen, PROFIBUS Slave; Ext. Temperature

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8216/025-000

750-8216/025-001 (PFC200; G2; 2ETH RS CAN DPS; Tele; T)
PFC200 Controller; 2nd Generation; 2 × ETHERNET, RS-232/485, CAN, CANopen, PROFIBUS Slave; Telecontrol Technology; Ext. Temperature

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8216/025-001

750-8216/040-000 (PFC200 G2 2ETH RS CAN DPS XTR)
PFC200 Controller G2; 2 × ETHERNET, RS-232/485, CAN, CANopen, PROFIBUS Slave; Extreme

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8216/040-000

750-8302 (PFC300; 2ETH RS485)
PFC300 Controller; 2 × ETHERNET, RS-485

Version Firmware	04.08.xx(30)
Product Detail Page	http://www.wago.com/750-8302

The complete operating instructions for the products consist of several applicable documents. The products must only be installed and operated in accordance with the complete operating instructions. Knowledge of all applicable documents is required for proper use. Please find all documents and information on the detailed product pages.

Applicable documents

System Manual I/O System 750/753
- Provisions
- Safety
- Planning
- Transport and Storage
- Assembly and Disassembly
- Conductor Termination
- Decommissioning

Product Manual of the used controller PFC100 G2, PFC200 G2 or PFC300
- Provisions
- Properties
- Planning
- Diagnostics
- Service

Information

This document describes the complete scope of functions. Not all functions described are supported by every product.

2 Overview

Controller PFC100

The compact PFC100 controller has 512 MB of memory – ideal for use in the building and mechanical engineering industries.

- Programmable via CODESYS per IEC 61131-1
- Open Linux® platform
- Comprehensive security functions

Controller PFC200

PFC200 Series Controllers have a variety of functions and are thus well-equipped for use in industrial, process and building automation.

- Fieldbus-independence
- Programmable with CODESYS per IEC 61131-1 on a Linux® operating system
- Comprehensive security functionalities
- XTR version for use under extreme conditions

Controller PFC300

The PFC300 is equipped with 2 GB of RAM and a 64 bit processor for larger applications in machine, process and building environments.

- Programmable with CODESYS per IEC 61131-1 on a Linux® operating system
- Comprehensive security functions
- Two process cores: DUAL core
- USB-C service interface

3 Functions

3.1 Function Overview

The functions listed here are not included in all products.
The functions included are available in the function overview in the corresponding product manual.

The functions are described in the following sections.

System Functions

- Product and system status [▸ 14]
- Real-Time Clock [▸ 15]
- Data Backup [▸ 65]
- Memory Card Function [▸ 69]
- CODESYS V3 Runtime Environment [▸ 16]

Hardware Functions

- Mode Selector Switch/Reset Button [▸ 18]
- Communication Interface [▸ 20]
- Service Interface [▸ 23]
- Address Selector Switch [▸ 18]

Configuration Functions

- Web-based Management (WBM) [▸ 23]

Network Functions

- Network configuration
- Network security
- Network services

Cloud Connectivity

Fieldbus Functions

- BACnet [▸ 52]
- OPC UA [▸ 51]
- CANopen Master and Slave [▸ 56]

Diagnostic Functions

- Diagnostics via Indicators [▸ 70]
- Diagnostics via WBM [▸ 75]

3.2 System Functions

3.2.1 Product and system status

The product properties are displayed on the WBM “Device Status” page in the “Device Details” group:

Table 1: 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

The most important network and interface properties of the product are displayed on the WBM “Device Status” page in the “Network TCP/IP Details” group:

Table 2: 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)
	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	

Information about the enabled runtime system is displayed on the WBM “PLC Runtime Information” page in the “Runtime” group:

Table 3: WBM “PLC Runtime Information” Page – “Runtime” Group

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

3.2.2 Real-Time Clock

3.2.2.1 Display/Manual Setting

Table 4: 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	
Local Date	Local Date	
Local Time	Local Time	
UTC Date	Date	
UTC Time	GMT Time	

3.2.2.2 Automatic Setting

Table 5: WBM “Configuration of NTP Client” Page – “NTP Client Configuration” Group

Parameters	Explanation	
Service enabled	Enable/disable automatic updating of the time;	
	☐	Updating the time is disabled; default setting
	☑	Updating the time is enabled.
Update Interval (sec)	Enter update interval of the time server.	
Time Server <n>	Enter the IP addresses of the time servers; a maximum of 4 time servers are possible.	
Additionally assigned (DHCP)	NTP server assigned by DHCP (or BootP if supported); If no time server has been assigned, “No additional servers assigned” is displayed.	

3.2.3 CODESYS V3 Runtime Environment

Note

Read CODESYS V3 documentation!

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

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.

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.

3.2.3.1 Memory Areas under CODESYS V3

3.2.3.1.1 Program and Data Memory

The program (also code) and data memory has already been requested in the system after a successful program download and can be fully utilized. The memory area is dynamically divided into program and data areas. The total size depends on the product and is specified in the technical data for the respective product.

3.2.3.1.2 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 area is calculated from the function block limitation x 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.

3.2.3.1.3 Flag Area (Memory) and Retain Area

The flag area (memory) and the retain area together form the retentive memory for the IEC 61131 application. The total size depends on the product and is specified in the technical data for the respective product.

3.2.3.2 CODESYS V3 Priorities

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

Table 6: 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

3.2.3.3 CODESYS V3 Service and Port Settings

Table 7: 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.

Table 8: 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.

Table 9: WBM “PLC Runtime Services” Page – “CODESYS V3” Group

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

3.3 Hardware Functions

3.3.1 Address Selector Switch

3.3.2 Mode Selector Switch/Reset Button

3.3.2.1 Activating/Deactivating the Mode Selector Switch / Reset Button

Primarily for safety reasons and difficult-to-access installations, the controller offers the option of activating/deactivating the mode selector switch and the reset button.

When the mode selector switch is deactivated, the controller must be controlled via the CODESYS development environment.
When the reset button is deactivated, it is still positive to perform a software reset (restart) via the WBM.

ⓘ Note

If the mode selector switch is deactivated and a CODESYS boot project has been loaded, it is executed automatically when the product restarts!

When the mode selector switch is deactivated, the only way to stop and reset a running application is by using the CODESYS development environment.

The settings can be made on the WBM "Controls Settings" page, "Configuration" tab. Change do not take effect until controller is restarted.

Table 10: WBM "Controls Settings" Page – "OMS Controls" Group

Parameters	Explanation	
Current Mode	Current status of the functionality of the mode selector switch and reset button	
	Inactive	The controller ignores any activation of the mode selector switch and the reset button.
	Active	The controller reacts to use of the mode selector switch and the reset button.
Activate	Activates/deactivates the mode selector switch and the reset button	
	☐	Deactivates mode selector switch and reset button
	☑	Activates mode selector switch and reset button

3.3.2.2 Temporarily Set Fixed IP Addresses

This process temporarily sets the IP addresses for the network interfaces X1 ... X<n> to fixed IP addresses.
For each bridge used, the assigned interfaces are assigned their own address, whereby bridge 1 receives the IP address "192.168.1.17", bridge 2 the IP address "192.168.2.17" and so on.

No reset is carried out.

To set temporary fixed IP addresses, proceed as follows:

1. Set the mode selector 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.

If you make changes to the IP configuration of a bridge after enabling the temporary IP addresses, the new settings are permanently adopted and applied immediately. The configured bridge exits the temporary IP address mode. The other bridges keep the temporarily set IP address until restart / reset.

To cancel the setting, proceed as follows:

- Perform a software reset.

or

- Switch the product off and on again.

3.3.2.3 Software Reset (Restart)

- 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.

3.3.2.4 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!

When the controller is reset ("controller reset"):
- Parameters and passwords of the Linux and WBM users of the controller are overwritten,
- deleted saved boot projects including existing Web visualizations,
- after-installed firmware functions not overwritten,
- Software licenses not deleted

The disabled system is not changed by the controller reset.
If you have any questions, contact WAGO Support.

The controller is restarted automatically after the controller is reset.

To perform a controller reset, proceed as follows:

✓ Requirement: Power supply is enabled.

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 alternately flashes red/green (approx. 8 seconds).
4. Release the mode selector switch and the reset button.

➡ The controller has been reset and restarts automatically.

3.3.3 Communication Interface

3.3.3.1 PFC100/PFC200

The controller has a configurable communication interface.

The interface mode can be switched between RS-232 and RS-485.

The interface supports the following communication parameters:
- 8 data bits
- Even/odd parity
- 0/1/2 stop bits

The communication interface can be assigned to the Linux console. In this case, only the Linux console can communicate via the interface.
If the interface is not assigned, the CODESYS program can access it via function blocks, for example.

The communication interface is set, for example, via the WBM "Configuration of Serial Interface" page.

The current configuration of the interface is displayed in the "Current Serial Interface Configuration" group.

Table 11: WBM "Configuration of Serial Interface" Page – "Current Serial Interface Configuration" Group

Parameters	Explanation	
Assigned to	Assignment of communication interface	
	Unassigned (usage by Applications, Libraries, PLC Runtime)	The communication interface is not assigned to any application. This allows the CODESYS program to access it via function blocks, for example.
	Linux Console	The communication interface is assigned to the Linux console.
Mode	Communication interface mode	
	RS-232	The communication interface is operated in RS-232 mode.
	RS-485	The communication interface is operated in RS-485 mode.

The assignment of the interface is set in the "Assign Owner of Serial Interface" group.

Table 12: WBM "Configuration of Serial Interface" Page – "Assign Owner of Serial Interface" Group

Parameters	Explanation
Unassigned (usage by Applications, Libraries, PLC Runtime)	The communication interface is not assigned to any application.
Linux Console	The communication interface is assigned to the Linux console.

The operating mode of the interface is set in the "Assign Mode of Serial Interface" group.

Table 13: WBM "Configuration of Serial Interface" Page – "Assign Mode of Serial Interface" Group

Parameters	Explanation
RS-232	The communication interface is operated in RS-232 mode.
RS-485	The communication interface is operated in RS-485 mode.

3.3.3.2 PFC300

The controller has a configurable communication interface.

The operating mode of the interface is permanently set to RS-485.

The interface supports the following communication parameters:
- 8 data bits
- Even/odd parity
- 0/1/2 stop bits

A biasing network prevents oscillations on the bus lines when no transmitter is active. These oscillations can lead to transmission errors. Pull-up and pull-down resistors ensure that all receiver inputs have a voltage difference between RxD+ and RxD- of more than 200 mV in the idle state.

A terminating resistor at each end of the bus lines prevents reflections on the bus lines. These reflections can also lead to transmission errors.

Depending on the bus requirements, the pull-up and pull-down resistors (1) of the bias network integrated in the interface and the integrated terminating resistor (2) can be switched on or off.

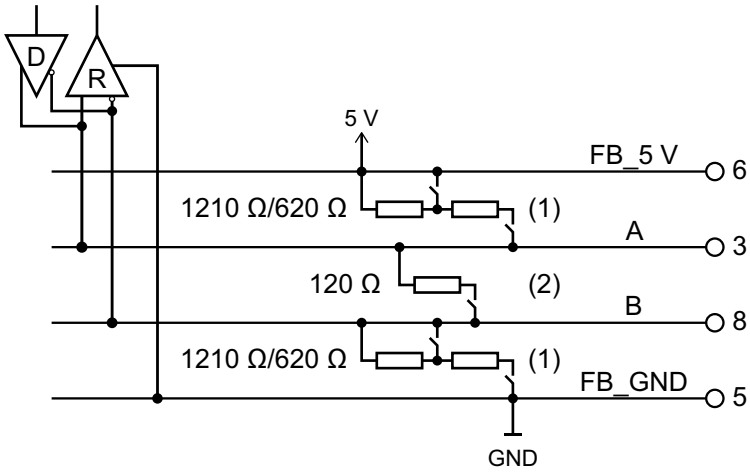

Figure 1: Communication interface, bus termination and bias network

The communication interface is set, for example, via the WBM "Configuration of Serial Interface" page.

The current configuration of the interface is displayed in the "Current Serial Interface Configuration" group.

Table 14: WBM "Configuration of Serial Interface" Page – "Current Serial Interface Configuration" Group

Parameters	Explanation	
Mode	Communication interface mode	
	RS485	The communication interface is operated in RS-485 mode.

Der Busabschluss ist in der Gruppe „Bus Termination" einstellbar.

Table 15: WBM "Configuration of Serial Interface" Page – "Bus Termination" Group

Parameters	Explanation	
Termination enabled	Activate/deactivate bus termination.	
	☐	The bus termination is deactivated.
	☑	The bus termination is activated.

Das Bias-Netzwerk ist in der Gruppe „Bias Network" einstellbar.

Table 16: WBM "Configuration of Serial Interface" Page – "Bias Network" Group

Parameters	Explanation
Off	No bias network is active.
Low	Bias network 1 (640 Ohm) is active.
High	Bias network 2 (1210 Ohm) is active.

3.3.4 Service Interface

The service interface is set, for example, via the WBM "Configuration of Service Interface" page.

Interface assignment:

Table 17: WBM "Configuration of Service Interface" Page – "Assign Owner of Service Interface" Group

Parameters	Explanation
WAGO Service Communication	The service interface is used for WAGO service communication or runtime system communication.
Linux Console	The service interface is assigned to the Linux console.
Unassigned (usage by Applications, Libraries, PLC Runtime)	The service interface is not assigned to any application. This allows the CODESYS program to access it via function blocks, for example.

3.4 Configuration Functions

3.4.1 Web-based Management (WBM)

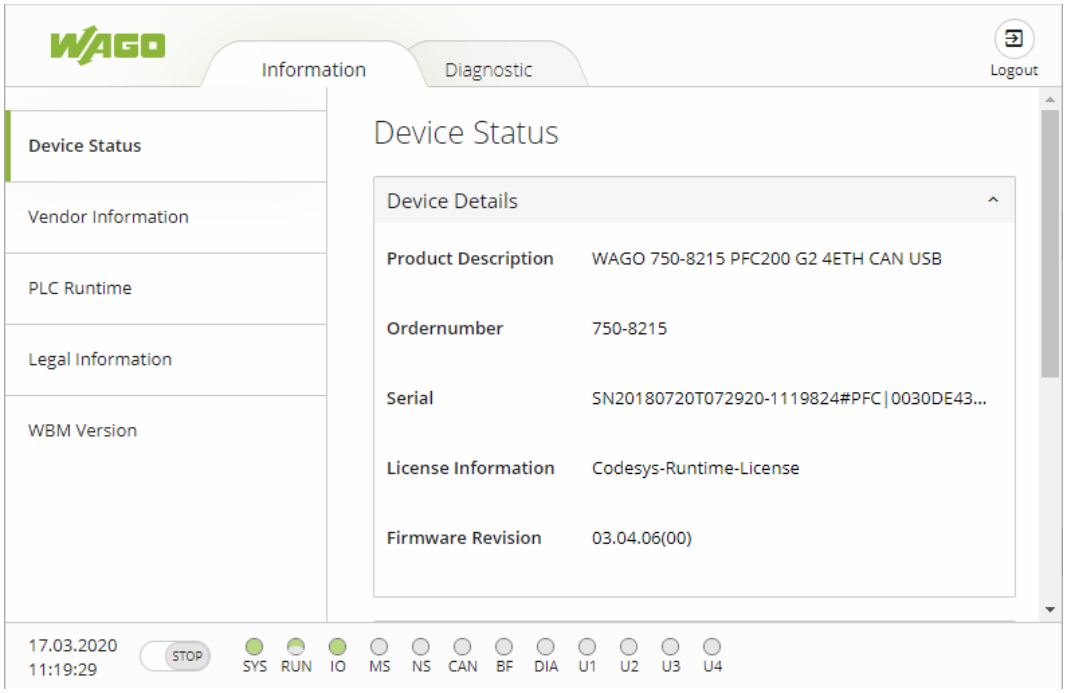

Figure 2: WBM Browser Window (Example)

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.

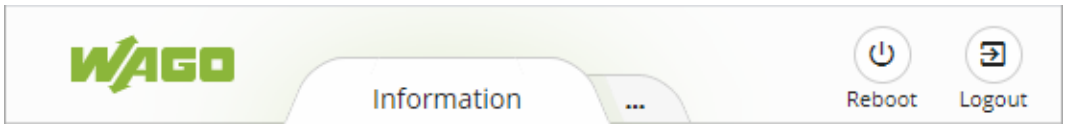

Figure 3: WBM Header with Tabs that Cannot be Displayed (Example)

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.

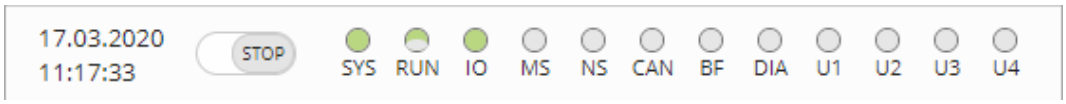

Figure 4: WBM Status Bar (Example)

- Date and time – local time and date on the device
- Status of the mode selector switch
- LED status of the device:
  The LEDs are labeled with their respective names (e.g., SYS, RUN, IO, ...) and the states are represented 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.

3.5 Network Functions

3.5.1 Network Configuration

3.5.1.1 Interface Configration

3.5.1.1.1 Bridge Configuration

3.5.1.1.2 Dummy Interfaces

3.5.1.1.3 VLAN Interfaces

3.5.1.1.4 Port Mirror Configuration (PFC100 G2, PFC200 G2 – 2-Port, PFC300)

3.5.1.1.5 Storm Control Configuration (PFC100 G2, PFC200 G2 – 2-Port)

Table 18: WBM "ETHERNET Configuration" Page – "Storm Control Settings" Group

Parameters	Explanation
Broadcast Protection	Data packet limiting value for broadcast; default value: 1 % of the maximum data rate

Parameters	Explanation	
Multicast Protection	Determines whether the data packet limitation applies only to broadcast or to broadcast and multicast together	
	☐	Data packet limitation applies only to broadcast packets
	☑	Data packet limitation applies to both broadcast and multicast packets

3.5.1.1.6 Storm Control Configuration (PFC200 G2 – 4-Port)

Table 19: WBM "ETHERNET Configuration" Page – "Storm Control Settings" Group

Parameters	Explanation
Broadcast Protection	Data packet limiting value for broadcast; default value: 1 Mbit
Multicast Protection	Data packet limiting value for multicast; default value: 1 Mbit

3.5.1.1.7 Storm Control Configuration (PFC300)

Table 20: WBM "ETHERNET Configuration" Page – "Storm Control Settings" Group

Parameters	Explanation
Broadcast Protection	Data packet limiting value for broadcast; default value: 20000 packets per second
Multicast Protection	Data packet limiting value for multicast; default value: 20000 packets per second

3.5.1.1.8 Ethernet Interface Configuration (PFC100 G2, PFC200 G2 – 2-Port)

Table 21: 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
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.	

3.5.1.1.9 Ethernet Interface Configuration (PFC200 G2 – 4-Port, PFC300)

Table 22: 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
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.	

3.5.1.2 TCP/IP Configuration

3.5.1.2.1 Bridge Interfaces

Table 23: 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	

3.5.1.2.2 Dummy-Interfaces

Table 24: WBM "TCP/IP Configuration" Page – "Dummy Interfaces" Group

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

3.5.1.2.3 VLAN Interfaces

Table 25: 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**.	

3.5.1.2.4 DNS Server

The controller can use a maximum of three enabled DNS servers.
DNS servers can be assigned via DHCP or manually.

The DNS servers that are actually used are determined by alternating merging of the DNS servers assigned via DHCP and the DNS servers assigned manually.
The first DNS server assigned via DHCP is assigned the highest priority.

You can display the assigned DNS servers and manually assign additional DNS servers, e.g., via the WBM "TCP/IP Configuration" page in the "DNS Server" group.

Table 26: 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.

3.5.1.3 Hostname/Domain Name

3.5.1.3.1 Hostname

Without a hostname configuration, the controller is assigned a default name which includes the last three values of the controller's MAC address. This name is valid for as long as a hostname was not configured, or hostname was not supplied to the controller via DHCP (for configuration of the controller see Section “Startup” > “Configuring”). When the hostname is set, a hostname supplied by a DHCP response is immediately enabled and displaces the configured or default hostname.

For multiple network interfaces with DHCP, the hostname is taken from the network interface (bridge or Wwan) with the highest priority. The priority is specified alphanumerically by the name of the network interface. Thus, Bridge1 has the highest priority, followed by Bridge2, Bridge3, ..., Wwan0.

If only the configured name is to be valid, the network administrator must adjust the configuration of the enabled DHCP server so that no hostnames are transferred in the DHCP response.

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

The hostname settings can be made, for example, on the WBM “Configuration of Host and Domain Name” page in the “Host Name” group.

Table 27: 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

3.5.1.3.2 Domain name

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.

The settings for the domain name are possible, for example, on the WBM page “Configuration of Host and Domain Name” in the “Domain Name” group.

Table 28: 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

3.5.1.4 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
- Interface

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 forwarding, "Enabled" must be selected in the "IP Forwarding through multiple interfaces" 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.

The forwarding of IP data packets can be set, for example, on the WBM "Routing" page in the "IP Forwarding through multiple interfaces" group.

Table 29: WBM "Routing" Page – "IP Forwarding through multiple interfaces" Group

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

3.5.1.4.1 Static routes

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

Default gateways, also called default routes, are generally set in conjunction with the IP configuration. Each default gateway has a metric that is unique among all default gateways. Bridge <n> has the metric 19+<n>. A default gateway can also be defined via the routing configuration, e.g., to define an individual metric. The value "default" must be set for "Destination Address" and the value "0.0.0.0" for Destination Mask.

Itinerary

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.

Alternatively, a bridge, a modem or a VPN interface can be specified in the "Interface" field, via which all data packets that are directed to the destination address are routed. Specifying an interface is optional. However, either a gateway address, an interface or both must be specified.

If the IP address of the gateway is outside the IP address space that the controller can reach, the associated route is not enabled. This also applies to routes in which an interface is specified, which e.g., is not enabled in the current bridge configuration.

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.

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 network
Destination mask:	255.255.255.0	Subnet mask of the destination network
Gateway address:	10.0.1.3	IP address of the gateway
Gateway metric:	20	Route priority

Example of a route via an interface:

In the following example, a route to a host with IP address 192.168.1.2 is to be specified. The route runs via the br1 interface, which corresponds to Bridge 2. To configure a host route to the target host via Bridge 2 on a controller with an enabled Bridge 2, 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 metric:	20	Route priority
Interface:	br1	Interface through which the packet is to be routed

The settings for the static routes can be made via the WBM "Routing" Page – "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 30: 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.	

3.5.1.4.2 Dynamic Routes

Besides the manually configurable routes, default gateways can also be set via DHCP replies. A unique metric is assigned to all default gateways assigned by DHCP.

The metric is assigned starting at 10 and depends on the network interface via which the DHCP response was received. The metric is assigned in ascending order based on the alphanumeric sorting of the network interface names (e.g., br0, br1, ... wwan0).

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.

All default gateways received via DHCP are displayed via the WBM "Routing" Page – "Dynamic Routes (assigned by DHCP)" group.

Each dynamic route has its own area in the display. If no dynamic are been received via DHCP, "no dynamic route" is displayed.

Table 31: WBM "Routing" Page – "Dynamic Routes (assigned by DHCP)" Group

Parameters	Explanation
Destination Address	Target address of the subscriber
Destination Mask	Subnet mask of the subscriber
Gateway Address	Gateway address
Gateway Metric	Metrics of the route
Interface	Interface through which the packets directed to the destination address are routed

3.5.1.4.3 IP masquerading

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.

Table 32: 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."	

3.5.1.4.4 Port forwarding

The controller also allows 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.

Table 33: WBM "Routing" Page – "Port Forwarding" Group

Parameters	Explanation
Enabled	Use Port Forwarding

Parameters	Explanation	
	☐	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.	

3.5.2 Network Security

3.5.2.1 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 34: 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		
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 35: 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 36: 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.

3.5.2.2 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 key role in all secure communication channels, using secure authentication is strongly recommended.
The security certificate stored on the controller is the basis for authentication.
As delivered, the controller uses a generic security certificate in x509 format.

To enable secure authentication, you must install a specific certificate created for the individual device.
Save the individual certificate to the device at the following path: `/etc/lighttpd/custom-cert.pem`.
After the Webserver is restarted, the individual certificate becomes active.

If the individual certificate is deleted from the device, the Webserver uses the generic security certificate again after a restart.

3.5.2.2.1 TLS Encryption

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

You can specify the permitted TLS versions and cryptographic methods in the settings ("Strong"/"Extended Compatibility").
When the "Strong" setting is used, the Webserver only allows TLS 1.3 and strong algorithms. Older software and older operating systems may not support TLS 1.3 and the encryption algorithms.
When the "Extended Compatibility" setting is used, TLS 1.2 is also permitted with less powerful cryptographic methods. Use is recommended only for backward compatibility with older systems.

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**.

The cryptographic methods allowed with HTTPS and the TLS versions that can be used can be switched in the –TLS Configuration" group of the WBM "Security Settings" page.

Table 37: 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.

3.5.2.3 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 [▸ 97]

3.5.2.4 Firewall

3.5.2.4.1 Global Firewall Settings

Table 38: 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

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.

3.5.2.4.2 Interface-Related Firewall Settings

Table 39: WBM "Interface Configuration" Page – "Firewall Configuration Bridge <n> / VPN / WAN" Group

Parameters	Explanation
Firewall enabled for Interface	Enable/disable firewall for the respective interface

Parameters	Explanation
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
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)	

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 40: Ports for Telecontrol Functionality

Protocol	Port
DNP3	20000
IEC60870-5-104	2404
IEC61850	102

3.5.2.4.3 MAC Address Filter

Global setting

Table 41: WBM “Configuration of MAC address filter” Page – “Global MAC address filter state” Group

Parameters	Explanation
Filter enabled	Enable/disable global MAC address filter

Bridge-related setting

Table 42: 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.

MAC address filter whitelist

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.

Each configured filter has its own area in the display.
If no MAC Address filter has been created, "no MAC Address filters" is displayed.

A maximum of 10 MAC address filters can be created in the "Add filter to whitelist" area.

Table 43: 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

3.5.2.4.4 User Filter

Each configured filter has its own area in the display.
If no user filter has been created, "no user filters" is displayed.

A maximum of 10 user filters can be created in the "Add new user filter" area.
You only need to enter values in the fields that are to be set for the filter.
At least one value must be entered, all other fields can remain empty.

Table 44: 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.

Parameters	Explanation	
	Bridge <n>	The interfaces assigned for bridge <n> are filtered. Only the configured bridges are displayed.
	VPN	The VPN interface is filtered.

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.

3.5.3 Network Services

3.5.3.1 DHCP Client

The controller can obtain network parameters from an external DHCP server via the DHCP client.

The following parameters can be obtained:
- IP address
- Subnet mask
- Router/Gateway
- Hostname
- Domain
- DNS Server
- NTP server

The entries for the IP address, subnet mask and router/gateway parameters are saved for each ETHERNET interface.

For multiple network interfaces with DHCP, the hostname is taken from the network interface (bridge or Wwan) with the highest priority. The priority is specified alphanumerically by the name of the network interface. Thus, Bridge1 has the highest priority, followed by Bridge2, Bridge3, ..., Wwan0.

3.5.3.2 DHCP Server

The controller provides the DHCP server service for the automatic configuration of IP addresses of network stations on the same subnet. Generally, only one DHCP server can be enabled on a subnet at one time.

The following can be set for the DHCP server:
- The service itself (enabled/disabled)
- The range of dynamically assigned IP addresses
- The lease time of the dynamically assigned IP addresses
- A list with static assignments of IP addresses to MAC addresses

In “Switched” mode, these settings are possible for both interfaces together and in “Separated” mode for each interface separately.

The DHCP server also passes other parameters in addition to the IP address. The following table shows the complete list.

Table 45: List of Parameters Transmitted via DHCP

Parameter	Explanation
IP address	An IP address from the range of permitted address; the range can be configured in the WBM. The DHCP server determines the IP address to be passed to the requesting network subscriber (client) from the MAC address of the network subscriber and the range of addresses to be assigned. As long as the configured address range does not change and no bottlenecks occur when assigning IP addresses, the DHCP server continuously reassigns the same IP addresses to requesting network subscribers. When a subscriber connects to the network, for whose MAC address a fixed IP address has been configured in the WBM, this address is passed to it. Such a fixed IP address can also be outside the range of freely-assignable IP addresses. A hostname can also be specified instead of the MAC address for identifying the requesting network subscriber.
Subnet mask	The subnet mask configured in the network settings of the DHCP server for the local network concerned is passed. The subnet mask and IP address determine the range of valid IP addresses on the local network.
Broadcast address	IP address with which an IP packet can be sent to all network subscribers on the subnet at the same time.
Lease time	Determines the validity period of the DHCP parameters passed to a network subscriber: Per protocol, the network subscriber is required to request the network settings again after half the period of validity. The lease time is configured in the WBM.
Hostname	The network name is passed to the network subscriber. The network subscriber normally sends its own name with its request for the IP address. It is then used by the DHCP server in its response.
Name server	The DHCP server passes its own IP address as the DNS name server to the network subscriber.
Default Gateway	The DHCP server passes its own IP address as the default gateway to the network subscriber. The default gateway is required to communication with subscribers outside the local network.

Not all parameters can be set in the WBM. If you want to set other values for the existing parameters or want to pass other parameters via DHCP, the DHCP server must be manually configured. For the controller, the DHCP server service is handled by the program "dnsmasq."
From a Linux® command line, an editor must be used to change the file "/etc/dnsmasq.d/dnsmasq_default.conf" to set the configuration.

The settings are made, for example, in the WBM via the "DHCP Configuration" page.

Table 46: WBM "DHCP Server Configuration" – "DHCP Server Configuration Bridge <n>" Group

Parameters	Explanation	
Service enabled	Enable/disable DHCP server service for the bridge <n>;	
	☐	The DHCP server service for the bridge <n> is not enabled.
	☑	The DHCP server service for the bridge <n> is enabled.
Start IP for Range	Enter the starting value of the available IP address range.	
End IP for Range	Enter the end value of the available IP address range.	
Lease time (min)	Enter the lease time in minutes. Default: 120 minutes	
Static Hosts	Static mappings of MAC IDs or host hubs to IP addresses; If no assignment is available, "No static hosts configured" is displayed.	
Add Static Host	Add static mappings of MAC addresses or hostnames to IP addresses; max. 15 mappings possible.	

Parameters	Explanation
MAC Address or Hostname	Enter MAC address or hostname; e.g., "01:02:03:04:05:06=192.168.1.20" or "hostname=192.168.1.20."
IP Address	Enter the IP address.

3.5.3.3 DNS Server

The controller offers the DNS server service for the automatic assignment of hostnames to IP addresses of network stations. The DNS server takes the names and IP addresses of local network stations from the DHCP server. This DNS server routes requests for non-local names, such as from the Internet, to higher-level DNS servers if configured and accessible.

The following settings are possible for the DNS server:

- The service itself (enabled/disabled)
- Access type to the assignments
  The requests are buffered in "Proxy" mode (throughput optimized).
  In Relay mode the requests are routed directly to higher-level name servers.
- A list with up to 15 static assignments of IP addresses to hostnames
  If only the hostname is used, the configured or default domain is added to the hostname automatically to ensure FQDN name resolution.

The settings are made, e.g., in the WBM, via the "Configuration of DNS Service" page.

Table 47: WBM "Configuration of DNS Server" Page – "DNS Server" Group

Parameters	Explanation	
Service enabled	Enable/disable DNS server service;	
	☐	The DNS server service is disabled.
	☑	The DNS server service is enabled.
Mode	Set operating mode;	
	Proxy	Requests are buffered to optimize throughput.
	Relay	All requests are routed directly.
Static Hosts	Static mapping of hostnames to IP addresses; If no mapping exists, "No static hosts configured" is displayed.	
Add Static Host	Add static IP address assignments to hostnames; max. 10 assignments possible.	
IP Address	Enter IP address; e.g., "192.168.1.20:hostname"	
Hostname	Enter hostname.	

3.5.3.4 SNMP

SNMP (Simple Network Management Protocol) is a standard protocol for monitoring and managing devices in a TCP/IP network. The Simple Network Management Protocol (SNMP) is responsible for transporting the control data that allows the exchange of management information, the status and statistic data between individual network components and a management system.

The protocol is available in versions v1, v 2c and v3. The versions are independent of each other and can be enabled and used in parallel or individually.

General settings for SNMP are possible, e.g., via the WBM "Configuration of general SNMP parameters" page.

Table 48: 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.	

3.5.3.4.1 SNMP v1/v2c

SNMP v1 and v2c is a community message exchange within a network community with a common community name.

The community name can be used to establish relationships between SNMP managers (trap recipients) and agents, which are each referred to as the community. The communities control identification and access between SNMP subscribers.
The community name can be evaluated by the trap receiver.
To use the SNMP protocol, a valid community name must always be specified.
The community name can be up to 32 characters long and contain no spaces. The default value is "public."

The access rights for the community and SNMP version via which the traps are to be sent can be set.

Settings for the SNMP v1/v2c parameters are possible, e.g., via the WBM "Configuration of SNMP v1/v2c Parameters" page.

Communities

A separate "Community <n>" area is displayed for each configured community.
If no community has been configured, "(no communities configured)" is displayed.

You can add a new community in the "Add new Community" area.

Table 49: 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

Trap Receiver

A separate "Trap Receiver <n>" area is displayed for each configured trap receiver.
If no trap receiver has been configured, "(no Trap Receivers configured)" is displayed.

You can create a new trap receiver in the "Add new Trap Receiver" area.

Table 50: WBM "Configuration of SNMP v1/v2cparameters" Page – "Trap Receivers" Group

Parameters	Explanation
Host	Hostname or IP address of the trap receiver (management station)

Parameters	Explanation
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

3.5.3.4.2 SNMP v3

SNMP v3 is used in security-relevant networks. The user data of the SNMP messages can be transmitted in encrypted form and requested values and values to be written cannot be listened to via ETHERNET.

It is possible to configure a password authentication and an encryption code.

The username must be unique; an existing username will not be accepted when entering a new one.
The username must be at least 8 characters long and may be a maximum of 32 characters long.
The username may contain lowercase letters (a … z), uppercase letters (A … Z), numbers (0 … 9), special characters (! () * ~ ' . – _) and no spaces.

The password (authentication key) and the encryption code (privacy key) must be at least 8 characters long and no more than 32 characters long.
The password and encryption code may contain lowercase letters (a … z), uppercase letters (A … Z), numbers (0 … 9), special characters (! () * ~ ' . – _) and no spaces.

Settings for the SNMP v3 parameters are possible, e.g., via the WBM "Configuration of SNMP v3 Parameters" page.

User

A separate "User <n>" area is displayed for each configured v3 user.
If no v3 user has been configured, "(no Users configured)" is displayed.

You can create a new v3 user in the "Add new v3 User" section.
You can create up to 10 users.

Table 51: 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

Parameters	Explanation
Access	Access rights for the v3 user; possible values are: ▪ ReadOnly ▪ ReadWrite

Trap Receiver

A separate "Trap Receiver <n>" area is displayed for each configured v3 trap receiver.
If no v3 trap receiver has been configured, "(no Trap Receivers configured)" is displayed.

You can create a new v3 trap receiver in the "Add new Trap Receiver" area.
You can create a maximum of 10 trap receivers.

Table 52: 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

3.5.3.5 FTP/FTPS

Table 53: 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.

Table 54: 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.

3.5.3.6 HTTP/HTTPS

Table 55: 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.

Table 56: 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.

3.5.3.7 I/O-CHECK

ⓘ 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.

Table 57: 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.

3.5.3.8 SSH Server

Table 58: 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.	

Parameters	Explanation
Allow password login	Enable or disable password request.

3.5.3.9 Docker®

Table 59: 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.

3.6 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.

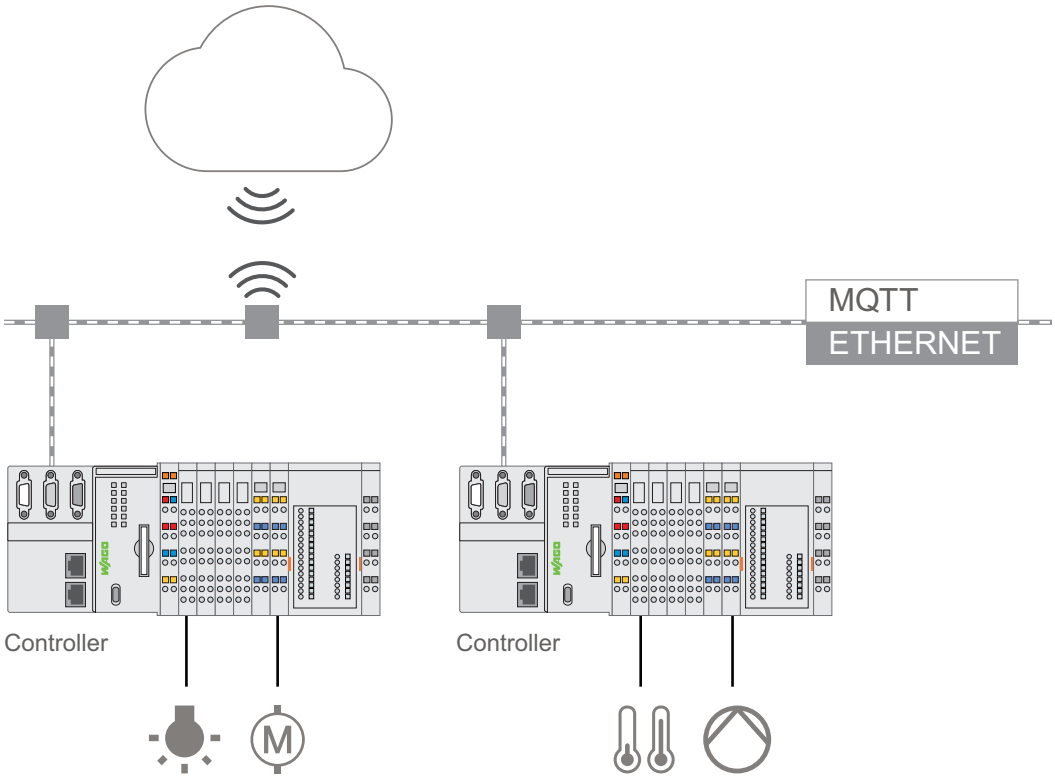

Figure 5: Connecting the Controllers to a Cloud Service (Example)

Data is transmitted from the controller to the cloud service as JSON files. The connection can be encrypted via TLS; see TLS Encryption.

You can find the settings that must be made in the controller to use the cloud connectivity functionality in the **Web-Based Management (WBM) [▸ 85]**.

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.

Table 60: 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.

Note

Observe the additional documentation!

You can find a detailed description of the "Cloud Connectivity" software package with a PFC100/200 and information on PLC programming in Application Note A500920 in the Downloads area at 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 61: 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

Table 62: 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

Parameters	Explanation
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
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

Parameters	Explanation
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>

Table 63: 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

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT Any-Cloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)
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 64: 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 65: 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 66: 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 67: 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		

3.7 Fieldbus Functions

3.7.1 OPC UA

Table 68: 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.	

Table 69: 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.	

3.7.2 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**.

Table 70: 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	

Table 71: WBM "BACnet Status" Page – "BACnet License" Group

Parameters	Explanation
Type	Display of BACnet licenses

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

Table 72: WBM "BACnet Status" Page – "BACnet Data Link" Group

Parameters	Explanation
Connection Info	Display of the connection status

Table 73: WBM "BACnet Configuration" Page – "PLC Runtime" Group

Parameters	Explanation
[Restart]	Restart runtime

Table 74: 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.
	☑	I-Am messages are sent to the BACnet broadcast address.

Table 75: 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.
override.xml Chose file ...	Select the required file on the PC
[Upload]	Transfer the selected file from the PC to the controller

Table 76: WBM "BACnet Configuration" Page – "BACnet Log Level" Group

Parameters	Explanation	
Error	Enable/disable error log outputs.	
	☐	Error log entries are not output.

Parameters	Explanation	
	☑	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.

Table 77: 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.
	☑	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.
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.	

Table 78: WBM "BACnet Data Link" Page – "BACnet Restart" Group

Parameters	Explanation
[Restart]	Restart the BACnet service

Table 79: WBM "BACnet Data Link" Page – "BACnet/IP" Group

Parameters	Explanation
Port Number	Input of the port for BACnet/IP communication

Table 80: 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.

Parameters	Explanation
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.

Table 81: 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.

Table 82: 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.

Table 83: 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

Table 84: WBM "BACnet Data Link" Page – "BACnet/SC Default Certificates" Group

Parameters	Explanation
[Generate]	Generation of a new certificate

Table 85: 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.

Table 86: 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.

Table 87: 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.
	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.

3.7.3 CANopen Master and Slave

In accordance with IEC 61131-3 programming, the process data is processed on site in the controller. The process results can be output directly to the actuators, or transmitted via the bus.

Process data is exchanged with PDOs and SDOs. To send process data via the CANopen fieldbus, the controller supports 512 TXPDOs and 512 RX PDOs and 128 SDOs.

In the local process image, a range of 4096 bytes serves as each input and output range for data exchange via the CANopen interface. Direct access to the I/O modules via the fieldbus is not provided.

All entries of the process image can be mapped as required to the RX PDOs and TX PDOs. The entire input and output data area can be read and written via SDOs.

After initialization, CANopen communication runs independently of the IEC application. When used as a CANopen slave, the baud rate and bus address can be changed according to the CANopen-LSS protocol.

3.7.3.1 Object Dictionary

All CANopen communication and process data objects are summarized in the object directory.

The following table provides a general overview of the definition in the CANopen definition:

Table 88: Overview of Addresses in the Object Directory

Index Range	Use
0000	Not used
0001-009F	Data Types
00A0-0FFF	Reserved (addresses used for other services)
1000-1FFF	Communication Profile
2000-5FFF	Vendor-specific range
6000-9FFF	Up to 8 standardized device profiles
A000-AFFF	Process images from IEC61131 devices
B000-BFFF	Process images from CANopen gateways to CiA 302-7
C000-FFFF	Reserved

The relevant objects available at the PFC are described below.

3.7.3.2 Communication Profile

0x1000 Device type

The stack reports on the bus as a DS-405 (IEC61131-3 programmable device) device, regardless of whether it is configured as a master or as a slave. Since direct access to the I/O modules is not permitted via the bus, the bits for information about inputs and outputs are 0.

Entry 0x000195 = DS 405 for master and slave

0x1001 Error Register

This entry contains 8 bit information about the error status. At present, bit 4 is used specifically for communication and bit 5 for the device profile. Bit 0 is set for each error.

0x1003 Pre-defined Error Field

This entry contains the list of accumulated errors that were signaled in Error Register 0x1001. Subindex 0 contains the number of entries. If a new error occurs, it is added to subindex 1 and all existing errors are moved down one sub-index. A maximum of 20 error entries is supported. If more than 20 errors occur, the error at sub-index 20 is overwritten. By writing a "0" to sub-index 0, the entire error memory is deleted.

Standard values: 0 in all entries

0x1005 COB IB Sync

This objects defines the COB ID for the synchronization message.

Default: 0x80

0x1006 Communication Cycle Period

The cycle length of the synchronization cycle in µs or 0 for no cyclic synchronization. Internal resolution is 1ms. If this value is 0, SYNC monitoring does not take place.

Default: 0

0x1008 Manufacturer Device Name

This object specifies the device name.

Item: Item number of the PFC200, e.g., "750-8216"

0x1009 Manufacturer Hardware Version

Entry: "V 1.0" or higher

0x100A Manufacturer Software Version

Item: "04.02.05(00)" or higher

0x100C Node Guarding Time

The object indicates the guarding time in milliseconds. An NMT master cyclically queries the NMT slave for its status. The time between two requests is the "Guard Time."

Default: 0 (Node guarding disabled)

0x100D Life Time Factor

The Life Time Factor is part of the Node Guarding Protocol. The NMT slave checks whether it was queried within the Node Life Time (guard time multiplied by the Life Time Factor). If not, the slave must assume that the NMT master is no longer in normal operation; it then initiates a life guarding event.

Default: 0 (Node guarding off)

0x1012h COB-ID Time Stamp Object

The time stamp object enables every device's clock on the bus to be synchronized. The ID for this object is indicated here. The synchronization signal is not evaluated by Runtime itself, but can be used with library functions.

Default: 0x100 (Time Stamp Consumer)

0x1014h Emergency COB ID

An emergency message is transmitted in the event of CANopen device errors. The ID for this object is specified here (for the master read-only).

Default: 0x80 + Device ID

0x1015h Emergency inhibit time

This object specifies the minimum time that must elapse before another emergency object is sent. An entry equal to zero disables delayed sending. One time unit is 100µs.

Default: 0

0x1016h Consumer heartbeat time

This entry can be used for monitoring of other devices on the bus. A check is made to determine whether each module defined in this object has generated a heartbeat within the set time. If the set time has been exceeded, a heartbeat event is triggered. The "Heartbeat

Time" is entered in milliseconds. If the time is 0, monitoring is disabled. The number of devices to be monitored is entered in index 0, the heartbeat time is entered in ms in the bottom 16 bits and the ID of the bus device in the 8 bits above that.

Default:

Index 0: 0 (currently still 127 = Number of possible entries)

All other entries are 0 (this function is not yet supported by the CAN master in Firmware 1.0).

0x1017h Producer heartbeat time

This object defines the time (in milliseconds) between two transmitted heartbeat messages. No heartbeat is sent if the time is set to 0.

Default: 0

0x1018h Identity

This object specifies the device being used. The manufacturer ID contains a unique number for each vendor. WAGO has been assigned an ID of 33.

The product code contains the device identifier.

The Rev. No. contains a specific CANopen behavior. The Major Rev. No. contains the CANopen functionality. If the functionality is changed, the Major Rev. No. is increased. You can use the Minor Rev. No. to distinguish between different versions with the same CANopen behavior.

The number is independent of the firmware revision. When used as a CANopen slave with CODESYS 3.5, the vendor ID, product code and revision number can be freely defined in the slave configuration.

Subindex 0	Number of entries:	4
Subindex 1	Vendor ID	33
Subindex 2	Product_code:	e.g., 8216 for 750-8216
Subindex 3	Revision_number:	0x00010003 or higher
Subindex 4	Serial_number	corresponds to the last 4 bytes of the MAC address.

0x1200 Server SDO Parameter Channels

The communication parameters for an SDO as the server are entered here. 1 server SDO channel is supported.

0x1280 … 0x128E Client SDO Parameter Channels

The communication parameters for an SDO transfer as the client are entered here. 16 client SDO channels are supported.

0x1029h Error behavior

This object defines how the slave responds in the event of an error.

Subindex 0	Number of entries:	1	
Subindex 1	Communication Error:	1	No change (default)
		0	Switching from Operational to Preoperational
		2	Switch to Stop

0x1F51 Program Control

The status of the PLC can be read out using this object. Writing is prohibited.

Entries: 0 = Stop 1 = Run 2 = Reset 3 = Clear

3.7.3.2.1 Master Configuration

These objects are only available at the bus end when the master has been configured.

0x102A NMT Inhibit Time

This object indicates the minimum time that must elapse before another NMT telegram is sent. An entry equal to zero disables delayed sending. One time unit is 100 µs.

Default: 0

0x1F80 NMT Startup

This object contains the configuration bits for the master status. If automatic startup is disabled, the master can be started by writing of 0x1F to this object.

0x1F81 ... 0x1F8A Slave Configuration

The configured slaves are entered in these lists. All of the entries are checked when the master is started and transferred to the slaves.

0x1F81 NMT Slave Assignment

Subindex 0:	128 = Number of possible entries	
Subindex 1 ... 128:	Bit 0:	Slave present
	Bit 2:	Slave is mandatory at startup
	Bit 3:	Slave reset is performed at startup.
	Bit 8 ... 15:	Guard Retry Factor
	Bit 16 ... 31:	Guard Time
Subindex 128:	Entire network (write-only)	

0x1F82 Request NMT

Subindex 0: 127 = Number of possible entries

Subindex = Master Node ID NMT State of the master

0x1F84 Device type identification

Subindex 0: 127 = Number of possible entries

Subindex 1 ... 127: Device Type of the slave

0x1F85 Vendor identification

Subindex 0: 127 = Number of possible entries

Subindex 1 ... 127: Vendor identification of the slave (not used by default)

0x1F86 Product code

Subindex 0: 127 = Number of possible entries

Subindex 1 ... 127: Product code of the slave (not used by default)

0x1F87 Revision number

Subindex 0: 127 = Number of possible entries

Subindex 1 ... 127: Revision number of the slave (not used by default)

0x1F88 Serial number

Subindex 0: 127 = Number of possible entries

Subindex 1 ... 127: Serial number of the slave (not used by default)

0x1F89 Boot Time

Time in ms between start of the slaves and operational readiness of all slaves

Default: 0 = disabled

0x1F8A Restore configuration

Subindex 0: 127 = Number of possible entries

Subindex 1 ... 127: Bit 0 = 1 Send Restore Configuration on start to slave

3.7.3.3 Data Exchange

The exchange of process data takes place with the CANopen fieldbus controller via the communication objects.

Each object consists of a CAN telegram with a maximum of 8 bytes process data and a COB (Communication Object Identifier) ID that is unique within the network.

These communication objects transmit data, trigger events, signal error statuses, etc.

The parameters required for the communication objects as well as CANopen device parameters and data are stored in an object directory.

3.7.3.3.1 Controller Communication Objects

The controller supports the following communication objects:

- 512 Tx-PDOs for process data exchange from input data of the fieldbus node
- 512 Rx-PDOs for process data exchange from output data of the fieldbus node
- Synchronization objects (SYNC) for network synchronization
- Emergency Objects (EMCY)
- Network Management Objects
  - Module Control Protocols,
  - Error Control Protocols, kte
  - Bootup Protocol.

3.7.3.3.2 Fieldbus-Specific Addressing

After configuring the CAN interface as a master or slave, the CODESYS variables for the CAN bus are mapped in an object directory (initialization). A CANopen fieldbus device uses the 16-bit indices and 8-bit sub-indices of the object directory to address data via PDOs or SDOs and to access the data. The position of the data in the process image is therefore not directly significant for the CANopen user at the fieldbus end.

The variables entered into the object directory are distinguished by data type (Integer8, Unsigned8, Boolean, Integer16, etc.) and by input/output. Access via PDOs can be either for reading or writing.

As CANopen does not transfer data by bits, the variable data is combined from a Boolean data type to bytes and assigned to the corresponding index; Boolean input variable data is assigned to index 0xA080, Boolean output variable data to index 0xA500.

Variable data that has a data width of 1 byte or more is assigned to the corresponding indices in a similar manner.

Note

Observe the direction of data flow!

The IEC 61131-3 input and output variables are defined from the perspective of the CAN fieldbus,
i.e.:
IEC 61131-3 input variables are PFC output variables and
IEC 61131-3 output variables are PFC input variables.

This table provides an overview of the indices of "IEC 61131-3" variables.

Table 89: Indexing of the "IEC 61131-3" variable data in the object directory

Data Type	"IEC 61131-3" Output Variables	"IEC 61131-3" Input Variables
	Index	
Integer8	0xA000	0xA480
Unsigned8	0xA040	0xA4C0
Boolean	0xA080	0xA500
Integer 16	0xA0C0	0xA540
Unsigned16	0xA100	0xA580
Integer24	0xA140	0xA5C0
Unsigned24	0xA180	0xA600
Integer32	0xA1C0	0xA640
Unsigned32	0xA200	0xA680
Float32	0xA240	0xA6C0
Unsigned40	0xA280	0xA700
Integer40	0xA2C0	0xA740
Unsigned48	0xA300	0xA780
Integer48	0xA340	0xA7C0
Unsigned56	0xA380	0xA800
Integer56	0xA3C0	0xA840
Integer64	0xA400	0xA880
Unsigned64	0xA440	0xA8C0

Using the associated indices for data types with a data width of 1 byte (Integer8, Unsigned8 and Boolean), read-only byte-by-byte access is possible from the fieldbus to data in the controller memory.

The sub-index is utilized to select a specific byte.

In contrast, when the indices for larger data blocks are used, several bytes can be accessed simultaneously.
For example, the described PFC output variable data can be accessed in a word-by-word manner using the index for Integer16 (0xA0C0) or for Unsigned16 (0xA100), three bytes can be accessed using index 0xA140 for Integer24, etc.

Example:

The first three bytes of the PFC output data for the data type integer or unsigned are accessed from the fieldbus:

Table 90: Fieldbus Access to the PFC Output Data

Access	PFC Output Data	Read with the index (Integer / Unsigned)	Sub-Index
Byte by byte (with Integer8 / Unsigned8)	Byte 6000	(0xA000 / 0xA040)	1
	Byte 6001	(0xA000 / 0xA040)	2
	Byte 6002	(0xA000 / 0xA040)	3
Word by word (with Integer16 / Unsigned16)	Word 3000 (byte 6000/6001)	(0xA0C0 / 0xA100)	1
	Word 3001 (byte 6002/6003)	(0xA0C0 / 0xA100)	2
3 bytes (with Integer24 / Unsigned24)	Bytes 6000 ... 6002	(0xA140 / 0xA180)	1

The following tables give an overview of addressing data with different data widths.

In this case, the corresponding indexing is assigned to the memory space for fieldbus variables (byte 6000 to byte 9999) as a function of the data width.

The indexing indicated in the tables continues up to the respective maximum index and sub-index.

Note t.b.d. (as above ???)

Figure t.b.d.

3.7.3.3.3 Examples of PFC Fieldbus Variable Definitions

The examples below show the allocation of several definitions for PFC variables with different data types to the associated object directory entries.

3.7.3.3.3.1 CODESYS Access to PFC Variables

Table 91: Examples of CODESYS Access to PFC Variables

Data Type of PFC Variables	PFC Input Variables		PFC Output Variables	
	Definition per IEC 61131-3	Index/sub-index	Definition per IEC 61131-3	Index/sub-index
Unsigned8	InByte0 AT %IB6000: BYTE;	0xA4C0/1	OutByte0 AT %QB6000: BYTE;	0xA040 /1
	InByte0 AT %IB6001: BYTE;	0xA4C0/2	OutByte0 AT %QB6001: BYTE;	0xA040 /2
Integer 16	InInt0 AT %IW3000: INT;	0xA540 /1	OutInt0 AT %QW3000: INT;	0xA0C0/1
	InInt1 AT %IW3001: INT;	0xA540 /2	OutInt1 AT %QW3001: INT;	0xA0C0/2

Data Type of PFC Variables	PFC Input Variables		PFC Output Variables	
	Definition per IEC 61131-3	Index/sub-index	Definition per IEC 61131-3	Index/sub-index
Unsigned16	InWord0 AT %IW3000: WORD;	0xA580 /1	OutWord0 AT %QW3000: WORD;	0xA100 /1
	InWord0 AT %IW3001: WORD;	0xA580 /2	OutWord0 AT %QW3001: WORD;	0xA100 /2
Unsigned32	InDWord0 AT %ID1500: DWORD;	0xA680 /1	OutDWord0 AT %QD1500: DWORD;	0xA200 /1
	InDWord0 AT %ID1501: DWORD;	0xA680 /2	OutDWord0 AT %QD1501: DWORD;	0xA200 /2

3.7.3.3.3.2 Maximum Indices

The maximum indices and sub-indices are a result of the memory size of the fieldbus controller with 4096 bytes, as well as the respective data width of the data types.

The table provides an overview of the maximum indices and sub-indices of the IEC 61131-3 variables.

Table 92: Maximum indices and sub-indices for "IEC 61131-3" variables

Data Type	"IEC 61131-3" Output Variables		"IEC 61131-3" Input Variables	
	Max. Index	Max. sub-index	Max. Index	Max. sub-index
Integer8	0xA00F	0xFF	0xA487	0xFF
Unsigned8	0xA04F	0xFF	0xA4C7	0xFF
Boolean	0xA08F	0xFF	0xA507	0xFF
Integer 16	0xA0C7	0xFF	0xA543	0xFF
Unsigned16	0xA107	0xFF	0xA583	0xFF
Integer24	0xA145	0x55	0xA5C0	0x55
Unsigned24	0xA185	0x55	0xA600	0x55
Integer32	0xA1C3	0xFF	0xA643	0xFF
Unsigned32	0xA203	0xFF	0xA683	0xFF
Float32	0xA243	0xFF	0xA6C3	0xFF
Unsigned40	0xA283	0x33	0xA703	0x33
Integer40	0xA2C3	0x33	0xA743	0x33
Unsigned48	0xA302	0xAA	0xA780	0xAA
Integer48	0xA342	0xAA	0xA7C0	0xAA
Unsigned56	0xA382	0x49	0xA802	0x49
Integer56	0xA3C2	0x49	0xA842	0x49
Integer64	0xA401	0xFF	0xA880	0xFF
Unsigned64	0xA441	0xFF	0xA8C0	0xFF

Example:

514 bytes of output variables are addressed by word by the data type Unsigned16.

Addressing of 257 data words then occurs with:

- Index 0xA580, sub-index 1 to 255 and
- Index 0xA581, sub-index 1 and 2.

Table 93: Example of "IEC 61131-3" Output Variables

Index	Sub-Index	Content	Description
0xA580	1	D1 *)	1st output variable block

Index	Sub-Index	Content	Description
	2	D2 *)	2st output variable block
	...	...	...
	255	D255 *)	255. Output variable block
0xA581	1	D256 *)	256st output variable block
	2	D257 *)	257st output variable block

*) D1 = Data word output variable 1, D255 = Data word output variable 255, etc.

3.7.3.3.4 Using the CANopen Slave (Device) under CODESYS V3

The CODESYS 3.5 slave configurator uses other object addresses for the process data than defined in the CANopen CiA 405 standard for IEC 61131 devices. Therefore, when operating as a CODESYS V3 slave, the CODESYS V3 object numbers are used:

0x3000 .. 0x31FF	Process data receipt (master => slave)
0x3800 .. 0x39FF	Send process data (slave => master)
0x5000 .. 0x507F	Read/write SDO access
0x5800 .. 0x587F	SDO Read Access

A more detailed description on how to use the CANopen interface is provided in the CODESYS V3 online manual. The WAGO-specific functions can be used via the WagoAppCanOpen and WagoAppCanLayer2 libraries.

3.7.3.3.5 Use as a CAN Layer 2 Device

As an alternative to the CANopen master or slave function, a pure Layer2 stack is also available on the controller. This can be used when no CANopen functions are required. It offers higher data throughput with a lower CPU load.

It is possible to set 127 receive filters with a total buffer of 127 telegrams or to use an unfiltered receive buffer of 255 telegrams.

The WAGO CanLayer2 device is selected on CAN for use with CODESYS V3. This functionality is used via the WagoAppCanLayer2 library.

3.8 Memory Functions

3.8.1 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.

3.8.1.1 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 94: WBM "Firmware Backup" Page – "Firmware Backup" Group

Parameters	Explanation
Boot Device	Storage medium from which the device was booted

Parameters	Explanation	
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.	

3.8.1.2 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".

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.

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.

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

Table 95: 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.

Parameters	Explanation	
	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.	

3.8.2 Memory Card Function

3.8.2.1 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.

3.8.2.2 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.

3.8.2.3 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 botted 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.

3.8.2.4 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 96: 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

3.9 Diagnostic Functions

3.9.1 Diagnostics via Indicators

Various indicators on the product allow direct diagnostics, e.g., LEDs for power supply, system, fieldbus and network.

The number and type of indicators depends on the product. The diagnostics for these indicators are described in the respective product manuals.

The blink sequences described in the following sections apply to all products listed in the scope of this document.

3.9.1.1 Diagnostics via Blink Sequences

Blink Sequences

A diagnosis (fault/error) is always displayed as three blink sequences in a cyclic manner:

1. The first blink sequence initiates the output of the error code and the error argument by flickering (10 Hz).
2. The second blink sequence flashes (1 Hz) the error code.
3. The third blink sequence flashes (1 Hz) the error argument.

Example of a Diagnostic Message via Blink Sequences

The example below illustrates the representation of a diagnostics message via the blink sequence. The "I/O" LED indicates a data error on the local bus. The data error is caused by the removal of an I/O module located at the 6th position of the fieldbus node.

Initiation of the Start Phase

1. The "I/O" LED flashes once in a cycle of approx. 10 Hz.

2. This is followed by a pause of approx. 1 second.

Error code 4: data error on the local bus

3. The "I/O" LED flashes for 4 cycles of approx. 1 Hz.

4. This is followed by a pause of approx. 1 second.

Error argument 5: I/O module in the 6th slot

5. The "I/O" LED flashes for 5 cycles of 1 Hz. This means that there is an interruption on the local bus after the 5th I/O module.

6. The blink sequence starts flickering when the start phase is initiated again. If there is only one error, this process is repeated.

3.9.1.1.1 I/O LED Error Codes

Table 97: Overview of "I/O" LED Error Codes

Error Code	Explanation
1	Hardware and configuration error
2	Configuration error
3	Local bus protocol error
4	Physical error on the local bus
5	Local bus initialization error
6	Not used
7	Unsupported I/O module
8	Not used
9	CPU exception error

Error Code 1 – Hardware and Configuration Error

Table 98: Error Code 1 – Hardware and Configuration Error: Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Corrective Action
-	Invalid parameter checksum for local bus interface	1. Switch off the power supply to the controller. 2. Switch out the controller. 3. Switch the power supply on again.
1	Internal buffer overflow (max. amount of data exceeded) during inline code generation.	1. Switch off the power supply to the controller. 2. Reduce the number of I/O modules. 3. Switch the power supply on again.
2	I/O module(s) with unsupported data type	1. Update the controller firmware. If the error persists, there is an error in an I/O module. Determine the error as follows: 2. Switch off the power supply to the controller. 3. Place the end module in the middle of the connected I/O modules. 4. Switch the power supply on again. 5. If the LED flashes red, switch the power supply back off and place the end module in the middle of the first half of the I/O modules (toward the controller). 6. If the LED is no longer flashing, switch the power supply off and place the end module in the middle of the second half of the I/O modules (away from the controller). 7. Switch the power supply on again. 8. Repeat this procedure until you establish which I/O module is defective. Then replace that module.
3	Unknown flash program memory module type	1. Switch off the power supply to the controller. 2. Switch out the controller. 3. Switch the power supply on again.
4	Error occurred while writing to the flash memory	1. Switch off the power supply to the controller. 2. Switch out the controller. 3. Switch the power supply on again.
5	Error occurred while erasing a flash sector	-
6	The I/O module configuration after a local bus reset does not match the I/O module configuration after the last controller start.	▪ Restart the controller by first switching off the power supply and then switching it back on, or by pressing the Reset button on the controller.
7	Error occurred while writing to the serial EEPROM	1. Switch off the power supply to the controller. 2. Switch out the controller. 3. Switch the power supply on again.
8	Invalid hardware/firmware combination	-
9	Invalid checksum in the serial EEPROM	-
10	Fault when initializing the serial EEPROM	-
11	Error occurred while reading from the serial EEPROM	1. Switch off the power supply to the controller. 2. Reduce the number of I/O modules. 3. Switch the power supply on again.
12	Time to access the serial EEPROM exceeded	1. Switch off the power supply to the controller. 2. Switch out the controller. 3. Switch the power supply on again.
14	Maximum number of gateway or mailbox modules exceeded	1. Switch off the power supply to the controller. 2. Reduce the number of gateway or mailbox modules. 3. Switch the power supply on again.

Error Argument	Cause	Corrective Action
16	Maximum number of I/O modules exceeded	1. Switch off the power supply to the controller. 2. Reduce the number of I/O modules. 3. Switch the power supply on again.

Error Code 2 – Configuration Error

Table 99: Error Code 2 – Configuration Error: Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Corrective Action
2	Maximum size of the process image exceeded	1. Switch off the power supply to the controller. 2. Reduce the number of I/O modules. 3. Switch the power supply on again.

Error Code 3 – Local Bus Protocol Error

Table 100: Error Code 3 – Local Bus Protocol Error: Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Corrective Action
-	Local bus communication fault; defective I/O module cannot be identified.	✓ If a power supply module (e.g., 750-602) is connected to the controller, make sure that it is working. If the supply module is free of errors, then there is a fault on an I/O module. Identify the I/O module as follows: 1. Switch off the power supply to the controller. 2. Place the end module in the middle of the connected I/O modules. 3. Switch the power supply on again. 4. If the I/O LED flashes red, switch the power supply back off and place the end module in the middle of the first half of the I/O modules (toward the controller). ✓ If only one I/O module remains, but the LED is still flashing, then this module or the local bus interface of the controller is faulty. Replace the defective I/O module or controller: 1. If the LED is no longer flashing, switch the power supply off and place the end module in the middle of the second half of the I/O modules (away from the controller). 2. Switch the power supply on again. 3. Repeat this procedure until you establish which I/O module is defective. Then replace that module.

Error Code 4 – Physical Error on the Local Bus

Table 101: Error Code 4 – Local Bus Physical Error: Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Corrective Action
-	Maximum permissible number of I/O modules exceeded	1. Switch off the power supply to the controller. 2. Reduce the number of I/O modules to an acceptable value. 3. Switch the power supply on again.
n*	Local bus interruption after the nth I/O module with process data.	1. Switch off the power supply to the controller. 2. Replace the (n+1)th I/O module with process data. 3. Switch the power supply on again. *) I/O modules that do not provide process data are ignored (e.g., supply module without diagnostics).

Error Code 5 – Local Bus Initialization Error

Table 102: Error Code 5 – Local Bus Initialization Error: Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Corrective Action
n*	Error in register communication during local bus initialization	1. Switch off the power supply to the controller. 2. Replace the (n+1)th I/O module with process data. 3. Switch the power supply on again. *) I/O modules that do not provide process data are ignored (e.g., supply module without diagnostics).

Error Code 7 – Unsupported I/O Module

Table 103: Error Code 7 – Unsupported I/O Module: Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Corrective Action
n	First non-supported I/O module at position n	1. Switch off the power supply to the controller. 2. Replace the nth I/O module with process data, or reduce the number of I/O modules to n-1. 3. Switch the power supply on again.

Error Code 9 – CPU Exception Error

Table 104: Error Code 9 – Exception Error: Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Corrective Action
1	Invalid program statement	Malfunction of the program sequence: ▪ Contact WAGO Support.
2	Stack overflow	Malfunction of the program sequence: ▪ Contact WAGO Support.
3	Stack underflow	Malfunction of the program sequence: ▪ Contact WAGO Support.
4	Invalid event (NMI)	Malfunction of the program sequence: ▪ Contact WAGO Support.
5	The local bus watchdog has responded.	✓ For CODESYS applications: ▪ Contact WAGO Support. ✓ For C applications: ▪ Check the time monitoring settings.

3.9.1.1.2 MS LED Error Codes

Table 105: Overview of "MS" LED Error Codes

Error Code	Explanation
1	Configuration error

Table 106: Error Code 1 – Configuration Error: Explanation of Blink Codes and Procedures for Troubleshooting

Error Argument	Cause	Remedy
5	Error when synchronizing the PLC configuration with the local bus	1. Check the information of the connected I/O modules in the CODESYS controller configuration. 2. Adjust this to match the I/O modules actually inserted. 3. Recompile the project. 4. Reload the project into the controller.

3.9.2 Diagnostics via WBM

Table 107: 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/*`

Table 108: WBM "Download" Page – "Diagnostic Information" Group

Parameters	Explanation
[Download]	Download diagnostic information from device

Table 109: 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"

Table 110: 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.	

Table 111: 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.

Table 112: WBM "Network Capture" Page – "Log Download" Group

Parameters	Explanation
Select Log File	Select the recording to be downloaded from the product.

4 Commissioning

4.1 Switching On the Controller

Before switching on the controller ensure that you have:

- Properly installed the controller (see Section "Installation")
- Connected all required data cables (see Section "Connections") to the corresponding interfaces and have secured the connectors by their attached locking screws
- Connected the system- and field-side power supply (see Section "Connections")
- Inserted the end module (see System Description)
- Performed appropriate potential equalization at your machine/system (see System Description)
- Performed shielding properly (see System Description)

To switch on both the controller and the connected I/O modules, switch on your power supply unit.

Starting of the controller is indicated by brief flashing of all LEDs.

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

The CODESYS V3 runtime system starts simultaneously.

Once the entire system has been successfully started, the SYS and I/O LEDs light up green.

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).

4.2 Determining the IP Address of the Host PC

To ensure that the host PC can communicate with the controller via ETHERNET, the host PC and controller must be located in the same subnet.

To determine the IP address of the host PC (with the Microsoft Windows® operating system) using the MS DOS prompt, proceed as follows:

1. Open the command prompt. Enter the "cmd" command in the input field under **Start** > **Windows System** >**Execute** (Windows® 10) or **Start** > **Search programs/files** (Windows® 7).
2. Click the **[OK]** button or press ***Enter*** to confirm the entry.
3. Enter the "ipconfig" command at the command prompt.
4. Press ***Enter*** to confirm the entry.

➡ The IP address, subnet mask and standard gateway, including the associated parameters, are displayed.

4.3 Setting an IP Address

When the product is delivered, the following IP addressing is enabled for the ETHERNET interface (port X1 and port X2):

Table 113: 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")

- Use one of the existing configuration tools (e.g., WBM or WAGO Ethernet Settings) to adapt the IP addressing to your system structure so that a PC and the product can communicate with each other (see Configuration [▸ 85]).

Example of integrating the product (192.168.1.17) into an existing network:

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

Table 114: Network mask: 255.255.255.0

Host PC	Subnet address space for the product
192.168.1.2	**192.168.1.**1 or **192.168.1.**3 … **192.168.1.**254

4.3.1 IP Connection via USB (PFC300)

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.

4.3.2 Setting an 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.

4.3.3 Assigning an IP Address with 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.

4.3.4 Changing an IP Address with “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.

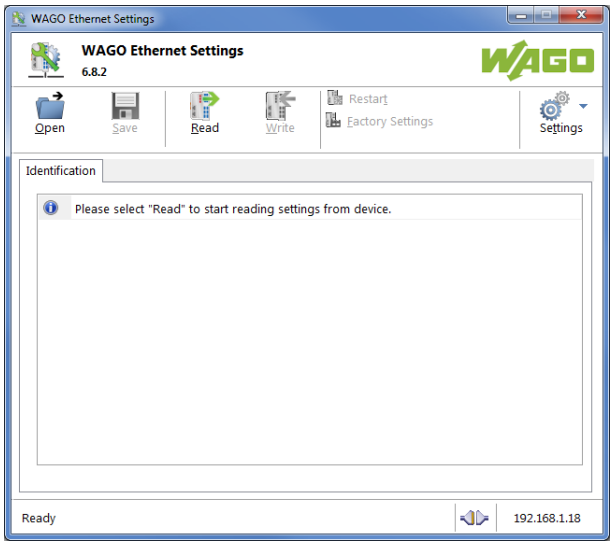

Figure 6: WAGO Ethernet Settings – Start Screen (Example Figure)

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

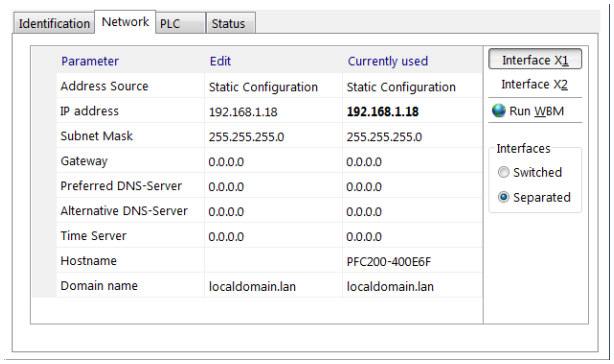

Figure 7: WAGO Ethernet Settings – Network Tab (Example Figure)

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.

4.3.5 Setting the IP Address with the Address selector switch

For products with an address selector switch, you can use this switch to change the network settings.

The address selection switch includes switches 1 ... 8 with the weight 1 ... 128. A disabled switch has the value 0. The set address value is derived from the sum of the weight of all enabled switches (example: Switches 7, 6 and 3 to "ON" corresponds to the address value 64 + 32 + 4 = 100). You can set an address value of 0 ... 255.

The address selection switch setting only queried when restarting the controller. Changing the switch positions during operation are ignored until the next restart.

If you operate the X1 and X2 ETHERNET interfaces in Separated mode, the settings only apply to the X1 interface. All settings remain unchanged for the X2 interface. If you operate the X1 and X2 ETHERNET interfaces in Switched mode, the settings apply to both the X1 and X2 interfaces.

The following table shows the significance of the address values of the address selection switch.

Table 115: Address Selection Switch

Address Value	Explanation
0	The IP parameters are set via the settings in the Web-Based Management (WBM) or by the factory settings.
1 … 254	A fixed IP address is assigned. The IP address consists of the network address and the address value setting. The network address can be configured via the WBM; the default value is 192.168.1.0 (subnet mask 255.255.255.0, default gateway 0.0.0.0).
255	The DHCP protocol is used to configure the IP parameters.

Examples:

The IP address setting is 192.168.129.129; the address selection switch is set to the value 203.

The entire fourth value of the IP address is replaced when the netmask is 255.255.255.0.

Netmask setting:	255.255.255.000
IP address setting:	192.168.129.129
Resulting network address:	192.168.129.000
Resulting device address:	---.---.---.129
Address selection switch:	---.---.---.203
Network address after restart:	192.168.129.000
Device address after restart:	---.---.---.203
IP address after restart:	192.168.129.203

254 addresses are possible and can be set (1 … 254).

If the netmask is higher (e.g., 255.255.255.240), the address value is limited. Only some of the DIP switches of the address switch are taken into account. In the following example, these are only switches 1 … 4. The setting of switches 5 … 8 is ignored:

Netmask setting:	255.255.255.240
IP address setting:	192.168.129.129
Resulting network address:	192.168.129.128
Resulting device address:	---.---.---.001
Address selection switch:	---.---.---.203
Network address after restart:	192.168.129.128
Device address after restart:	---.---.---.011
IP address after restart:	192.168.129.139

254 addresses can be set (1 … 254), but only 14 addresses (1 … 14) are possible.

If the netmask is lower (e.g., 255.255.240.000), the possible number of devices on one subnet increases, but only some of the possible device addresses can be set with the address switch.

Netmask setting:	255.255.240.000
IP address setting:	192.168.129.129
Resulting network address:	192.168.128.000
Resulting device address:	---.---.--1,129
Address selection switch:	---.---.---.203
Network address after restart:	192.168.128.000
Device address after restart:	---.---.---.203
IP address after restart:	192.168.128.203

4094 addresses are possible (1 ... 4094), but only 254 addresses can be set (1 ... 254).

4.3.6 Temporarily Set Fixed IP Addresses

This process temporarily sets the IP addresses for the network interfaces X1 ... X<n> to fixed IP addresses.
For each bridge used, the assigned interfaces are assigned their own address, whereby bridge 1 receives the IP address "192.168.1.17", bridge 2 the IP address "192.168.2.17" and so on.

No reset is carried out.

To set temporary fixed IP addresses, proceed as follows:

1. Set the mode selector 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.

If you make changes to the IP configuration of a bridge after enabling the temporary IP addresses, the new settings are permanently adopted and applied immediately. The configured bridge exits the temporary IP address mode. The other bridges keep the temporarily set IP address until restart / reset.

To cancel the setting, proceed as follows:

- Perform a software reset.

or

- Switch the product off and on again.

4.4 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.

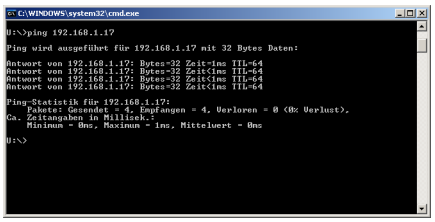

Figure 8: Example of a Functional Test

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

4.5 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 [▸ 34].

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.

4.6 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.

5 Configuration

5.1 Configuration in the 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.

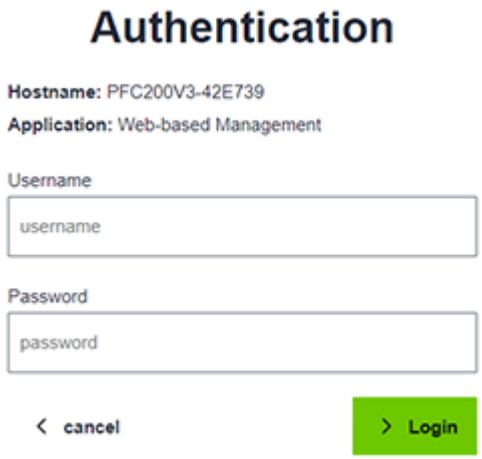

Figure 9: Log-in Window

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.

5.1.1 General Page Information

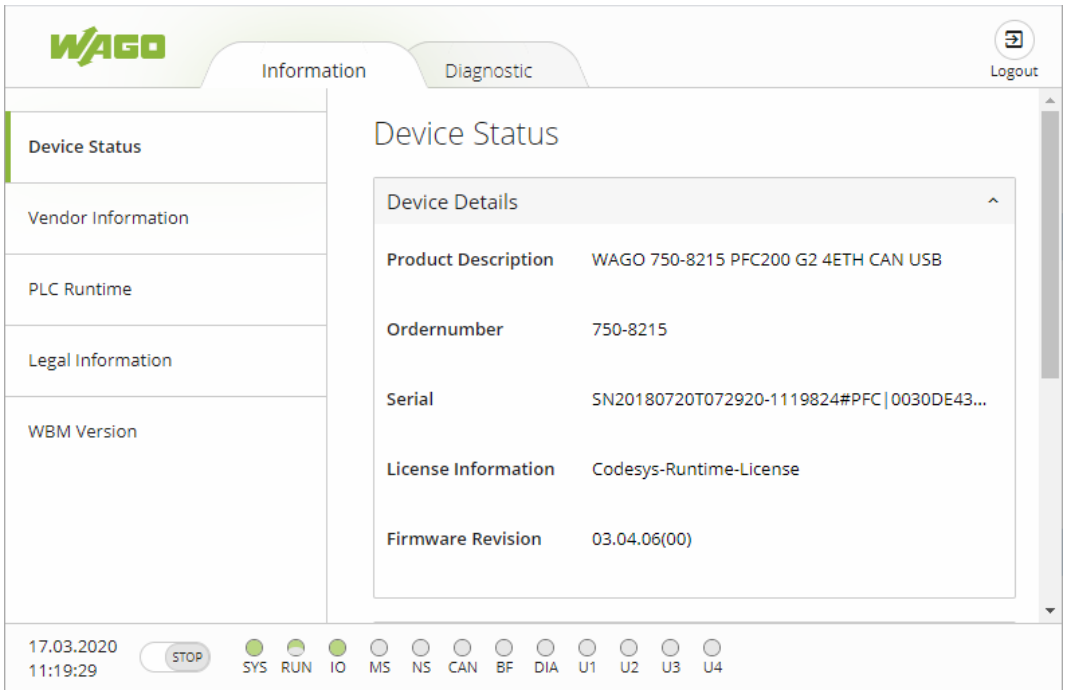

Figure 10: WBM Browser Window (Example)

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.

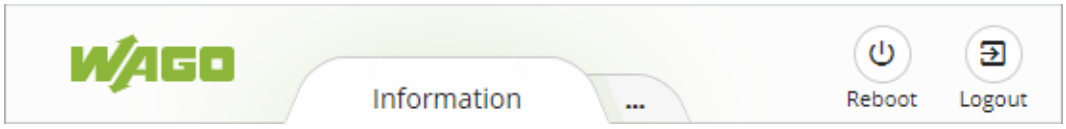

Figure 11: WBM Header with Tabs that Cannot be Displayed (Example)

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.

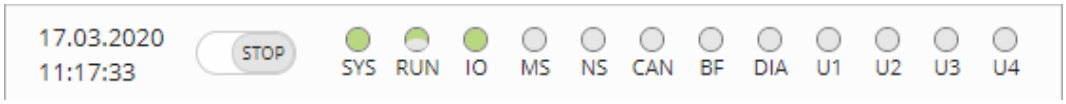

Figure 12: WBM Status Bar (Example)

- 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.

5.1.2 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 116: 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
		Trademarks Information	Trademarks Information	
	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 Domainname	user
		Routing	Routing	user
		STP/RSTP	Spanning Tree Protocol	user
	Clock		Clock Settings	user
	Administration			
		Serial Interface	Configuration of Serial Interface RS232/ RS485	admin
		Service Interface	Configuration of Service Interface	admin
		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

Tab	Navigation		WBM Page Title	User
		DHCP Server	DHCP Server Configuration	admin
		DNS	Configuration of DNS Server	admin
	Cloud Connectivity			
		Status	Status Overview	admin
		Connection <n>	Configuration of Connection <n>	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 Parameters	admin
	Commissioning		Commissioning Settings	admin
	Docker		DockerSettings	admin
	Users		WBM User Configuration	admin
	Modem		Configuration of internal 4G Modem	admin
Fieldbus	OPC UA		OPC UA Configuration	admin
	PROFIBUS DP		Configuration of PROFIBUS DP Slave	user
	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
	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

5.2 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.

ⓘ 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.

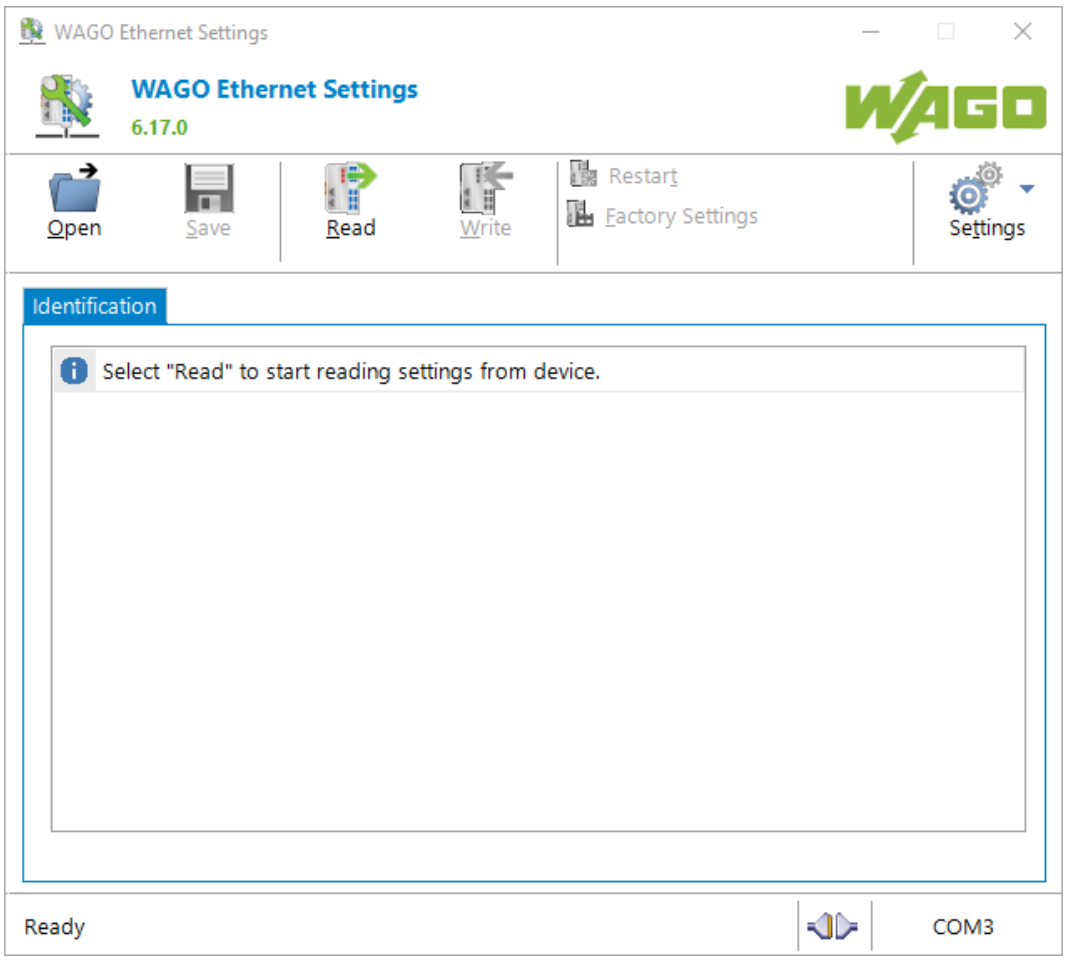

Figure 13: "WAGO Ethernet Settings" – Start Screen (Example)

- To do so, click "Settings" and then "Communication."

➡ In the "Communication Settings" window that then opens, modify the settings according to your needs.

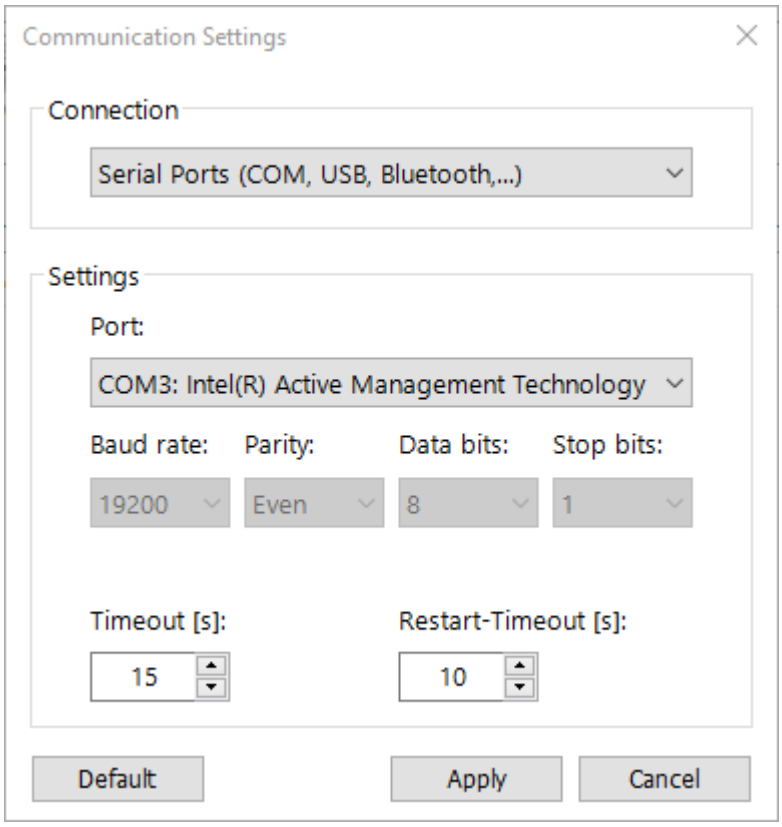

Figure 14: "WAGO ETHERNET Settings" – Communication Link (Example)

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]**.

5.2.1 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.

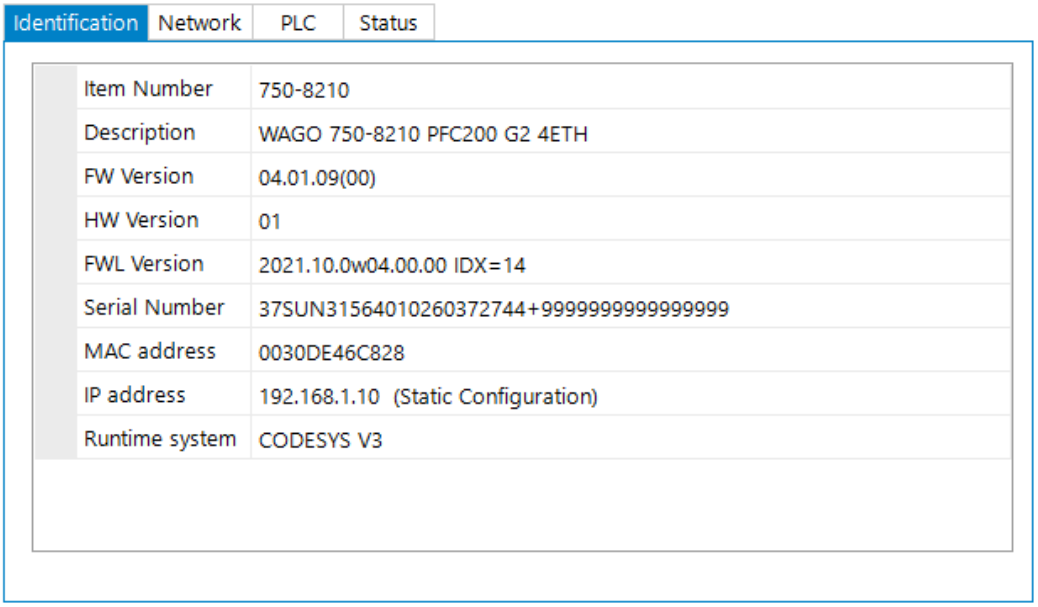

Figure 15: "WAGO Ethernet Settings" – Identification Tab (Example)

5.2.2 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.

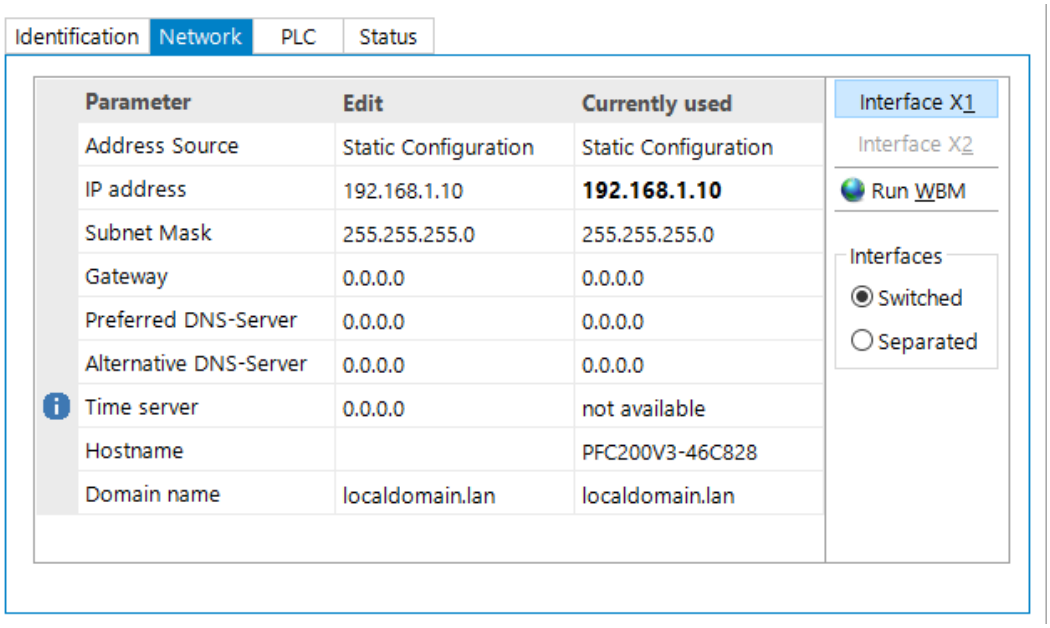

Figure 16: "WAGO Ethernet Settings" – Network Tab (Example)

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 it to set its system time via NTP.

Hostname

This indicates the controller's hostname. When delivered, the hostname is composed of the string "PFCx00-" and the last 3 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.

5.2.3 PLC Tab

Here you can select the runtime system.

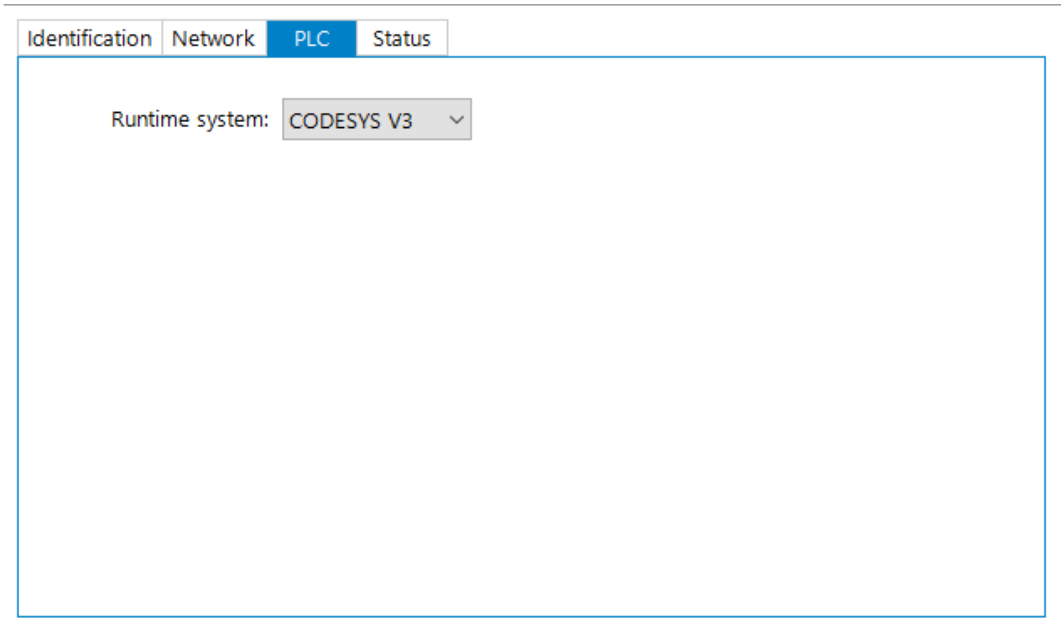

Figure 17: "WAGO Ethernet Settings" – Protocol Tab (Example)

5.2.4 Status Tab

This shows general information about the controller's status.

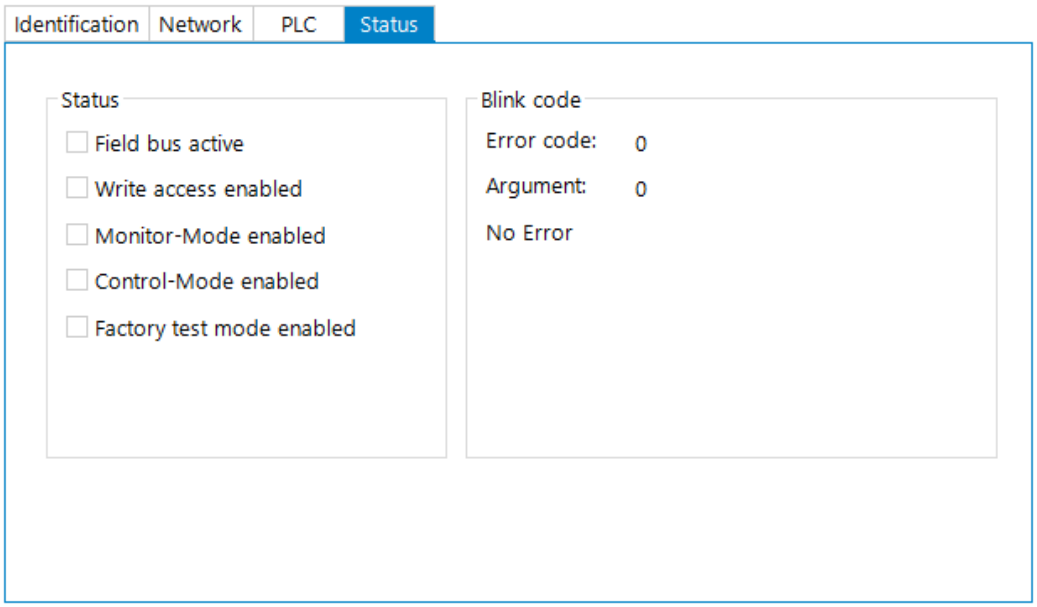

Figure 18: "WAGO Ethernet Settings" – Status Tab (Example)

6 Service

6.1 Firmware Updates

NOTICE

Do not switch the controller off!

The controller can be damaged by interrupting the update/downgrade process.

- Do not switch the controller off during the update/downgrade process and do not disconnect the power supply!

Note

Note the firmware version!

For devices with a factory installation of a firmware >= FW 05, a simple downgrade to a version <= FW 04 is not possible!
Use a special downgrade image.

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.

You can update the firmware in two different ways using:
- WAGOupload
- Memory card and WBM

6.1.1 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.

6.1.2 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.

6.2 Clearing Reset Functions

You can initiate various reset functions using the mode selector switch and the Reset button.

6.2.1 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.

6.2.2 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.

6.2.3 Software Reset (Restart)

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.

6.2.4 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!

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.

Note

Do not interrupt the reset operation!

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

6.3 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.

7 Appendix

7.1 Configuration Dialog

7.1.1 WBM Pages

7.1.1.1 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 117: 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
		Trademarks Information	Trademarks Information	
	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 Domainname	user
		Routing	Routing	user
		STP/RSTP	Spanning Tree Protocol	user
	Clock		Clock Settings	user
	Administration			
		Serial Interface	Configuration of Serial Interface RS232/ RS485	admin
		Service Interface	Configuration of Service Interface	admin
		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

Tab	Navigation		WBM Page Title	User
		DNS	Configuration of DNS Server	admin
	Cloud Connectivity			
		Status	Status Overview	admin
		Connection <n>	Configuration of Connection <n>	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 Parameters	admin
	Commissioning		Commissioning Settings	admin
	Docker		DockerSettings	admin
	Users		WBM User Configuration	admin
	Modem		Configuration of internal 4G Modem	admin
Fieldbus	OPC UA		OPC UA Configuration	admin
	PROFIBUS DP		Configuration of PROFIBUS DP Slave	user
	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
	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

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

7.1.1.2 "Information" Tab

7.1.1.2.1 "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 118: 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 119: 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)
	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	

7.1.1.2.2 “Vendor Information” Page

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

7.1.1.2.3 “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 120: 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.

7.1.1.2.4 "WAGO Software License Agreement" Page

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

7.1.1.2.5 "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.

7.1.1.2.6 "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.

7.1.1.2.7 "Trademarks Information" Page

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

7.1.1.2.8 "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.

7.1.1.3 "Configuration" Tab

7.1.1.3.1 "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 121: 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.

Parameters	Explanation	
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 122: 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.

7.1.1.3.2 "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 123: 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 124: WBM "TCP/IP Configuration" Page – "Dummy Interfaces" Group

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

Parameters	Explanation
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 125: 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 126: 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.

7.1.1.3.3 "Ethernet Configuration" Page

The Ethernet settings are found on the "Ethernet Configuration" page.

“Bridge Configuration” Group

Table 127: 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.

“Dummy Interfaces” Group

Table 128: WBM “Ethernet Configuration” Page – “Dummy Interfaces” Group

Parameters	Explanation
Name	Name of the selected dummy interface
[Delete]	Delete selected entry; The button is only displayed if there are entries.
Add dummy interface	Create new dummy interface
Name	Enter the name of the new dummy interface
[Add]	Add new entry.

“VLAN Interfaces” Group

Table 129: WBM “Ethernet Configuration” Page – “VLAN Interfaces” Group

Parameters	Explanation
Name	Name of the selected VLAN interface
VLAN ID	VLAN ID of the selected VLAN interface
Link	Assigned bridge of the selected VLAN interface
[Delete]	Delete selected entry; The button is only displayed if there are entries.
Add VLAN Interface	Create a New VLAN Interface
Name	Enter the name of the new VLAN interface
VLAN ID	Enter VLAN ID; Permissible values are 3 … 4094.
Link	Select assigned bridge
[Add]	Add new entry.

“Port Mirror Settings” Group

PFC100 G2, PFC200 G2 – 2-Port, PFC300

Table 130: WBM "ETHERNET Configuration" Page – "Port Mirror Settings" Group

Parameters	Explanation	
Enabled	Switch on/off mirroring of data traffic between ports.	
	☐	Data traffic is not mirrored (default).
	☑	Data traffic is mirrored between the selected ports.
Source	Source port of the mirrored data traffic (X1 … X<n>)	
Destination	Target port of the mirrored data traffic (X1 … X<n>)	
[Submit]	Apply change; The change takes effect immediately.	

The “Port Mirror” group is not available for PFC200 G2 – 4-port products.

"Current Control Settings" Group

PFC100 G2, PFC200 G2 – 2-Port

Table 131: WBM "ETHERNET Configuration" Page – "Storm Control Settings" Group

Parameters	Explanation	
Broadcast Protection	Data packet limiting value for broadcast; default value: 1 % of the maximum data rate	
Multicast Protection	Determines whether the data packet limitation applies only to broadcast or to broadcast and multicast together	
	☐	Data packet limitation applies only to broadcast packets
	☑	Data packet limitation applies to both broadcast and multicast packets
[Submit]	Apply change; The change takes effect immediately.	

PFC200 G2 – 4-Port

Table 132: WBM "ETHERNET Configuration" Page – "Storm Control Settings" Group

Parameters	Explanation
Broadcast Protection	Data packet limiting value for broadcast; default value: 1 Mbit
Multicast Protection	Data packet limiting value for multicast; default value: 1 Mbit

PFC300

Table 133: WBM "ETHERNET Configuration" Page – "Storm Control Settings" Group

Parameters	Explanation
Broadcast Protection	Data packet limiting value for broadcast; default value: 20000 packets per second
Multicast Protection	Data packet limiting value for multicast; default value: 20000 packets per second
[Submit]	Apply change; The change takes effect immediately.

"Ethernet Interface Configuration" Group

PFC100 G2, PFC200 G2 – 2-Port

Table 134: 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

Parameters	Explanation	
	☑	Broadcast protection is enabled
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.	

PFC200 G2 – 4-Port, PFC300

Table 135: 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
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.	

7.1.1.3.4 "Configuration of Host and Domain Name" Page

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

"Hostname" Group

Table 136: 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

Parameters	Explanation
[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 137: 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.

7.1.1.3.5 "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 138: WBM "Routing" Page – "IP Forwarding through multiple interfaces" Group

Parameters	Explanation	
Enabled	Allow forwarding of IP data packets between different network interfaces	
	☐	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 139: WBM "Routing" Page – "Custom Routes" Group

Parameters	Explanation	
Enabled	Using the selected route	
	☐	The route is not used.
	☑	The route is used.

Parameters	Explanation	
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 140: 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 141: 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.

7.1.1.3.6 "Spanning Tree Protocol" Page

The settings for STP/RSTP are shown on the "Spanning Tree Protocol" page.

"Status" Group

The "Status" group displays the current values of the enabled STP/RSTP configuration.

Table 142: WBM "Spanning Tree Protocol" Page – "Status" Group

Parameters	Explanation	
Current Status	Current Status	
	☐	STP/RSTP is disabled.
	☑	STP/RSTP is enabled.
Current Bridge	Selected Bridge	
Current Mode	Current Protocol	
	STP	Spanning Tree Protocol is enabled.
	RSTP	Rapid Spanning Tree Protocol is enabled.

Parameters	Explanation	
Current Priority	Current Bridge Priority	
Current Hello Time (sec)	Current "Hello" time in seconds	
Current Forward Delay (sec)	Current "Forward Delay" time in seconds	
Current Max Age (sec)	Current "Max Age Time" in Seconds	
Current Max Hops	Current Max Hops	
Current Path Cost	Current Path Cost	
Port X[n]	A separate area is displayed for each port X[n] of the selected bridge. The port settings are only displayed after STP/RSTP has been successfully enabled.	
Current Bpdu Filter	Current "Bpdu Filter" status	
	☐	Bpdu filter is disabled.
	☑	Bpdu filter is enabled.
Current Bodu Guard	Current "Blue Guard" status	
	☐	Bpdu Guard is disabled.
	☑	Bpdu Guard is enabled.
Current Edge Port	Current Port Status	
	☐	Port is not an edge port.
	☑	Port is an edge port.
Current Root Guard	Current "Root Guard" status	
	☐	Root Guard is disabled.
	☑	Root Guard is enabled.
Current Path Cost	Current path costs	
Current Priority	Current priority	
Current Role	Current role of the port	
	Designated	The port selected in each LAN segment that offers the lowest root path cost. The higher the connection speed, the lower the cost value.
	Disabled	The port is disabled.
Current Status	Current port status	
	Forwarding	The port can send and receive data, learn MAC addresses and forward data to its destination.
	Discarding	The port does not forward data to other switches in the network and does not update MAC address tables.

"Parameter Settings" Group

In the "Parameter Settings" group, you can change the settings for the STP/RSTP configuration.

Table 143: WBM "Spanning Tree Protocol" Page – "Parameter Settings" Group

Parameters	Explanation	
Enabled	Enable/disable Spanning Tree Protocol.	
	☐	Spanning Tree Protocol is disabled.
	☑	Spanning Tree Protocol is enabled.

Parameters	Explanation	
Bridge	Select bridge.	
Mode	Select protocol;	
	STP	Spanning Tree Protocol
	RSTP	Rapid Spanning Tree Protocol
Priority	Set bridge priority; Permissible values: 1 … 15	
Hello time	Set Hello Time; Permissible Values: 1 … 19	
Forward Delay	Set forward delay; Permissible values: 4 … 30	
Max Age	Set max age; Permissible values: 6 … 40	
Max Hops	Set max hops; Permissible values: 6 … 40	
[Submit]	Apply change; The change takes effect immediately.	
Port X[n]	Each port X[n] has its own area. The port settings are only available after STP/RSTP has been successfully enabled.	
Bpdu Filter	Bpdu Enable/disable filter.	
	☐	Bpdu filter is disabled.
	☑	Bpdu filter is enabled.
Blue Guard	Enable/disable the Bpdu Guard.	
	☐	Bpdu Guard is disabled.
	☑	Bpdu Guard is enabled.
Edge Port	Enable/disable port as edge port.	
	☐	Port is not an edge port.
	☑	Port is an edge port.
Root Guard	Enable/disable root guard.	
	☐	Root Guard is disabled.
	☑	Root Guard is enabled.
Pathcost	Set Path Cost; Permissible Values: 0 … 65535	
Priority	Set priority; Permissible values: 0 …15, Default = 8	
[Submit]	Apply change; The change takes effect immediately.	

7.1.1.3.7 "Clock Settings" Page

On this page, date and time settings are possible.

"Timezone and Format" Group

Table 144: WBM "Clock" Page – "Timezone" Group

Parameters	Explanation
Timezone	Select time zone, default setting:

Parameters	Explanation	
	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 145: 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 146: 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.

7.1.1.3.8 Seite „Configuration of Serial Interface"

Settings for the serial interface are possible on this page.

7.1.1.3.8.1 PFC100/PFC200

"Current Serial Interface Configuration" Group

Displays the application to which the serial interface is currently assigned and the current interface mode.

Table 147: WBM "Configuration of Serial Interface" Page – "Current Serial Interface Configuration" Group

Parameters	Explanation
Assigned to	Assignment of communication interface

Parameters	Explanation	
	Unassigned (usage by Applications, Libraries, PLC Runtime)	The communication interface is not assigned to any application. This allows the CODESYS program to access it via function blocks, for example.
	Linux Console	The communication interface is assigned to the Linux console.
Mode	Communication interface mode	
	RS-232	The communication interface is operated in RS-232 mode.
	RS-485	The communication interface is operated in RS-485 mode.

NOTICE

Material damage due to a change of owner or mode!

Switching over can damage connected RS-232/RS-485 devices.

- Remove the devices before switching.

"Assign Mode of Serial Interface" Group

You can specify the operating mode of the communication interface.

Table 148: WBM "Configuration of Serial Interface" Page – "Assign Mode of Serial Interface" Group

Parameters	Explanation
RS-232	The communication interface is operated in RS-232 mode.
RS-485	The communication interface is operated in RS-485 mode.
[Submit]	Apply change; The change only takes effect after the next restart.

"Assign Owner of Serial Interface" Group

You can specify the application that the serial interface is to assigned after the next controller reboot.

Table 149: WBM "Configuration of Serial Interface" Page – "Assign Owner of Serial Interface" Group

Parameters	Explanation
Unassigned (usage by Applications, Libraries, PLC Runtime)	The communication interface is not assigned to any application.
Linux Console	The communication interface is assigned to the Linux console.
[Submit]	Apply change; The change only takes effect after the next restart.

7.1.1.3.8.2 PFC300

"Current Serial Interface Configuration" Group

The current interface mode is displayed in this group.

Table 150: WBM "Configuration of Serial Interface" Page – "Current Serial Interface Configuration" Group

Parameters	Explanation	
Mode	Communication interface mode	
	RS485	The communication interface is operated in RS-485 mode.

"Bus Termination" Group

Here you can activate or deactivate the bus termination for the communication interface.

Table 151: WBM "Configuration of Serial Interface" Page – "Bus Termination" Group

Parameters	Explanation	
Termination enabled	Activate/deactivate bus termination.	
	☐	The bus termination is deactivated.
	☑	The bus termination is activated.
[Submit]	Apply change; The change takes effect immediately.	

"Bias Network" Group

Here you can set the bias network for the communication interface.

Table 152: WBM "Configuration of Serial Interface" Page – "Bias Network" Group

Parameters	Explanation
Off	No bias network is active.
Low	Bias network 1 (640 Ohm) is active.
High	Bias network 2 (1210 Ohm) is active.
[Submit]	Apply change; The change takes effect immediately.

7.1.1.3.9 "Configuration of Service Interface" Page

The settings for the service interface are shown on the "Configuration of the Service Interface" page.

"Service Interface assigned to" Group

The application that the service interface is currently assigned to is displayed.

"Assign Owner of Service Interface" Group

You can specify the application to which the service interface is assigned after the next controller reboot.

Table 153: WBM "Configuration of Service Interface" Page – "Assign Owner of Service Interface" Group

Parameters	Explanation
WAGO Service Communication	The service interface is used for WAGO service communication or runtime system communication.
Linux Console	The service interface is assigned to the Linux console.
Unassigned (usage by Applications, Libraries, PLC Runtime)	The service interface is not assigned to any application. This allows the CODESYS program to access it via function blocks, for example.
[Submit]	Apply change; The change only takes effect after the next restart.

7.1.1.3.10 "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 154: 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:	
	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.

7.1.1.3.11 "Firmware Backup" Page

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

"Firmware Backup" Group

Table 155: 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.	

Parameters	Explanation	
	☐	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.	
[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.

7.1.1.3.12 "Firmware Restore" Page

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

“Firmware Restore” Group

Table 156: 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	

ⓘ 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

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.

ⓘ 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.

7.1.1.3.13 "Active System" Page

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

"Boot Device" Group

Table 157: 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 158: 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!

7.1.1.3.14 "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 159: 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 160: 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	

7.1.1.3.15 “Software Uploads” Page

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

Table 161: 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.

7.1.1.3.16 “Configuration of Network Services” Page

Auf dieser Seite sind Einstellungen zu verschiedenen Diensten möglich.

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 162: 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 163: 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 164: 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 165: 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 166: 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.	

7.1.1.3.17 "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 167: WBM "Configuration of NTP Client" Page – "NTP Client Configuration" Group

Parameters	Explanation	
Service enabled	Enable/disable automatic updating of the time;	
	☐	Updating the time is disabled; default setting
	☑	Updating the time is enabled.
Update Interval (sec)	Enter update interval of the time server.	
Time Server <n>	Enter the IP addresses of the time servers; a maximum of 4 time servers are possible.	
Additionally assigned (DHCP)	NTP server assigned by DHCP (or BootP if supported); If no time server has been assigned, "No additional servers assigned" is displayed.	
[Update Time]	Update time	
[Submit]	Apply change; The change takes effect immediately.	

7.1.1.3.18 "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 168: 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.	

7.1.1.3.19 "SSH Server Settings" Page

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

"SSH Server" Group

Table 169: 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.	

7.1.1.3.20 "DHCP Server Configuration" Page

The "DHCP Configuration" page displays the DHCP service settings.

A separate group is displayed for each configured bridge.

"DHCP Server Configuration Bridge <n>" Group

Table 170: WBM "DHCP Server Configuration" – "DHCP Server Configuration Bridge <n>" Group

Parameters	Explanation	
Service enabled	Enable/disable DHCP server service for the bridge <n>;	
	☐	The DHCP server service for the bridge <n> is not enabled.
	☑	The DHCP server service for the bridge <n> is enabled.
Start IP for Range	Enter the starting value of the available IP address range.	
End IP for Range	Enter the end value of the available IP address range.	
Lease time (min)	Enter the lease time in minutes. Default: 120 minutes	
[Submit]	Apply change; The change takes effect immediately.	
Static Hosts	Static mappings of MAC IDs or host hubs to IP addresses; If no assignment is available, "No static hosts configured" is displayed.	
[Delete]	Delete selected entry; The button is only displayed if there are entries.	
Add Static Host	Add static mappings of MAC addresses or hostnames to IP addresses; max. 15 mappings possible.	
MAC Address or Hostname	Enter MAC address or hostname; e.g., "01:02:03:04:05:06=192.168.1.20" or "hostname=192.168.1.20."	
IP Address	Enter the IP address.	
[Add]	Add new entry.	

7.1.1.3.21 "Configuration of DNS Server" Page

Settings for the DNS service are possible on this page.

"DNS Server" Group

Table 171: WBM "Configuration of DNS Server" Page – "DNS Server" Group

Parameters	Explanation	
Service enabled	Enable/disable DNS server service;	
	☐	The DNS server service is disabled.
	☑	The DNS server service is enabled.
Mode	Set operating mode;	
	Proxy	Requests are buffered to optimize throughput.
	Relay	All requests are routed directly.
[Submit]	Apply change; The change takes effect immediately.	
Static Hosts	Static mapping of hostnames to IP addresses; If no mapping exists, "No static hosts configured" is displayed.	
[Delete]	Delete selected entry; The button is only displayed if there are entries.	
Add Static Host	Add static IP address assignments to hostnames; max. 10 assignments possible.	
IP Address	Enter IP address; e.g., "192.168.1.20:hostname"	
Hostname	Enter hostname.	
[Add]	Add new entry.	

7.1.1.3.22 "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 172: 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

7.1.1.3.23 "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 173: 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

Parameters	Explanation
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
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 174: 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 175: 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 176: 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 177: 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 178: 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		

7.1.1.3.24 "Controls Settings" Page

The settings and information for activating/deactivating the mode selector switch and reset button can be found on the "Configuration" tab, "Controls Settings" page.

Table 179: WBM "Controls Settings" Page – "OMS Controls" Group

Parameters	Explanation
Current Mode	Current status of the functionality of the mode selector switch and reset button

Parameters	Explanation	
	Inactive	The controller ignores any activation of the mode selector switch and the reset button.
	Active	The controller reacts to use of the mode selector switch and the reset button.
Activate	Activates/deactivates the mode selector switch and the reset button	
	☐	Deactivates mode selector switch and reset button
	☑	Activates mode selector switch and reset button
[Submit]	Apply change; The change only takes effect after the next restart.	

Note

If the mode selector switch is deactivated and a CODESYS boot project has been loaded, it is executed automatically when the product restarts!

When the mode selector switch is deactivated, the only way to stop and reset a running application is by using the CODESYS development environment.

7.1.1.3.25 "Configuration of general SNMP parameters" Page

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

"General SNMP Configuration" Group

Table 180: 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.	

7.1.1.3.26 "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 181: WBM "Configuration of SNMP v1/v2c Parameters" Page – "Communities" Group

Parameters	Explanation
Name	Community name for the SNMP manager configuration

Parameters	Explanation
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 182: 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.

7.1.1.3.27 "Configuration of SNMP v3 Parameters" Page

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

"Users" Group

Table 183: 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 184: 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.

7.1.1.3.28 "Commissioning Settings" Page

The "Commissioning Settings" page contains information and settings for the "Commissioning Agent" service.

"Commissioning" Group

Table 185: WBM "Commissioning Settings" Page – "Commissioning" Group

Parameters	Explanation	
Service Enabled	Enable/disable "Commissioning Agent" service;	
	☐	The "Commissioning Agent" service is disabled.
	☑	The "Commissioning Agent" service is enabled.
Commissioning State	Current status of the "Commissioning Agent" service	
	inactive	The service is disabled.
	searching	The service is looking for a server.
	requesting	The service has found a server and is attempting to connect.
	awaiting response	The service is waiting to be accepted by the server.
	no server found	The service did not find a valid server within the given time of five minutes. To restart the scan, the device must be restarted.
	processing	The service starts installing packages received from the server.
	error exit	The service aborted the installation due to an internal error.
	Success	The service has successfully completed the installation.
Connected Server	Domain of the server to which the product is connected; If the product is not connected, "-" is displayed.	
[Submit]	Apply change; The change takes effect immediately.	

7.1.1.3.29 Docker® Settings Page

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

"Docker® Status" Group

Table 186: 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.	

7.1.1.3.30 "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 187: 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.

Parameters	Explanation
[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.

7.1.1.4 “Fieldbus” Tab

7.1.1.4.1 “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 188: 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 189: 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	
	☐	
	☑	

Parameters	Explanation	
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.	
	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.	

7.1.1.4.2 "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 190: 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 191: 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 192: WBM "BACnet Status" Page – "BACnet Data Link" Group

Parameters	Explanation
Connection Info	Display of the connection status

7.1.1.4.3 "BACnet Configuration" Page

You can make special settings for the BACnet fieldbus on this page.

"Restart" Group

Table 193: WBM "BACnet Data Link" Page – "BACnet Restart" Group

Parameters	Explanation
[Restart]	Restart the BACnet service

"BACnet Service" Group

Table 194: 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.
	☑	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 195: 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 196: WBM "BACnet Configuration" Page – "BACnet Log Level" Group

Parameters	Explanation	
Error	Enable/disable error log outputs.	
	☐	Error log entries are not output.

Parameters	Explanation	
	☑	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 197: 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.
	☑	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.	

7.1.1.4.4 "BACnet Data Link" Page

"Restart" Group

Table 198: WBM "BACnet Data Link" Page – "BACnet Restart" Group

Parameters	Explanation
[Restart]	Restart the BACnet service

"BACnet/IP" Group

Table 199: WBM "BACnet Data Link" Page – "BACnet/IP" Group

Parameters	Explanation
Port Number	Input of the port for BACnet/IP communication

Parameters	Explanation
[Submit]	Apply change; The change is only applied after the controller is restarted or after a BACnet restart.

"BACnet/SC" Group

Table 200: 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 201: 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 202: 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 203: 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)

Parameters	Explanation
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 204: WBM "BACnet Data Link" Page – "BACnet/SC Default Certificates" Group

Parameters	Explanation
[Generate]	Generation of a new certificate

7.1.1.4.5 "BACnet Storage Location" Page

You can make settings for saving the BACnet-specific parameters on the "BACnet Storage Location" page.

"BACnet Persistence" Group

Table 205: 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 206: 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 207: 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.	

7.1.1.4.6 “BACnet Info” Page

The settings for displaying BACnet specific information are shown on the “BACnet Info” page.

“Refresh Options” Group

Table 208: 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 209: 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 210: 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 211: 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.

7.1.1.5 "Security" Tab

7.1.1.5.1 "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 212: 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 213: 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

7.1.1.5.2 "General Firewall Configuration" Page

The "General Firewall Configuration" page displays the global firewall settings.

"Global Firewall Parameter" Group

Table 214: 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.

7.1.1.5.3 "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 215: 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 216: Ports for Telecontrol Functionality

Protocol	Port
DNP3	20000
IEC60870-5-104	2404
IEC61850	102

7.1.1.5.4 "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 217: 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 218: 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 219: 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.

7.1.1.5.5 "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 220: 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.

7.1.1.5.6 "Certificates" Page

You find certficate settings on this page.

"Installed Certificates" Group

Table 221: 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 222: 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.

7.1.1.5.7 “Boot Mode Configuration” Page

See the “Boot mode configuration” page for boot option settings.

ⓘ 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 223: 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.	

7.1.1.5.8 “Security Settings” Page

This page displays the network security settings.

“TLS Configuration” Group

Table 224: 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.

7.1.1.5.9 "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 225: 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 226: 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.

7.1.1.5.10 "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 227: 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 228: 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.	

7.1.1.6 "Diagnostic" Tab

7.1.1.6.1 "Log Message Viewer" Page

The settings for displaying the diagnostic messages are shown on the "Log Message Viewer" page.

Table 229: 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.

7.1.1.6.2 "Download" Page

On the "Download" page, you have the option of downloading diagnostic data from the product.

Table 230: 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.

7.1.1.6.3 "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 231: 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 232: 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 233: 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 234: 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

List of Tables

Table 1 WBM “Device Status” Page – “Device Details” Group 14
Table 2 WBM “Device Status” Page – “Network TCP/IP” Group 14
Table 3 WBM “PLC Runtime Information” Page – “Runtime” Group 15
Table 4 WBM “Clock” Page – “Timezone” Group 15
Table 5 WBM “Configuration of NTP Client” Page – “NTP Client Configuration” Group 15
Table 6 CODESYS V3 Priorities 17
Table 7 WBM “PLC Runtime Configuration” Page – “General PLC Runtime Configuration” Group 17
Table 8 WBM “PLC Runtime Configuration” Page – “Webserver Configuration” Group 18
Table 9 WBM “PLC Runtime Services” Page – “CODESYS V3” Group 18
Table 10 WBM “Controls Settings” Page – “OMS Controls” Group 19
Table 11 WBM “Configuration of Serial Interface” Page – “Current Serial Interface Configuration” Group 21
Table 12 WBM “Configuration of Serial Interface” Page – “Assign Owner of Serial Interface” Group 21
Table 13 WBM “Configuration of Serial Interface” Page – “Assign Mode of Serial Interface” Group 21
Table 14 WBM “Configuration of Serial Interface” Page – “Current Serial Interface Configuration” Group 22
Table 15 WBM “Configuration of Serial Interface” Page – “Bus Termination” Group 22
Table 16 WBM “Configuration of Serial Interface” Page – “Bias Network” Group 22
Table 17 WBM “Configuration of Service Interface” Page – “Assign Owner of Service Interface” Group 23
Table 18 WBM “ETHERNET Configuration” Page – “Storm Control Settings” Group 24
Table 19 WBM “ETHERNET Configuration” Page – “Storm Control Settings” Group 25
Table 20 WBM “ETHERNET Configuration” Page – “Storm Control Settings” Group 25
Table 21 WBM “Ethernet Configuration” Page – “Ethernet Interface Configuration” Groups 25
Table 22 WBM “Ethernet Configuration” Page – “Ethernet Interface Configuration” Groups 26
Table 23 WBM “TCP/IP Configuration” Page – “Bridge Interfaces” Group 26
Table 24 WBM “TCP/IP Configuration” Page – “Dummy Interfaces” Group 27
Table 25 WBM “TCP/IP Configuration” Page – “VLAN Interfaces” Group 27
Table 26 WBM “TCP/IP Configuration” Page – “DNS Server” Group 27
Table 27 WBM “Configuration of Host and Domain Name” Page – “Hostname” Group 28
Table 28 WBM “Configuration of Host and Domain Name” Page – “Domain Name” Group 28
Table 29 WBM “Routing” Page – “IP Forwarding through multiple interfaces” Group 29
Table 30 WBM “Routing” Page – “Custom Routes” Group 31
Table 31 WBM “Routing” Page – “Dynamic Routes (assigned by DHCP)” Group 32
Table 32 WBM “Routing” Page – “IP Masquerading” Group 32
Table 33 WBM “Routing” Page – “Port Forwarding” Group 32
Table 34 Services and Users 33

Table 35 Linux® user 34
Table 36 WBM "WBM User Configuration" Page – "Change Passwords" Group 34
Table 37 WBM "Security Settings" Page – "TLS Configuration" Group 35
Table 38 WBM "General Firewall Configuration" Page – "Global Firewall Parameter" Group 36
Table 39 WBM "Interface Configuration" Page – "Firewall Configuration Bridge <n> / VPN / WAN" Group 36
Table 40 Ports for Telecontrol Functionality 37
Table 41 WBM "Configuration of MAC address filter" Page – "Global MAC address filter state" Group 37
Table 42 WBM "Configuration of MAC address filter" Page – "MAC address filter state Bridge <n>" Group 37
Table 43 WBM "Configuration of MAC address filter" Page – "MAC address filter whitelist" Group 38
Table 44 WBM "Configuration of User Filter" Page – "User Filter" Group 38
Table 45 List of Parameters Transmitted via DHCP 40
Table 46 WBM "DHCP Server Configuration" – "DHCP Server Configuration Bridge <n>" Group 40
Table 47 WBM "Configuration of DNS Server" Page – "DNS Server" Group 41
Table 48 WBM "Configuration of general SNMP parameters" Page – "General SNMP Configuration" Group 42
Table 49 WBM "Configuration of SNMP v1/v2c Parameters" Page – "Communities" Group 42
Table 50 WBM "Configuration of SNMP v1/v2cparameters" Page – "Trap Receivers" Group 42
Table 51 WBM "Configuration of SNMP v3 Parameters" Page – "Users" Group 43
Table 52 WBM "Configuration of SNMP v3 Parameters" Page – "Trap Receivers" Group 44
Table 53 WBM "Configuration of Network Services" Page – "FTP" Group 44
Table 54 WBM "Configuration of Network Services" Page – "FTPES (explicit FTPS)" Group 44
Table 55 WBM "Configuration of Network Services" Page – "HTTP" Group 45
Table 56 WBM "Configuration of Network Services" Page – "HTTPS" Group 45
Table 57 WBM "Configuration of Network Services" Page – "I/O-*CHECK*" Group 45
Table 58 WBM "SSH Server Settings" Page – "SSH Server" Group 45
Table 59 WBM "Docker Settings" Page – "Docker Status" Group 46
Table 60 Components of the Cloud Connectivity Software Package 47
Table 61 WBM "Overview" Page – "Connection <n>" Group 47
Table 62 WBM "Configuration of Connection <n>" Page – "Configuration" Group 47
Table 63 Displays the selection and input fields depending on the cloud platform selected 49
Table 64 Option for selecting the data protocol depending on the cloud platform selected 50
Table 65 Displays the selection and input fields depending on the selected data protocol 50
Table 66 Option for selecting the cache mode depending on the selected data protocol 50
Table 67 Display of input fields depending on the selected authentication 51
Table 68 WBM "OPC UA Configuration" Page – "OPC UA Server Configuration" Group 51
Table 69 WBM "OPC UA Configuration" Page – "OPC UA Server Security Settings" Group 51
Table 70 WBM "BACnet Status" Page – "BACnet Information" Group 52

Table 71 WBM "BACnet Status" Page – "BACnet License" Group ... 52
Table 72 WBM "BACnet Status" Page – "BACnet Data Link" Group ... 53
Table 73 WBM "BACnet Configuration" Page – "PLC Runtime" Group ... 53
Table 74 WBM "BACnet Configuration" Page – "BACnet Service" Group ... 53
Table 75 WBM "BACnet Configuration" Page – "BACnet Data" Group ... 53
Table 76 WBM "BACnet Configuration" Page – "BACnet Log Level" Group ... 53
Table 77 WBM "BACnet Configuration" Page – "BACnet Network Capture" Group ... 54
Table 78 WBM "BACnet Data Link" Page – "BACnet Restart" Group ... 54
Table 79 WBM "BACnet Data Link" Page – "BACnet/IP" Group ... 54
Table 80 WBM "BACnet Data Link" Page – "BACnet/SC" Group ... 54
Table 81 WBM "BACnet Data Link" Page – "BACnet/SC Certificate Authority (CA)" Group ... 55
Table 82 WBM "BACnet Data Link" Page – "BACnet/SC Certificate" Group ... 55
Table 83 WBM "BACnet Configuration" Page – "BACnet/SC Certificate Signing Request (CSR)" Group ... 55
Table 84 WBM "BACnet Data Link" Page – "BACnet/SC Default Certificates" Group ... 55
Table 85 WBM "BACnet Storage Location" Page – "BACnet Persistence" Group ... 56
Table 86 WBM "BACnet Storage Location" Page – "BACnet Trendlog" Group ... 56
Table 87 WBM "BACnet Storage Location" Page – "BACnet Eventlog" Group ... 56
Table 88 Overview of Addresses in the Object Directory ... 57
Table 89 Indexing of the "IEC 61131-3" variable data in the object directory ... 62
Table 90 Fieldbus Access to the PFC Output Data ... 63
Table 91 Examples of CODESYS Access to PFC Variables ... 63
Table 92 Maximum indices and sub-indices for "IEC 61131-3" variables ... 64
Table 93 Example of "IEC 61131-3" Output Variables ... 64
Table 94 WBM "Firmware Backup" Page – "Firmware Backup" Group ... 66
Table 95 WBM "Firmware Restore" Page – "Firmware Restore" Group ... 68
Table 96 Loading a Boot Project ... 70
Table 97 Overview of "I/O" LED Error Codes ... 71
Table 98 Error Code 1 – Hardware and Configuration Error: Explanation of Blink Codes and Procedures for Troubleshooting ... 72
Table 99 Error Code 2 – Configuration Error: Explanation of Blink Codes and Procedures for Troubleshooting ... 73
Table 100 Error Code 3 – Local Bus Protocol Error: Explanation of Blink Codes and Procedures for Troubleshooting ... 73
Table 101 Error Code 4 – Local Bus Physical Error: Explanation of Blink Codes and Procedures for Troubleshooting ... 73
Table 102 Error Code 5 – Local Bus Initialization Error: Explanation of Blink Codes and Procedures for Troubleshooting ... 74
Table 103 Error Code 7 – Unsupported I/O Module: Explanation of Blink Codes and Procedures for Troubleshooting ... 74

Table 104 Error Code 9 – Exception Error: Explanation of Blink Codes and Procedures for Troubleshooting ... 74
Table 105 Overview of "MS" LED Error Codes ... 74
Table 106 Error Code 1 – Configuration Error: Explanation of Blink Codes and Procedures for Troubleshooting ... 74
Table 107 WBM "Log Message Viewer" Page – "Refresh Options" Group ... 75
Table 108 WBM "Download" Page – "Diagnostic Information" Group ... 75
Table 109 WBM "Network Capture" Page – "State" Group ... 75
Table 110 WBM "Network Capture" Page – "Configuration" Group ... 75
Table 111 WBM "Network Capture" Page – "Filter Configuration" Group ... 76
Table 112 WBM "Network Capture" Page – "Log Download" Group ... 76
Table 113 Default IP Addresses for ETHERNET Interfaces ... 78
Table 114 Network mask: 255.255.255.0 ... 78
Table 115 Address Selection Switch ... 81
Table 116 Access Rights for WBM Pages ... 87
Table 117 Access Rights for WBM Pages ... 98
Table 118 WBM "Device Status" Page – "Device Details" Group ... 100
Table 119 WBM "Device Status" Page – "Network TCP/IP" Group ... 100
Table 120 WBM "PLC Runtime Information" Page – "Runtime" Group ... 101
Table 121 WBM "PLC Runtime Configuration" Page – "General PLC Runtime Configuration" Group ... 101
Table 122 WBM "PLC Runtime Configuration" Page – "Webserver Configuration" Group ... 102
Table 123 WBM "TCP/IP Configuration" Page – "Bridge Interfaces" Group ... 103
Table 124 WBM "TCP/IP Configuration" Page – "Dummy Interfaces" Group ... 103
Table 125 WBM "TCP/IP Configuration" Page – "VLAN Interfaces" Group ... 104
Table 126 WBM "TCP/IP Configuration" Page – "DNS Server" Group ... 104
Table 127 WBM "Ethernet Configuration" Page – "Bridge Configuration" Group ... 105
Table 128 WBM "Ethernet Configuration" Page – "Dummy Interfaces" Group ... 105
Table 129 WBM "Ethernet Configuration" Page – "VLAN Interfaces" Group ... 105
Table 130 WBM "ETHERNET Configuration" Page – "Port Mirror Settings" Group ... 105
Table 131 WBM "ETHERNET Configuration" Page – "Storm Control Settings" Group ... 106
Table 132 WBM "ETHERNET Configuration" Page – "Storm Control Settings" Group ... 106
Table 133 WBM "ETHERNET Configuration" Page – "Storm Control Settings" Group ... 106
Table 134 WBM "Ethernet Configuration" Page – "Ethernet Interface Configuration" Groups ... 106
Table 135 WBM "Ethernet Configuration" Page – "Ethernet Interface Configuration" Groups ... 107
Table 136 WBM "Configuration of Host and Domain Name" Page – "Hostname" Group ... 107
Table 137 WBM "Configuration of Host and Domain Name" Page – "Domain Name" Group ... 108
Table 138 WBM "Routing" Page – "IP Forwarding through multiple interfaces" Group ... 108
Table 139 WBM "Routing" Page – "Custom Routes" Group ... 108

Table 140 WBM "Routing" Page – "IP Masquerading" Group ... 109
Table 141 WBM "Routing" Page – "Port Forwarding" Group ... 110
Table 142 WBM "Spanning Tree Protocol" Page – "Status" Group ... 110
Table 143 WBM "Spanning Tree Protocol" Page – "Parameter Settings" Group ... 111
Table 144 WBM "Clock" Page – "Timezone" Group ... 112
Table 145 WBM "Clock" Page – "UTC Time and Date" Group ... 113
Table 146 WBM "Clock" Page – "Local Time and Date" Group ... 113
Table 147 WBM "Configuration of Serial Interface" Page – "Current Serial Interface Configuration" Group ... 113
Table 148 WBM "Configuration of Serial Interface" Page – "Assign Mode of Serial Interface" Group ... 114
Table 149 WBM "Configuration of Serial Interface" Page – "Assign Owner of Serial Interface" Group ... 114
Table 150 WBM "Configuration of Serial Interface" Page – "Current Serial Interface Configuration" Group ... 114
Table 151 WBM "Configuration of Serial Interface" Page – "Bus Termination" Group ... 115
Table 152 WBM "Configuration of Serial Interface" Page – "Bias Network" Group ... 115
Table 153 WBM "Configuration of Service Interface" Page – "Assign Owner of Service Interface" Group ... 115
Table 154 WBM "Create bootable Image" – "Create bootable image from boot device" Group ... 116
Table 155 WBM "Firmware Backup" Page – "Firmware Backup" Group ... 116
Table 156 WBM "Firmware Restore" Page – "Firmware Restore" Group ... 118
Table 157 WBM "Active System" Page – "Boot Device" Group ... 119
Table 158 WBM "Active System" Page – "System n (Internal Flash)" Group ... 119
Table 159 WBM "Mass Storage" Page – "Devices" Group ... 120
Table 160 WBM "Mass Storage" Page – "Create new Filesystem on Memory Card" Group ... 120
Table 161 WBM "Software Uploads" Page – "Upload New Software" Group ... 120
Table 162 WBM "Configuration of Network Services" Page – "FTP" Group ... 121
Table 163 WBM "Configuration of Network Services" Page – "FTPES (explicit FTPS)" Group ... 121
Table 164 WBM "Configuration of Network Services" Page – "HTTP" Group ... 121
Table 165 WBM "Configuration of Network Services" Page – "HTTPS" Group ... 122
Table 166 WBM "Configuration of Network Services" Page – "I/O-*CHECK*" Group ... 122
Table 167 WBM "Configuration of NTP Client" Page – "NTP Client Configuration" Group ... 122
Table 168 WBM "PLC Runtime Services" Page – "CODESYS V3" Group ... 122
Table 169 WBM "SSH Server Settings" Page – "SSH Server" Group ... 123
Table 170 WBM "DHCP Server Configuration" – "DHCP Server Configuration Bridge <n>" Group ... 124
Table 171 WBM "Configuration of DNS Server" Page – "DNS Server" Group ... 124
Table 172 WBM "Overview" Page – "Connection <n>" Group ... 125
Table 173 WBM "Configuration of Connection <n>" Page – "Configuration" Group ... 125
Table 174 Displays the selection and input fields depending on the cloud platform selected ... 127
Table 175 Option for selecting the data protocol depending on the cloud platform selected ... 128

Table 176 Displays the selection and input fields depending on the selected data protocol ... 128
Table 177 Option for selecting the cache mode depending on the selected data protocol ... 128
Table 178 Display of input fields depending on the selected authentication ... 128
Table 179 WBM “Controls Settings” Page – “OMS Controls” Group ... 128
Table 180 WBM “Configuration of general SNMP parameters” Page – “General SNMP Configuration” Group ... 129
Table 181 WBM “Configuration of SNMP v1/v2c Parameters” Page – “Communities” Group ... 129
Table 182 WBM “Configuration of SNMP v1/v2cparameters” Page – “Trap Receivers” Group ... 130
Table 183 WBM “Configuration of SNMP v3 Parameters” Page – “Users” Group ... 130
Table 184 WBM “Configuration of SNMP v3 Parameters” Page – “Trap Receivers” Group ... 131
Table 185 WBM “Commissioning Settings” Page – “Commissioning” Group ... 131
Table 186 WBM “Docker Settings” Page – “Docker Status” Group ... 132
Table 187 WBM “WBM User Configuration” Page – “Change Passwords” Group ... 132
Table 188 WBM “OPC UA Configuration” Page – “OPC UA Server Configuration” Group ... 133
Table 189 WBM “OPC UA Configuration” Page – “OPC UA Server Security Settings” Group ... 133
Table 190 WBM “BACnet Status” Page – “BACnet Information” Group ... 134
Table 191 WBM “BACnet Status” Page – “BACnet License” Group ... 134
Table 192 WBM “BACnet Status” Page – “BACnet Data Link” Group ... 134
Table 193 WBM “BACnet Data Link” Page – “BACnet Restart” Group ... 135
Table 194 WBM “BACnet Configuration” Page – “BACnet Service” Group ... 135
Table 195 WBM “BACnet Configuration” Page – “BACnet Data” Group ... 135
Table 196 WBM “BACnet Configuration” Page – “BACnet Log Level” Group ... 135
Table 197 WBM “BACnet Configuration” Page – “BACnet Network Capture” Group ... 136
Table 198 WBM “BACnet Data Link” Page – “BACnet Restart” Group ... 136
Table 199 WBM “BACnet Data Link” Page – “BACnet/IP” Group ... 136
Table 200 WBM “BACnet Data Link” Page – “BACnet/SC” Group ... 137
Table 201 WBM “BACnet Data Link” Page – “BACnet/SC Certificate Authority (CA)” Group ... 137
Table 202 WBM “BACnet Data Link” Page – “BACnet/SC Certificate” Group ... 137
Table 203 WBM “BACnet Configuration” Page – “BACnet/SC Certificate Signing Request (CSR)” Group ... 137
Table 204 WBM “BACnet Data Link” Page – “BACnet/SC Default Certificates” Group ... 138
Table 205 WBM “BACnet Storage Location” Page – “BACnet Persistence” Group ... 138
Table 206 WBM “BACnet Storage Location” Page – “BACnet Trendlog” Group ... 138
Table 207 WBM “BACnet Storage Location” Page – “BACnet Eventlog” Group ... 138
Table 208 WBM “BACnet Info” Page – “Refresh Options” Group ... 139
Table 209 WBM “BACnet Info” Page – “BACnet/IP Statistics” Group ... 139
Table 210 WBM “BACnet Info” Page – “BACnet/SC Statistics” Group ... 139
Table 211 WBM “BACnet Info” Page – “BACnet/SC Connections” Group ... 139

Table 212 WBM “OpenVPN / IPsec” Page – “OpenVPN” Group 140
Table 213 WBM “OpenVPN / IPsec” Page – “IPsec” Group 140
Table 214 WBM “General Firewall Configuration” Page – “Global Firewall Parameter” Group 141
Table 215 WBM “Interface Configuration” Page – “Firewall Configuration Bridge <n> / VPN / WAN” Group 141
Table 216 Ports for Telecontrol Functionality 142
Table 217 WBM “Configuration of MAC address filter” Page – “Global MAC address filter state” Group 143
Table 218 WBM “Configuration of MAC address filter” Page – “MAC address filter state Bridge <n>” Group 143
Table 219 WBM “Configuration of MAC address filter” Page – “MAC address filter whitelist” Group 143
Table 220 WBM “Configuration of User Filter” Page – “User Filter” Group 144
Table 221 WBM “Certificates” Page – “Installed Certificates” Group 144
Table 222 WBM “Certificates” Page – “Installed Private Keys” Group 145
Table 223 WBM “Boot Mode Configuration” Page – “Force Internal Boot” Group 145
Table 224 WBM “Security Settings” Page – “TLS Configuration” Group 145
Table 225 WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Run AIDE check at startup” Group 146
Table 226 WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Control AIDE and show log” Group 146
Table 227 WBM “WAGO Device Access” Page – “Unauthenticated Requests” Group 147
Table 228 WBM “WAGO Device Access” Page – “CORS Configuration” Group 147
Table 229 WBM “Log Message Viewer” Page – “Refresh Options” Group 148
Table 230 WBM “Download” Page – “Diagnostic Information” Group 148
Table 231 WBM “Network Capture” Page – “State” Group 148
Table 232 WBM “Network Capture” Page – “Configuration” Group 149
Table 233 WBM “Network Capture” Page – “Filter Configuration” Group 149
Table 234 WBM “Network Capture” Page – “Log Download” Group 149

List of Figures

Figure 1 Communication interface, bus termination and bias network 22
Figure 2 WBM Browser Window (Example) 23
Figure 3 WBM Header with Tabs that Cannot be Displayed (Example) 24
Figure 4 WBM Status Bar (Example) 24
Figure 5 Connecting the Controllers to a Cloud Service (Example) 46
Figure 6 WAGO Ethernet Settings – Start Screen (Example Figure) 80
Figure 7 WAGO Ethernet Settings – Network Tab (Example Figure) 80
Figure 8 Example of a Functional Test 83
Figure 9 Log-in Window 85
Figure 10 WBM Browser Window (Example) 86
Figure 11 WBM Header with Tabs that Cannot be Displayed (Example) 86
Figure 12 WBM Status Bar (Example) 86
Figure 13 “WAGO Ethernet Settings” – Start Screen (Example) 89
Figure 14 “WAGO ETHERNET Settings” – Communication Link (Example) 90
Figure 15 “WAGO Ethernet Settings” – Identification Tab (Example) 91
Figure 16 “WAGO Ethernet Settings” – Network Tab (Example) 91
Figure 17 “WAGO Ethernet Settings” – Protocol Tab (Example) 92
Figure 18 “WAGO Ethernet Settings” – Status Tab (Example) 93

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

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