WAGO TECHDOCS

Manual

WAGO Edge Controller

752-8303/8000-0002

Version 1.5.0, valid from FW Version 04.05.08(27)

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

WAGO GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Phone: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 844 169

E-Mail: info@wago.com

Web: www.wago.com

Technical Support

Phone: +49 (0) 571/8 87 – 4 45 55
Fax: +49 (0) 571/8 87 – 84 45 55

E-Mail: support@wago.com

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

E-Mail: documentation@wago.com

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

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1 Regulations 8
1.1 Validity of this Documentation 8
1.2 Document portfolio 8
1.3 Copyright 8
1.4 Property rights 9
1.5 Symbols 11
1.6 Number Notation 13
1.7 Font Conventions 13
1.8 Legal Bases 14
1.8.1 Subject to Changes 14
1.8.2 Personnel Qualification 14
1.8.3 Intended Use 14
1.8.3.1 Improper Use 14
1.8.3.2 Warranty and Liability 15
1.8.3.3 Obligations of Installers/Operators 15

2 Safety Information 16
2.1 Safety Advice (Precautions) 16
2.2 Special Use Conditions 18

3 Overview 19

4 Properties 20
4.1 View 20
4.2 Labeling 21
4.3 Connectors 23
4.3.1 Connectors on the front 23
4.3.2 Connectors on top 23
4.3.3 “X1” and “X2” ETHERNET Interfaces 24
4.3.4 “X3” – RS-232/485 Serial Interface 24
4.3.4.1 Operating as an RS-232 Interface 25
4.3.4.2 Operating as an RS-485 Interface 25
4.3.5 “X4” – CAN Interface 26
4.3.6 “X5” Supply Voltage 27
4.3.7 “X6” and “X7” USB-2.0 Interfaces 27
4.3.8 “X8” – Line-out Audio Output (Headphones) 27
4.3.9 “X9” – HDMI Interface Type A 28
4.3.10 ”X10” – USB-C Interface 28
4.3.11 “X11” – Four Digital Inputs and Outputs DIO 28
4.3.12 “microSD” Memory Card Slot 29
4.4 Real-Time Clock 31
4.5 Display Elements 32
4.5.1 Status LED 32
4.6 Operating Elements 33
4.6.1 Mode Selector Switch 33
4.6.2 “CFG/RST” Button 33
4.7 Schematic Diagram 34
4.8 Technical Data 35

4.8.1 Device 35
4.8.2 Climatic Environmental Conditions 35
4.8.3 Power Supply 35
4.8.4 Hardware 36
4.8.5 Communication 36
4.8.6 Interfaces 36
4.8.7 Connectors 37
4.9 Approvals 38
4.10 Standards and Guidelines 38

5 Functions 39

5.1 Web Browser 39
5.2 Connection Monitoring 40
5.3 WBM for Configuration/Parameterization 40
5.4 Network 40
5.4.1 Interface Configuration 40
5.4.1.1 Operation with Separate Network Interfaces 40
5.4.2 Network Security 40
5.4.2.1 Users and Passwords 40
5.4.2.2 Services and Users 42
5.4.2.3 WBM User Group 42
5.4.2.4 Linux® User Group 42
5.4.2.5 SNMP User Group 43
5.4.2.6 Web Protocols for WBM Access 44
5.4.2.7 TLS Encryption 44
5.4.3 Network Configuration 44
5.4.3.1 Host Name/Domain Name 44
5.4.3.2 Default Gateways 45
5.5 Memory Card Functions 45
5.5.1 Backup 45
5.5.2 Restore 46
5.5.3 Create Image 46
5.6 Downloading Software 46
5.7 Booting 47
5.8 Licensed Software Components 49

6 Mounting 50

6.1 Assembly Guidelines/Standards 50
6.2 Mounting position 50
6.3 Mount to the Rail 51

7 Connecting 52

7.1 Earthing 52
7.2 Connecting Devices 52
7.3 Connecting the Power Supply 53

8 Commissioning 54

8.1 Switching ON 54
8.2 Login 54
8.3 Determining the IP Address of the Host PC 54
8.4 Setting an IP Address 54

8.4.1 IP Connection via USB 55
8.4.2 Changing an IP Address using “WAGO Ethernet Settings” 55
8.4.3 Temporarily Setting a Fixed IP Address 57
8.4.4 Setting the IP Address via the WBM 58
8.4.5 Assigning an IP Address using DHCP 58
8.5 Initiating Reset Functions 59
8.5.1 Warm Start Reset 59
8.5.2 Cold Start Reset 59
8.5.3 Software Reset 60
8.5.4 Factory Reset 60
8.6 Configuring in the Web-Based Management (WBM) 62
8.6.1 WBM User Administration 64
8.6.2 General Information about the Page 68
8.6.3 Reboot Function 70

9 Run-time System CODESYS V3 71

9.1 General Notes 71
9.2 CODESYS V3 Priorities 72
9.3 Memory Spaces under CODESYS V3 73
9.3.1 Program and Data Memory 73
9.3.2 Function Block Limitation 73
9.3.3 Remanent Memory 73
9.3.4 File Access from the IEC Application 73
9.3.5 Changing Network Settings from the IEC Application 74
9.3.6 EtherCAT 74

10 Diagnostics 75

11 Service 76

11.1 Changing the Configuration with the WBM 76
11.2 Firmware Changes 77
11.2.1 Use WAGOupload to Update/Downgrade the Firmware 78
11.2.2 Perform Firmware Update/Downgrade 79

12 Removal 80

12.1 Removal from the Rail 80

13 Disposal 81

13.1 Electrical and electronic equipment 81
13.2 Packaging 81

14 Accessories 83

15 Appendix 84

15.1 Configuration Dialogs 84
15.1.1 Web-Based-Management (WBM) 84
15.1.1.1 “Information” Tab 84
15.1.1.1.1 “Device Status” Page 84
15.1.1.1.2 “Vendor Information” Page 86
15.1.1.1.3 “PLC Runtime Information” Page 87
15.1.1.1.4 “WAGO Software License Agreement” Page 88
15.1.1.1.5 “Open Source Licenses” Page 89
15.1.1.1.6 “WBM Third Party License Information” Page 90

15.1.1.1.7 “Trademarks Information” Page 91
15.1.1.1.8 “WBM Version” Page 92
15.1.1.2 “Configuration” Tab 93
15.1.1.2.1 “PLC Runtime Configuration” Page 93
15.1.1.2.2 “TCP/IP Configuration” Page 95
15.1.1.2.3 “Ethernet Configuration” Page 97
15.1.1.2.4 Configuration of Host and Domain Name” Page 101
15.1.1.2.5 “Routing” Page 103
15.1.1.2.1 “Spanning Tree Protocol” Page 108
15.1.1.2.2 “Clock Settings” Page 111
15.1.1.2.3 “Configuration of Serial Interface” Page 113
15.1.1.2.4 “Configuration of Service Interface” Page 115
15.1.1.2.5 “Create Bootable Image” Page 116
15.1.1.2.6 “Firmware Backup” Page 117
15.1.1.2.7 “Firmware Restore” Page 119
15.1.1.2.8 “Active System” Page 121
15.1.1.2.9 “Mass Storage” Page 122
15.1.1.2.10 “Software Uploads” Page 123
15.1.1.2.11 “Configuration of Network Services” Page 124
15.1.1.2.12 “Configuration of NTP Client” Page 126
15.1.1.2.13 “PLC Runtime Services” Page 127
15.1.1.2.14 “SSH Server Settings” Page 128
15.1.1.2.15 “DHCP Server Configuration” Page 129
15.1.1.2.16 “Configuration of DNS Server” Page 130
15.1.1.2.17 “Status overview” Page 131
15.1.1.2.18 “Configuration of Connection <n>” Page 132
15.1.1.2.19 “Configuration of General SNMP Parameters” Page 139
15.1.1.2.20 “Configuration of SNMP v1/v2c Parameters” Page 140
15.1.1.2.21 “Configuration of SNMP v3 Parameters” Page 142
15.1.1.2.22 “Favorites” Page 146
15.1.1.2.23 “Autostart” Page 148
15.1.1.2.24 “Monitoring” Page 149
15.1.1.2.25 “Browser Security” Page 150
15.1.1.2.1 “Commissioning Settings” Page 151
15.1.1.2.2 Page “Docker Settings” 152
15.1.1.2.3 “Fonts” Page 153
15.1.1.2.4 “Display Orientation” Page 154
15.1.1.2.5 “Screensaver” Page 155
15.1.1.2.6 “WBM User Configuration” Page 156
15.1.1.3 “Fieldbus” Tab 157
15.1.1.3.1 “OPC UA Configuration” Page 157
15.1.1.3.1 “BACnet Status” Page 159
15.1.1.3.2 “BACnet Configuration” Page 160
15.1.1.3.3 “BACnet Data Link” Page 162
15.1.1.3.4 “BACnet Storage Location” Page 164
15.1.1.4 “Security” Tab 166
15.1.1.4.1 “OpenVPN / IPsec Configuration” Page 166
15.1.1.4.2 “General Firewall Configuration” Page 168
15.1.1.4.3 “Interface Configuration” Page 169
15.1.1.4.4 “Configuration of MAC Address Filter” Page 171

15.1.1.4.5 “Configuration of User Filter” Page ... 173
15.1.1.4.6 “Certificates” Page ... 175
15.1.1.4.7 “Boot mode configuration” Page ... 176
15.1.1.4.8 “Security Settings” Page ... 177
15.1.1.4.9 “Advanced Intrusion Detection Environment (AIDE)” Page ... 178
15.1.1.4.10 “WAGO Device Access” Page ... 180
15.1.1.5 “Diagnostic” Tab ... 181
15.1.1.5.1 “Log Message Viewer” Page ... 181
15.1.1.5.2 “Download” Page ... 182
15.1.1.5.3 “Network Capture” Page ... 183

List of Figures ... 186

List of Tables ... 187

1 Regulations

The WAGO product shall only be installed and operated according to the instructions in this documentation.

Note

Always retain this documentation!
This documentation is part of the product. Therefore, retain the documentation during the entire service life of the product. Pass on the documentation to any subsequent user. In addition, ensure that any supplement to this documentation is included, if necessary.

1.1 Validity of this Documentation

This documentation applies to the product 752-8303/8000-0002.

1.2 Document portfolio

Besides this manual, you should consult the following WAGO documents:

- WAGO I/O SYSTEM 750, manual for the PFC Controller used
- WAGO I/O SYSTEM 750, “Cybersecurity for PFC100/PFC200 Controllers” manual
- Migration guide; Migration from ***e!****COCKPIT* to CODESYS V3.5
- “Industrial ETHERNET” technology manual

These documents are available for download on the WAGO Website www.wago.com.

You can find more information on CODESYS V3.5 in the CODESYS online help at help.codesys.com (up to service pack 17) and in the new online help at helpme-codesys.com (current service pack).

1.3 Copyright

This Manual, including all figures and illustrations, is copyright-protected. Any further use of this Manual by third parties that violate pertinent copyright provisions is prohibited. Reproduction, translation, electronic and phototechnical filing/archiving (e.g., photocopying) as well as any amendments require the written consent of WAGO GmbH & Co. KG, Minden, Germany. Non-observance will involve the right to assert damage claims.

1.4 Property rights

Third-party trademarks are used in this documentation. This section contains the trademarks used. The “®” and “TM” symbols are omitted hereinafter.

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

- PROFIBUS® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).
- PROFINET® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).
- QR Code is a registered trademark of DENSO WAVE INCORPORATED.
- Subversion® is a trademark of the Apache Software Foundation.
- Windows® is a registered trademark of Microsoft Corporation.

1.5 Symbols

DANGER

Personal Injury!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.

DANGER

Personal Injury Caused by Electric Current!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.

WARNING

Personal Injury!
Indicates a moderate-risk, potentially hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

Personal Injury!
Indicates a low-risk, potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

NOTICE

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

NOTICE

Damage to Property Caused by Electrostatic Discharge (ESD)!
Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.

Note

Important Note!
Indicates a potential malfunction which, if not avoided, however, will not result in damage to property.

Information

Additional Information:
Refers to additional information which is not an integral part of this documentation (e.g., the Internet).

1.6 Number Notation

Table 1: Number Notation

Number Code	Example	Note
Decimal	100	Normal notation
Hexadecimal	0x64	C notation
Binary	'100' '0110.0100'	In quotation marks, nibble separated with dots (.)

1.7 Font Conventions

Table 2: Font Conventions

Font Type	Indicates
italic	Names of paths and data files are marked in italic-type. e.g.: *C:\Program Files\WAGO Software*
Menu	Menu items are marked in bold letters. e.g.: **Save**
>	A greater-than sign between two names means the selection of a menu item from a menu. e.g.: **File** > **New**
Input	Designation of input or optional fields are marked in bold letters, e.g.: **Start of measurement range**
“Value”	Input or selective values are marked in inverted commas. e.g.: Enter the value “4 mA” under **Start of measurement range**.
[Button]	Pushbuttons in dialog boxes are marked with bold letters in square brackets. e.g.: **[Input]**
[Key]	Keys are marked with bold letters in square brackets. e.g.: **[F5]**

1.8 Legal Bases

1.8.1 Subject to Changes

WAGO GmbH & Co. KG reserves the right to provide for any alterations or modifications. WAGO GmbH & Co. KG owns all rights arising from the granting of patents or from the legal protection of utility patents. Third-party products are always mentioned without any reference to patent rights. Thus, the existence of such rights cannot be excluded.

1.8.2 Personnel Qualification

All sequences implemented on Series 752 devices may only be carried out by electrical specialists with sufficient knowledge in automation technology. These specialists must be familiar with the current standards and guidelines for the devices and the automated environments.

All changes to the controller shall always be performed by qualified personnel with sufficient skills in PLC programming.

1.8.3 Intended Use

The Edge controller is suitable for use in the area of control and automation. Its use extends beyond residential and commercial areas, as well as industrial areas. Technical data must be observed for all types of applications.

Use of the HDMI interface is not permitted in residential, business, commercial areas, as well as small businesses.
Use of the HDMI interface is permitted in the industrial sector.

The product is an open system and is designed for installation in an additional enclosure.
This product fulfills the requirements of protection type IP20 and is designed for use in dry indoor spaces.

1.8.3.1 Improper Use

Improper use of the product is not permitted. Specifically, improper use occurs in the following cases:

- Non-observance of the intended use.
- Use without protective measures in an environment in which moisture, salt water, salt spray mist, dust, corrosive fumes, gases, direct sunlight or ionizing radiation can occur.
- Use of the product in areas with special risk that require flawless continuous operation and in which failure or operation of the product can result in an imminent risk to life, limb or health or cause serious damage to

property or the environment (such as the operation of nuclear power plants, weapon systems , aircraft and motor vehicles).

1.8.3.2 Warranty and Liability

The terms set forth in the General Business & Contractual Conditions apply to deliveries and services of WAGO GmbH & Co. KG, and the WAGO Software License Contract applies to software products and products with integrated software. Both are available at www.wago.com. In particular, the warranty is void if:

- The product is improperly used.
- The deficiency (hardware and software configurations) is due to special instructions.
- Modifications to the hardware or software have been made by the user or third parties that are not described in this documentation and that has contributed to the fault.

Individual agreements always have priority.

1.8.3.3 Obligations of Installers/Operators

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

2 Safety Information

2.1 Safety Advice (Precautions)

This section includes an overall summary of the most important safety requirements and notes that are mentioned in each individual section. To protect your health and prevent damage to devices as well, it is imperative to read and carefully follow the safety guidelines.

For installing and operating purposes of the relevant device to your system the following safety precautions shall be observed:

DANGER

Do not work when devices are energized!
High voltage can cause electric shock or burns.
Always disconnect the power supply from those parts of the system on which you wish to mount or remove the device!

DANGER

Use SELV power source only!
The device must only be powered from a SELV (Safety Extra Low Voltage) power source complying with the limited power source (LPS) requirements per DIN EN 60950-1.

DANGER

Ensure a standard connection!
To minimize any hazardous situations resulting in personal injury or to avoid failures in your system, the data and power supply lines shall be installed according to standards, with careful attention given to ensuring the correct terminal assignment. Always adhere to the EMC directives applicable to your application.

NOTICE

Consider the IP protection type!
The device is an open unit whose is IP20 protected. If the operating environment does not fulfill these requirements you have to install the device into cabinet resp. housing.

NOTICE

Replace defective or damaged devices!
Replace defective or damaged device/module (e.g., in the event of deformed contacts).

NOTICE

Protect the components against materials having seeping and insulating properties!
The components are not resistant to materials having seeping and insulating properties such as: aerosols, silicones and triglycerides (found in some hand creams). If you cannot exclude that such materials will appear in the component environment, then install the components in an enclosure being resistant to the above-mentioned materials. Clean tools and materials are imperative for handling devices/modules.

NOTICE

Clean only with permitted materials!
Clean housing and soiled contacts with propanol.

NOTICE

Do not use any contact spray!
Do not use any contact spray. The spray may impair contact area functionality in connection with contamination.

NOTICE

Do not use in telecommunication circuits!
Only use devices equipped with ETHERNET or RJ-45 connectors in LANs. Never connect these devices with telecommunication networks.

NOTICE

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

2.2 Special Use Conditions

If not otherwise specified, ETHERNET devices are intended for use on local networks. Please note the following when using ETHERNET devices in your system:

- Do not connect control components and control networks to an open network such as the Internet or an office network. WAGO recommends putting control components and control networks behind a firewall.
- In the control components (e.g., for CODESYS) close all ports and services not required by your application to minimize the risk of cyber attacks and to enhance cyber security.
  Only open ports and services during commissioning and/or configuration.
- Limit physical and electronic access to all automation components to authorized personnel only.
- Change the default passwords before first use! This will reduce the risk of unauthorized access to your system.
- Regularly change the passwords used! This will reduce the risk of unauthorized access to your system.
- Regularly perform threat analyses. You can check whether the measures taken meet your security requirements.
- Use “defense-in-depth” mechanisms in your system's security configuration to restrict the access to and control of individual products and networks.

Note

Please note the risks of using cloud services!
If you use third-party cloud services, sensitive data is transferred to the cloud service provider at one's own responsibility. External access may result in manipulated data and/or unwanted control commands affecting the performance of your control system.

Use encryption methods to protect your data and observe the information provided by the Federal Office for Information Security – “Cloud: Risks and Security Tips”.
Observe comparable publications of the competent, public institutions of your country.

3 Overview

The controller combines HMI and control functions and can thus replace a PLC controller. Visu software and runtime software both run on the controller. It is suitable for mounting on a DIN rail and stands out on account of its various interfaces.

The interfaces are ETHERNET, USB, microSD and a line out (headphone output) and HDMI.

Furthermore, the interfaces also include digital inputs and outputs, an RS-232/RS-485 interface and a CAN interface for connecting additional I/Os.

The controller also has a NVRAM.

4 Properties

4.1 View

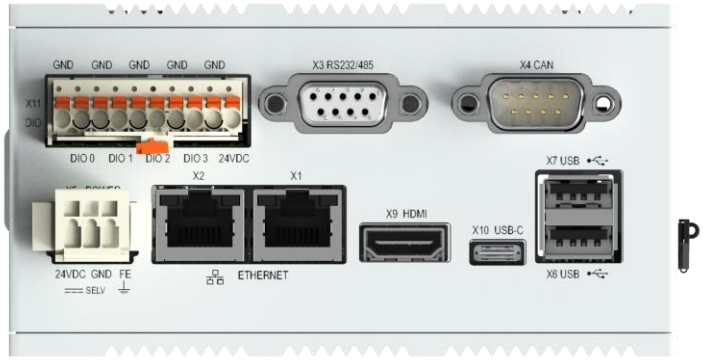

Figure 1: Front view

The connectors are located on the **front**. For details, see section “Properties” > “Connectors.”

Figure 2: View on top

The operating mode switch with the connector “X8 Lineout”, the settings RESET-STOP-RUN, the “CFG/RST” button, the “SYS, RUN, CAN, H11, H22” LEDs and the “µSD” memory card slot are located on the **top**. For details, see section “Properties” > “Connectors” > “Display Elements” and > “Operating Elements”.

4.2 Labeling

The labeling and the type plate are located on the bottom.
The following information about the product is included:

Table 3: Labeling

Field	Example
Supply voltage	SELV 24V [−25 % … +30 %], LPS
Protection class	Class III
IP degree of protection	IP20

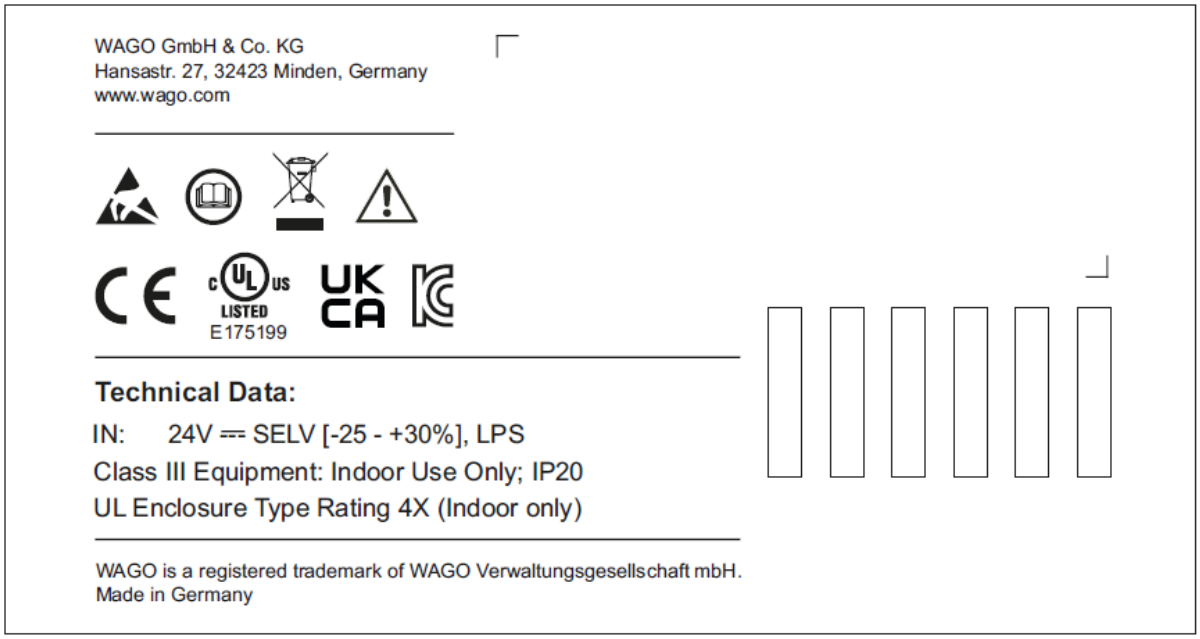

Figure 3: Labeling (Example)

Table 4: Type plate

Field	Example
Item Number	ITEM-NO.: 0752-8303/8000-0002
Item description 1	Edge Controller
Item description 2	EC PIO3
Control number	24703.5303
Date of manufacture (year – month)	2021-02
Release index: Hardware version	 01
Power consumption	Pmax.=9,4 W
Supply voltage	U=SELV 24V DC (−25 % … +30 %), LPS
Serial number	SN:37SUN31564010260448761+0 000000002331381
Barcode	
Data matrix code	

Figure 4: Type plate (Example)

4.3 Connectors

4.3.1 Connectors on the front

Table 5: Connectors on the front

Connector	Function
X1 und X2	ETHERNET Interface with LED
X3	Serial Interface RS-232 or RS-485
X4	CAN Interface
X5	POWER. Power supply
X6 and X7	USB 2.0 Host Interface
X9	HDMI Interface
X10	USB-C Interface
X11	4 digital Inputs and Outputs DIO

4.3.2 Connectors on top

Table 6: Connectors on top

Connector	Function
X8	Line-out audio output (headset)
microSD	Slot for microSD and microSDHC cards with cap, sealable

4.3.3 “X1” and “X2” ETHERNET Interfaces

The ETHERNET interfaces are RJ-45 ports. The orange LED illuminates when there is a LINK and the green one blinks during data transfer.

The connectors and cables meet category 5e requirements and guidelines for ETHERNET interfaces.

The integrated 10/100 Mbit ETHERNET switch supports Auto-MDI(X).
A crossover or patch cable can be used.

4.3.4 “X3” – RS-232/485 Serial Interface

This interface is designed as a D-sub 9 socket and is electrically isolated from the supply voltage of the product and the other interfaces. Baud rates from 1200 to 115,200 are supported.

The socket combines an interface as per RS-232 and an interface as per RS-485. However, the two interfaces must NOT be used simultaneously!

These communication partners must be set to the same interface type, since the voltage levels of the two types are NOT compatible!

Table 1: X3 Pin Assignment

Pin	Assignment as per EIA 232	Assignment as per EIA 485
1	-	-
2	RxD (receive data)	-
3	TxD (transmit data)	RXTX-P (Signal pos.)
4	-	-
5	GND (system ground)	GND (system ground)
6	-	VPP (system 5 V) (only for resistor or bias network)
7	-	-
8	-	RXTX-N (signal neg.)
9	-	-
Housing	Shielding	Shielding

NOTICE

Incorrect parameterization can damage the communication partners!
The voltage levels for RS-232 and RS-485 are not compatible!
If the controller interfaces differ from those of the communication partners (RS-232 <> RS-485 or RS-485 <> RS-232), this may damage the interface of the communication partner. Therefore, always ensure that the controller interface matches those of its communication partners when configuring these items!

Continuous shielding is essential in order to increase the immunity to interference. For this purpose, the metallic housing of the socket is connected to functional ground.

The connected data cable must be shielded. The cable clamp that is used must guarantee sufficient strain relief and contact between the shield and housing over a large area at the same time.

The data direction of the RS 232 interface of the product corresponds to device type DCE.

4.3.4.1 Operating as an RS-232 Interface

Depending on the device type DTE (Data Terminal Equipment, e.g., PC) or DCE (Data Communication Equipment, e.g., PFC, modem), the RS-232 signals have different data directions.

Table 7: Function of RS-232 Signals for DTE/DCE

Contact	Signal	Data Direction	
		DTE	DCE
2	RxD	Input	Output
3	TxD	Output	Input
5	FB_GND	---	---

For a DTE-to-DCE connection, the signals are connected directly (1:1).

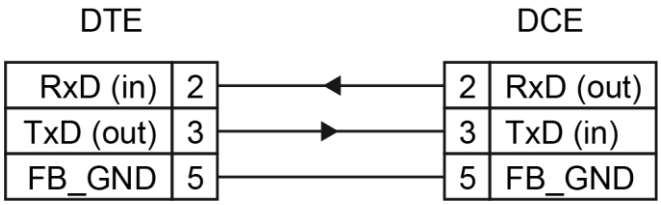

Figure 5: Termination with DTE-DCE Connection (1:1)

For a DCE-to-DCE connection, the signal connections are crossed (cross-over).

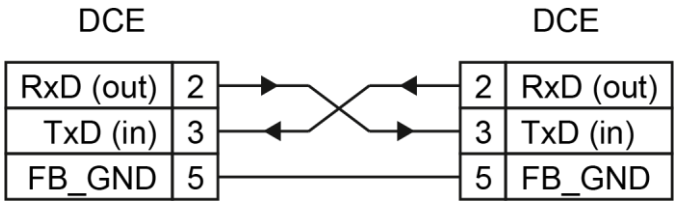

Figure 6: Termination with DCE-DCE Connection (Cross-Over)

4.3.4.2 Operating as an RS-485 Interface

To minimize reflection at the end of the line, the RS-485 line must be terminated at both ends by a cable termination. If required, one pull-up or pull-down resistor may be used. These resistors ensure a defined level on the bus when no subscriber is active, i.e., when all subscribers are in “Tri-state”.

Note

Attention — bus termination!
The RS-485 bus must be terminated at both ends!
No more than two terminations per bus segment may be used!
Terminations may not be used in stub and branch lines!
Drop cables must be kept as short as possible!
Operation without proper termination of the RS-485 network may result in transmission errors.

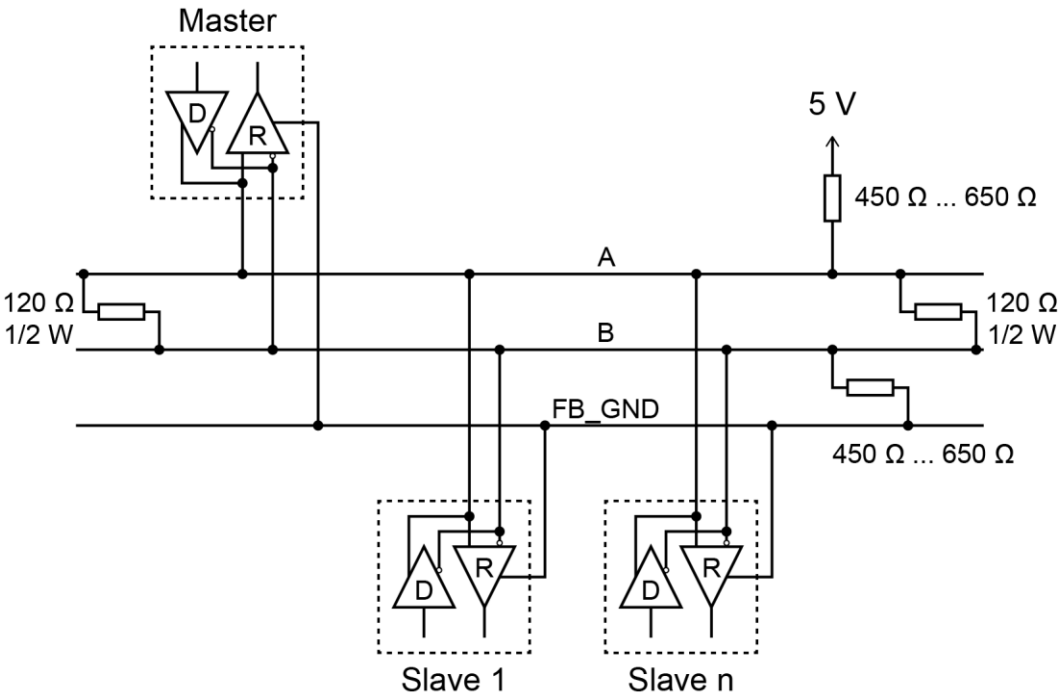

Figure 7: RS-485 Bus Termination

4.3.5 “X4” – CAN Interface

This interface is designed as a D-sub 9 plug and is electrically isolated from the supply voltage of the device and the other interfaces.
The interface corresponds to ISO 11898-2.

Table 1: X4 Pin Assignment

Pin	Assignment
1	-
2	CAN-L (CAN data low)
3	GND (reference potential 0 V or ground)
4	-
5	-
6	-
7	CAN-H (CAN data high)
8	-
9	-

Continuous shielding is essential in order to increase the immunity to interference. The metallic housing of the plug is capacitively connected to functional ground.
The connected data cable must be shielded. The cable clamp that is used must guarantee sufficient strain relief and contact between the shield and housing over a large area at the same time.

4.3.6 “X5” Supply Voltage

Connect the supply voltage to the X5 connector. For this, use the included 734-103 female connector featuring three CAGE CLAMP® connections.
For more information about the supply voltage, see section “Device Description” > “Technical Data”.

Table 8: X5 Pin Assignment

Pin	Description	Assignment
1	24VDC	Supply voltage: +24 VDC
2	GND	Reference potential 0V (ground)
3	FE	Functional earth

4.3.7 “X6” and “X7” USB-2.0 Interfaces

The USB 2.0 host interfaces are designed with 4-pin type A sockets. Each interface can supply max. 500 mA.

The connectors comply with the USB 2.0 specification.

Keyboards or mice can be connected as alternative input devices or up to 2 USB memory devices. These USB devices must be connected before power ON.

4.3.8 “X8” – Line-out Audio Output (Headphones)

The audio output is a three-pole, 3.5 mm stereo socket. Headphones or a compatible audio device can be connected to this socket, e.g. in order to output acoustic warning signals or voice messages that the control application contains.

4.3.9 “X9” – HDMI Interface Type A

HDMI stands for “High Definition Multimedia Interface”. The HDMI port is a standard connection for simultaneous transmission of video and audio via a single cable. The product can be connected to a monitor via the HDMI interface. FULL HD resolution (1920×1080) is supported.

Note

HDMI Interface designed for different areas of application!
Use of the HDMI interface is not permitted in residential, business, commercial areas, as well as small businesses.
Use of the HDMI interface is permitted in the industrial sector.

4.3.10 ”X10” – USB-C Interface

You can establish an IP connection via the USB service interface for commissioning and for service purposes, see also chapter “Commissioning” > “Setting an IP Address” > “IP Connection via USB”.

The USB service interface is designed as a USB-C socket. The interface supports USB Specification 2.0.

The controller appears on the host device (PC) as a peripheral device in device mode.

4.3.11 “X11” – Four Digital Inputs and Outputs DIO

There are four digital connectors, configurable as inputs or outputs, for connecting actuators and sensors.
A 10-pole *picoMAX*® plug is used with 10 push-in CAGE CLAMP®S connections (female connector 2091-1110).
The connections are specified per EN 61010-2-201:
DC, general use

Table 9: X11 Pin Assignment

CAGE CLAMP®	Name	Assignment
1	GND	Reference potential 0 V (ground)
2	DIO 0	Digital I/O 0
3	GND	Reference potential 0 V (ground)
4	DIO 1	Digital I/O 1
5	GND	Reference potential 0 V (ground)
6	DIO 2	Digital I/O 2
7	GND	Reference potential 0 V (ground)
8	DIO 3	Digital I/O 3
9	GND	Reference potential 0 V (ground)
10	24VDC	Supply voltage for digital inputs and outputs

The digital inputs/outputs are electrically isolated from the supply voltage of the product and from the other interfaces.

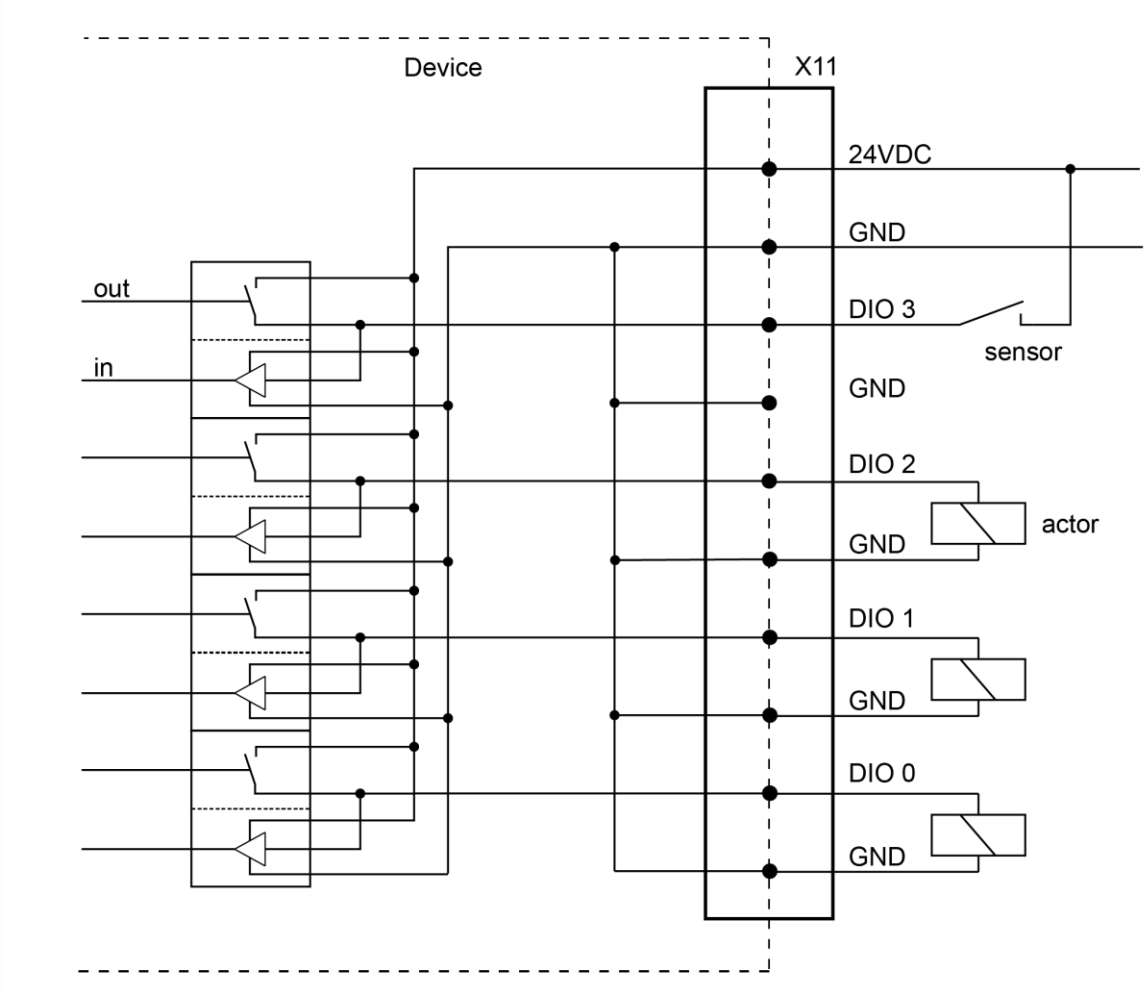

Figure 8: Connections DIO X11 (Example)

4.3.12 “microSD” Memory Card Slot

The product is equipped with a laterally mounted slot for microSD and microSDHC memory cards.

microSD (max. 2 GB) and microSDHC (max. 32 GB) cards tested by WAGO can be used.

⚠ CAUTION

Use only WAGO memory cards!
Proper function and performance cannot be ensured when using SD/SDHC memory cards not approved by WAGO.

Note

Pay attention to the memory card preformatting!
Please note that memory cards ≤ 2 GB are often formatted with the “FAT16” file system type and can generate up to 512 entries in the root directory. For more than 512 entries, generate them in a subdirectory or format the memory card as “FAT32.

4.4 Real-Time Clock

The real-time clock RTC is installed internally and not accessible. It is for internal use only.

Deviation/accuracy

The deviation is less than ± 4 sec/day with an ambient temperature of 25 °C.

Power reserve

The clock continues to run min. 35 days (corresponds to 840 hours) at 25 °C after shutting off the power supply.
After more than 35 days without a power supply, a clock setting dialog appears to enter the time again. The appearance of the dialog can be switched ON or OFF in the configuration.
There is no battery for buffering.

Resolution

The resolution of the clock for date and time is 1 sec.
Date and time are supplied and queried by the application.

4.5 Display Elements

4.5.1 Status LED

On the left side, there are 1 tricolor LED and 4 two color LEDs.

The SYS LED indicates the status.

Table 10: SYS LED

LED Display	Explanation
Green, steady	The product is ready to operate.
Red, flashing	There is an error. The specific error message is displayed.
Blue, flashing	There is a connection error to the controller. No communication

The RUN LED indicates the program status.

Table 11: RUN LED

LED Display	Explanation
Green, flashing	No application and no boot project loaded.
Green, steady	CODESYS V3 applications running.
Red, steady	All CODESYS V3 applications have stopped.

The CAN LED indicates the CANopen status.

Table 12: CAN LED

LED Display	Explanation
Green, steady	CAN communication is running.
Red, steady	CAN communication is disrupted.

Two other user LEDs, “H11” and “H22,” are provided for future applications.

4.6 Operating Elements

You can find the operating mode switch and the “CFG/RST” button on top.

4.6.1 Mode Selector Switch

The Mode Selector Switch has the following positions:

Table 13: Positions Mode Selector Switch

Position	Actuation	Function
RESET	Spring-return	**Reset warm start** or **Reset cold start** (depending on length of actuation, see Section “Starting” > “Initiating Reset Functions”)
STOP	Latching	**Stop** All CODESYS V3 applications have stopped.
RUN	Latching	**Normal operation** CODESYS V3 applications running.

Using the button “CFG/RST” button you can initiate a “Factory Reset”. See section „Service“ > „Factory Reset“.

4.6.2 “CFG/RST” Button

The “CFG/RST” button is installed inside a hole to prevent accidental operation. It is a shortstroke button with a low actuating force of 1.1 N … 2.1 N (110 gf … 210 gf). The button can be actuated using a suitable object (e.g., a pen).

With the “CFG/RST” button, you can:

- Change the configuration with the WBM
- Restore the factory settings (“factory reset”)

Please refer to the sections of the same names further back in this manual for information about the functions.

4.7 Schematic Diagram

NOTICE

Do not use grounded USB devices!

USB interface shielding is not grounded directly, but rather via interference-suppression capacitors. Only keyboards, mice and USB memory sticks should be connected to the USB ports. Do not connect devices that are grounded, e.g., printers, because they bridge the interference-suppression capacitors, and immunity to interference is reduced.

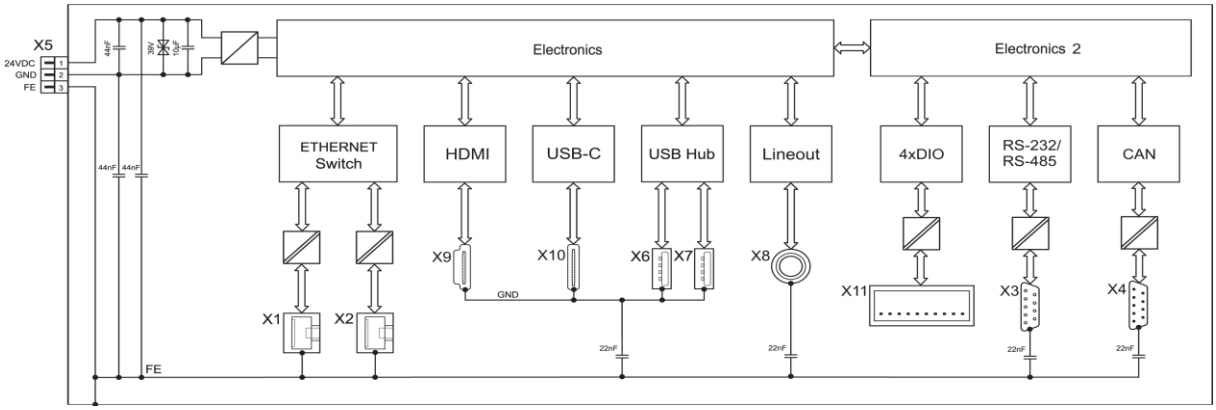

Figure 9: Schematic Diagram

4.8 Technical Data

4.8.1 Device

Table 14: Technical Data – Device

Housing material	Aluminum, powder-coated
Dimensions (width × height × depth)	65 × 123 × 115 mm
Type of mounting	DIN-rail
Weight	835 g
IP degree of protection	IP20
Protection class	SK III
Overvoltage category	II
Pollution degree	2

4.8.2 Climatic Environmental Conditions

Table 15: Technical Data – Climatic Environmental Conditions

Permissible ambient temperatures	−20 ... +60 °C
Permissible storage temperature	−20 ... +80 °C
Relative humidity (without condensation)	90 %
Operating altitude	0 … 2000 m

4.8.3 Power Supply

Table 16: Technical Data – Power Supply

Operating Voltage	SELV (Safety Extra Low Voltage) – voltage source that meets the requirements of a LPS (Limited Power Source) as per EN 60950-1 24 VDC (18 ... 31,2 V) with reverse voltage protection
Max. current consumption across the entire voltage range, without/with external USB devices	120 mA / 390 mA
Max. power consumption across the entire voltage range, without/with external USB devices	2,9 W / 9,4 W

4.8.4 Hardware

Table 17: Technical Data – Hardware

Processor	ARM® Cortex® A9 Quadcore 1.0 GHz
External memory extension („µSD“ Slot)	microSD memory card (max. 2 GB) or microSDHC memory card (max. 32 GB)
Main memory (RAM)	2 GB
Internal memory (flash)	4 GB

4.8.5 Communication

Table 18: Technical Data – Communication

Fieldbus	MODBUS TCP/UDP/RTU und CAN
Protocols	ETHERNET TCP/IP, DHCP, DNS, FTP, FTPS, HTTP, HTTPS und SSH

4.8.6 Interfaces

Table 19: Technical Data – Interfaces Hardware

ETHERNET Interfaces	2 × RJ-45,witht Switch, 10/100 Mbit/s, connecting cables twisted pair SF-UTP, 100 Ohms, category 5e, patch or crossover, max. 100 m
Serial Interface RS-232/-485	1 × D-Sub-9
CAN Interface	1 × D-Sub-9
USB Interfaces	2 × USB 2.0 Host (type A), 480 Mbit/s, connecting cables max. 3 m, Current draw max. 2 × 500 mA 1 × USB OTG (type C)
„µSD“ Slot	For memory cards microSD and microSDHC
HDMI	1 × HDMI (Type A)

4.8.7 Connectors

Table 20: Technical Data – Connections Hardware

Voltage supply	3 × CAGE CLAMP®, connection cable, max. 3 m to power supply, conductor cross section: 0.14 … 1.5 mm² / AWG 25 … 14, strip length: 7 mm / 0.28 inch, Conductor material cooper (Cu), Temperature resistance of conductors min. 75 °C
Audio output for headphones	3-pole stereo socket, 3,5 mm, headphone output: 62.5 mW at 16 ohm, frequency range: 20 … 20,000 Hz
Four DIO digital inputs or outputs	10 × push-in CAGE CLAMP®, 4 inputs as per IEC 61131-2 type 1/outputs as high-side switch, 24 V 0.5 A conductor cross section: 0.2 … 1,5 mm² / AWG 24 … 14, strip length: 8 … 9 mm / 0.31 … 0.35 inch, Conductor material cooper (Cu), Temperature resistance of conductors min. 75 °C

4.9 Approvals

The following approvals have been granted to the products:

Conformity Marking

UK Conformity Assessed

cULus: UL61010-1, UL61010-2-201

Korea Certification: R-R-W43-EDGE752

Eurasian Conformity: EAC RU Д-DE.PA01.B.09690/21

Information

Detailed information regarding approvals
Detailed information regarding approvals can be found at:
https://www.wago.com <item no.>

4.10 Standards and Guidelines

The products meet the following requirements on emission and immunity of interference:

EMC CE-Immunity to interference	EN 61000-6-2
EMC CE-Emission of interference	EN 61000-6-3

Note

HDMI Interface designed for different areas of application!
Use of the HDMI interface is not permitted in residential, business, commercial areas, as well as small businesses.
Use of the HDMI interface is permitted in the industrial sector.

5 Functions

The Controller combines HMI and control functions, since it is a PLC as per IEC 61131-3. Furthermore, four actuators/sensors can be connected to the four digital I/Os. If more are needed, fieldbus nodes can be connected via the fieldbus interfaces.

Commissioning is performed in the Web browser with the “Web-Based Management WBM” software. During ongoing operation of the system that is to be controlled, the target visualization, which was programmed on the engineering PC with the CODESYS V3 application is then displayed with CODESYS V3 via the HDMI interface. The visualization can also be provided to other display devices through the integrated Webserver.

ETHERNET is used for communication with the engineering PC. Communication with other controllers/couplers occurs over ETHERNET or a fieldbus.

Note

HDMI Interface designed for different areas of application!
Use of the HDMI interface is not permitted in residential, business, commercial areas, as well as small businesses.
Use of the HDMI interface is permitted in the industrial sector.

5.1 Web Browser

The integrated Web browser displays the controller websites.
Up to 10 controllers can be configured in the WBM. The “PLC List”/”Browser Favorites” is used to select a controller and to launch his Web visualization directly via the HDMI interface.

The Web browser can display Web pages via encrypted connections (HTTPS).

The virtual keyboard opens automatically when an input field is actuated. The user can use the “Switch keyboard” button to switch between levels (letters and numbers).
The user can choose between the “virtual keyboard” and “CODESYS numpad and keypad” in a CODESYS visualization.

The following can be configured as the start page:

- the WBM
- the selection list “PLC List”/”Browser Favorites”
- the Web visualization of a specific controller directly

See “Favorites” Page in the WBM for the configuration of the start page.

5.2 Connection Monitoring

If a CODESYS visualization connection is interrupted, an error message is displayed in the browser. It automatically attempts to restore the connection (reconnect) every 10 seconds.

5.3 WBM for Configuration/Parameterization

The Web-Based Management (WBM) provides an interface for configuring or parameterizing the controller. The WBM can be called up from the controller directly or on the engineering PC.

A detailed description of all available elements and functions is available in Section “Commissioning”.

5.4 Network

5.4.1 Interface Configuration

The X1 and X2 ETHERNET interfaces are connected to an internal 3-port switch, whose third port is connected to the CPU. The “Configuration Type” is set to “DHCP” by default. The TCP/IP settings such as IP address or subnet

5.4.1.1 Operation with Separate Network Interfaces

When operating with separate network interfaces, both ETHERNET interfaces can be configured and used separately.
Note that the two interfaces still have the same MAC address. Therefore, they must not be operated in the same network segment.

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

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

5.4.2 Network Security

5.4.2.1 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

Default passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs.

5.4.2.2 Services and Users

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

	Users					
	WBM		Linux®			
Service	**admin**	**user**	**root**	**admin**	**user**	**SNMP**
Web-Based Management (WBM)	X	X				
Linux® console			X	X	X	
CODESYS				X		
Telnet			X	X	X	
FTP			X	X	X	
FTPS			X	X	X	
SSH			X	X	X	
SNMP						X

5.4.2.3 WBM User Group

The Web-Based Management (WBM) has its own user management. The users in this system are isolated from the other user groups in the system for security reasons.
At initial start-up, you are prompted in the WBM to change the password when logging in as an Admin user.
This does not change the passwords for the Linux® “root” and “admin” users!

Table 21: WBM Users

User	Permissions	Default Password
admin	All (administrator)	wago
user	Supported to a limited extent	user

5.4.2.4 Linux® User Group

The Linux® user group includes the actual users of the operating system who are also used by most services. The passwords for these users are to be configured via SSH terminal connection.

Table 22: Linux® User

User	Special Feature	Home Directory	Default Password
root	Superuser	/root	wago
admin	CODESYS user	/home/admin	wago
user	Normal user	/home/user	user

Note

Change passwords
Default passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs.

Example

The PuTTY SSH client is used via ETHERNET to change the default password for the Linux® user “root”.
After launching putty.exe, “login as:” appears. Enter “root” and press [**Enter**]. You are prompted to enter the password. Enter “wago” as the default password. You are prompted to assign a “New password:”. Enter a unique password that meets the required level of security and press [**Enter**]. You are prompted to “Retype password:”. Enter your password again and press [**Enter**] to change the password.
Repeat the process when logging in as a Linux® “admin” user.

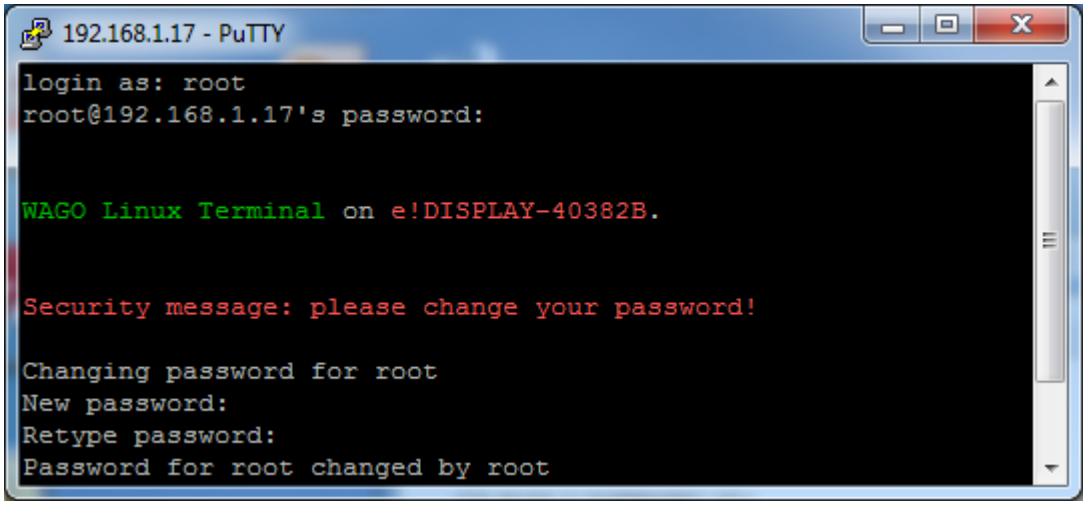

Figure 10: Example for Linux® Password

5.4.2.5 SNMP User Group

The SNMP service manages its own users. In its initial state, no users are stored in the system.

5.4.2.6 Web Protocols for WBM Access

The HTTP and HTTPS web protocols can be used to access the WBM pages. HTTPS is preferred because it uses the SSL/TLS protocol. The SSL/TLS protocol ensures secure communication through encryption and authentication.

5.4.2.7 TLS Encryption

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

The “TLS Configuration” group of the WBM page “Security” can be used to switch the cryptographic methods allowed for HTTPS and the TLS versions that can be used.

The settings “Strong” and “Standard” are possible.
If “Strong” is set, the Webserver only allows TLS Version 1.2 and 1.3 and strong algorithms.
Older software and older operating systems may not support TLS 1.2 and TLS 1.3 and encryption algorithms.
If “Standard” is set, TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.3 are allowed, as well as cryptographic methods that are no longer considered secure.

Information

BSI Technical Guidelines TR-02102
The rules for the “Strong” setting are based on technical guidelines TR-02102 of the German Federal Office for Information Security.
You can find the guidelines on the Internet at: https://www.bsi.bund.de > “Publications” > “Technical Guidelines.”

Information

BSI Guidelines on Migration to TLS 1.2 or TLS 1.3
The German Federal Office for Information Security guidelines on migration to TLS 1.2 or TLS 1.3 contain “compatibility matrices” that show what software is comparable with TLS 1.2 or TLS 1.3.
You can find the guidelines on the Internet at: https://www.bsi.bund.de > “Topics” > “Standards and Criteria” > “Minimum Standards“.

5.4.3 Network Configuration

5.4.3.1 Host Name/Domain Name

If the host name is not configured, the product receives a default name based on the last three values of the product’s MAC address. The name applies as long as no host name is configured or no host name is given to the product by DHCP (to configure, see section “Commissioning” > “Configuring in the Web-Based Management (WBM)”). When the host name is set, a host name supplied by a

DHCP response is immediately active and displaces the configured or default host name. If only the configured name should apply, the network administrator must adjust the configuration of the active DHCP server, so that no host name is passed in the DHCP response.

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

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

5.4.3.2 Default Gateways

Two default gateways can be set for the product in the TCP/IP configuration. A network station transmits to a default 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.

A so-called metric is assigned to the default gateways that specifies with what time delay, sometimes called cost factor, a data packet can be forwarded via the gateway. If multiple default gateways are configured, the operating system transmits the data packets to the default gateway configured with the lowest metric. If this gateway is not accessible, an attempt is made to access the gateway with the next higher metric. If several of the gateways have the same metric, the gateway is determined randomly. If this gateway cannot transmit the data packet, the data packet is sent simultaneously to all other gateways of the same metric.

The metric of the configured default gateways can be specified for the product. The default value for the metric is 20. Besides the directly configured gateways, other gateways can be set via DHCP responses so that more than two gateways are possible. All gateways transferred via DHCP are assigned a permanent metric of 10. The DHCP gateways are thus normally given priority on account of their low metric.

5.5 Memory Card Functions

The memory card is optional and is used as an additional memory range for the internal memory or drive. Device settings and the product's firmware can be saved on the memory card.

5.5.1 Backup

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

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

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

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

5.5.2 Restore

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

The network, or when inserted, the memory card or can be selected as the source medium.

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.

Note

The device restarts if parameters change!
Note that the device loading the data executes a restart if parameters in the internal drive are overwritten with different parameter settings from the memory card.

Note

Data size may not be larger than the internal drive size!
Note that the size of data in the media/sd/copy directory may not exceed the total size of the internal drive.

5.5.3 Create Image

This WBM function can be used to create a bootable copy of the system currently booted. If the product was started from the internal flash, a copy is written to the memory card via the function “Create Image”. If the product was started from the memory card, a copy is saved to the internal flash. The existing image is deleted.

5.6 Downloading Software

The product has the option to install or update individual software packages. The software packages are available from WAGO.
You can install them from your PC via WBM. See also WBM page „Software Uploads“.

5.7 Booting

Start Behavior

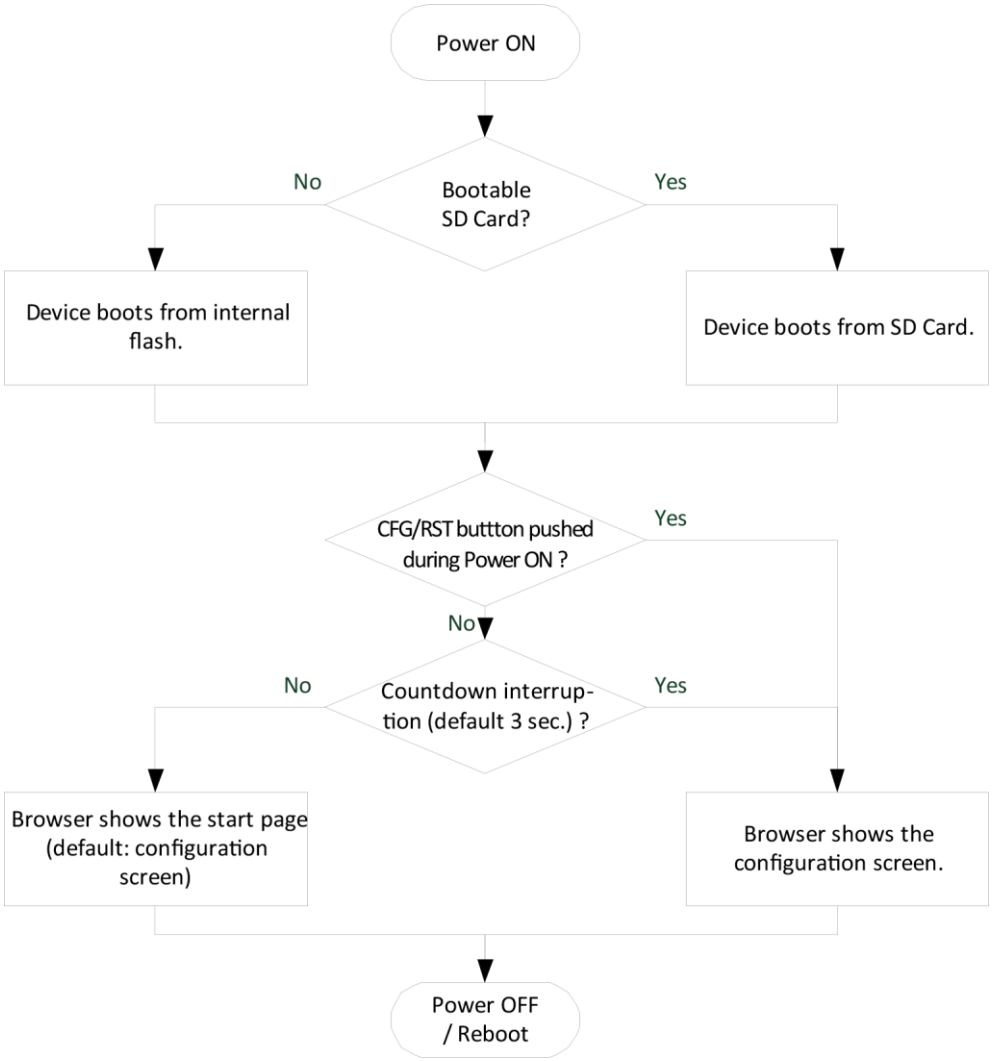

Figure 11: Start Behavior

Browser

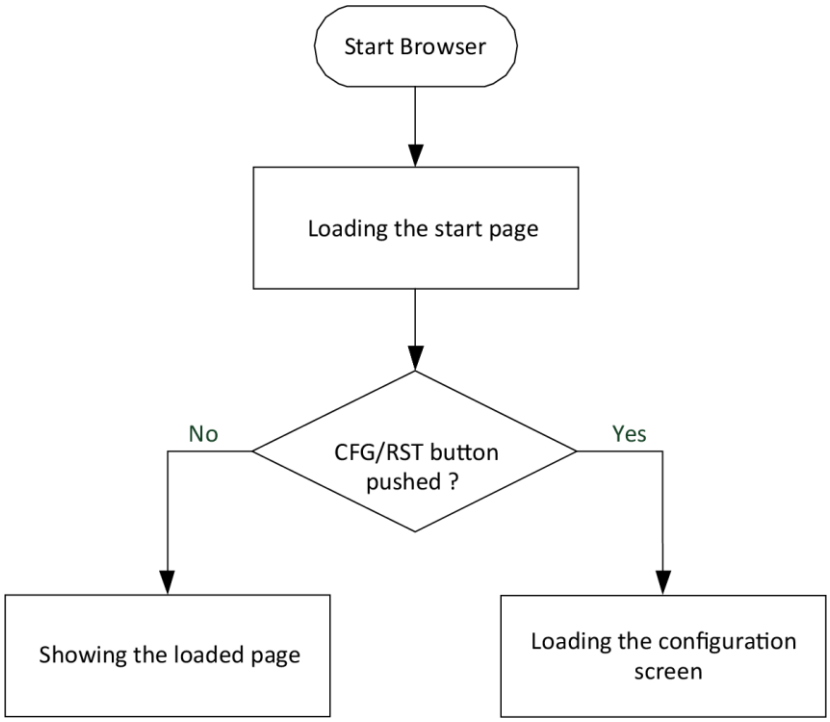

Figure 12: Browser process

Button “CFG/RST”

Pressing the button “CFG/RST” at run-time opens the WBM.
Pressing the button at products startup (power ON) prevents the normal auto start and only the WBM starts. The button is not used to make any changes to the settings.

5.8 Licensed Software Components

The CODESYS V3 runtime system software components that are subject to license verification are available for the product.

The Add-on Licensing can be used for licensing.

A license key is required for productive use without time restriction of a software component that is subject to licensing. Full use of the software component is possible even without a license is limited in time. This trial period only includes the amount of time that is required for actual use. Access without a license key is no longer possible after the trial period.

The license status (“Evaluation period not yet expired” or “Evaluation period has expired”) is displayed by the controller via the SYS LED.

6 Mounting

NOTICE

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

NOTICE

Do not cover the ventilation openings!
To ensure adequate air circulation, the ventilation openings must be kept clear. Keep at least 100 mm from the ventilation openings to adjacent surfaces.

Note

Avoid exposure to direct light!
Position the product to avoid direct exposure to a strong light source, e.g., sunlight!

6.1 Assembly Guidelines/Standards

- DIN 60204 Electrical equipment of machines
- DIN EN 50178 Electronic equipment for use in power installations (replacement for VDE 0160)
- EN 60439 Low-voltage switchgear and controlgear assemblies

6.2 Mounting position

Nominal mounting position: Front, marking legible, top and bottom ventilation openings.

The product can also be mounted in a horizontal position so that the connections face downward. The DIN-rail adapter must be removed from the back panel for this and attached on the side.

Device must not be operated without air gap. If adjacent device is equivalent under full load the air gap has to be at least 12 mm. If adjacent device does not generate heat the air gap has to be at least 6 mm.

6.3 Mount to the Rail

Mount the product by snapping it into the rail according to EN 60715:

1. Place the product with its rail guide on the top edge of the rail.
2. Press the product onto the rail while simultaneously pulling on the latch until it locks into place.
3. To ensure secure fastening on the rail, fit end clips on either side of the device (e.g., Article No. 249-197).

7 Connecting

7.1 Earthing

Earthing is performed via connector X5.
For this, use the included 734-103 Female Connector featuring three CAGE CLAMP® connections. First, open CAGE CLAMP® no. 3 using an operating tool. Then insert the conductor (strip length: 7 mm, max. 1.5 mm²) and remove the tool.
Plug the female connector into the X5 connector and then verify that the clamping connection is secured.

7.2 Connecting Devices

Peripherals are connected electrically by the interfaces on the bottom and front side.

The **ETHERNET interfaces** are used to connect to a LAN or to the Internet for communication with the controller. Crossover or patch cables category 5e can be used.

The **USB 2.0 interfaces** can be used to connect a keyboard or mouse as an alternative input device. Also, up to 2 USB memory devices can be connected. Because there are a large number of USB devices on the market, no guarantee can be made about the function of individual devices.
USB/HDMI devices must be connected before power ON because they are not hot-pluggable.

NOTICE

Do not use USB devices connected to earth!
USB interface shielding is not earthed directly, rather via interference-suppression capacitor. Only keyboards, mice and USB memory sticks may be connected. Do not connect devices that are earthed, e.g., printers, because they bridge the interference-suppression capacitors and thus interference immunity is reduced.

NOTICE

HDMI in an industrial environment only!
The HDMI interface may only be used in an industrial environment.
Do not connect the HDMI port in residential, commercial, business or small business areas.

Insert **microSD** memory cards as far into the slot until they click into place. The slot can be sealed to protect the card.
To remove, press the card further down until the lock releases. The card can then be removed.

If your application includes acoustic signals/warnings, you can plug the 3.5 mm stereo plug of headphones or similar audio systems into the **audio output socket**.

For more information about the interfaces, see section “Device Description” > “Connectors” and “Technical Data”.

7.3 Connecting the Power Supply

Connect the power supply to connector X5, pin 1 (+) and 2 (−). To do this, you must also use the included 734-103 Female Connector.

8 Commissioning

8.1 Switching ON

The product does not have an ON/OFF switch and is switched on together with your machine resp. system.

After booting the system, you are taken, either automatically or manually, via the HDMI interface to the WBM, “PLC-List”/“Browser Favorites” or a selected controller, depending on the settings (in the menu, accessed by swiping downward from the top edge of the screen). You can interrupt the automatic sequence and arrive at a selection menu if you interrupt the countdown shown by clicking.

8.2 Login

Before the WBM interface can be displayed, you are prompted to log in with a user name and password. When starting the WBM for the first time, you have to use the initial password. You can log in as “administrator” or “user”. Different functionalities are available to the different user groups. See “Configuring in the Web-Based Management (WBM) > User Management of the WBM” and “Configuring in the Web-Based Management (WBM) > Access Rights.”

8.3 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 MS DOS 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 **[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 appropriate parameters, are displayed.

8.4 Setting an IP Address

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

Table 23: Default IP Addresses for ETHERNET Interfaces

ETHERNET Interface	Default Setting
X1/X2 (switched mode)	Dynamic assignment of IP address using DHCP (“Dynamic Host Configuration Protocol”)

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

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

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

Table 24: Network Mask 255.255.255.0

Host PC	Subnet Address Range for the Controller
192.168.1.2	**192.168.1**.1 or **192.168.1**.3 … **192.168.1**.254

8.4.1 IP Connection via USB

1. Connect the controller to your PC via the USB service interface and a suitable USB-C 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.

8.4.2 Changing an IP Address using “WAGO Ethernet Settings”

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

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

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

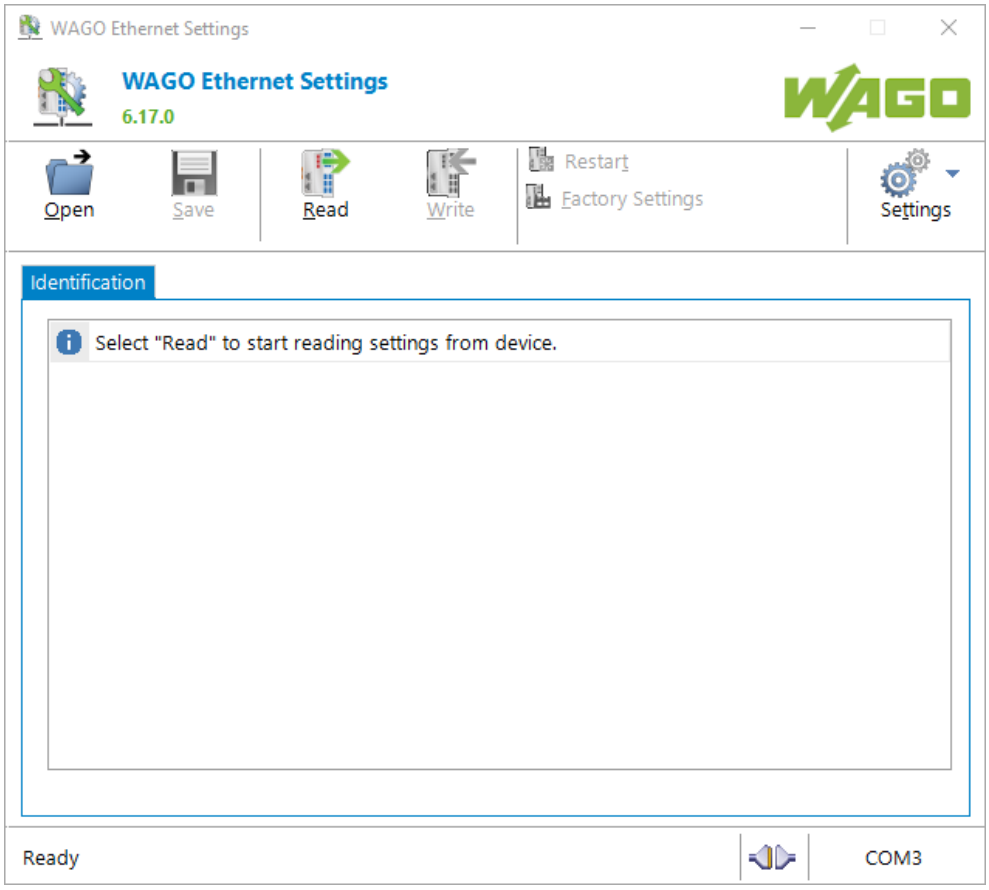

Figure 13: “WAGO Ethernet Settings” – Starting Screen (Example)

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

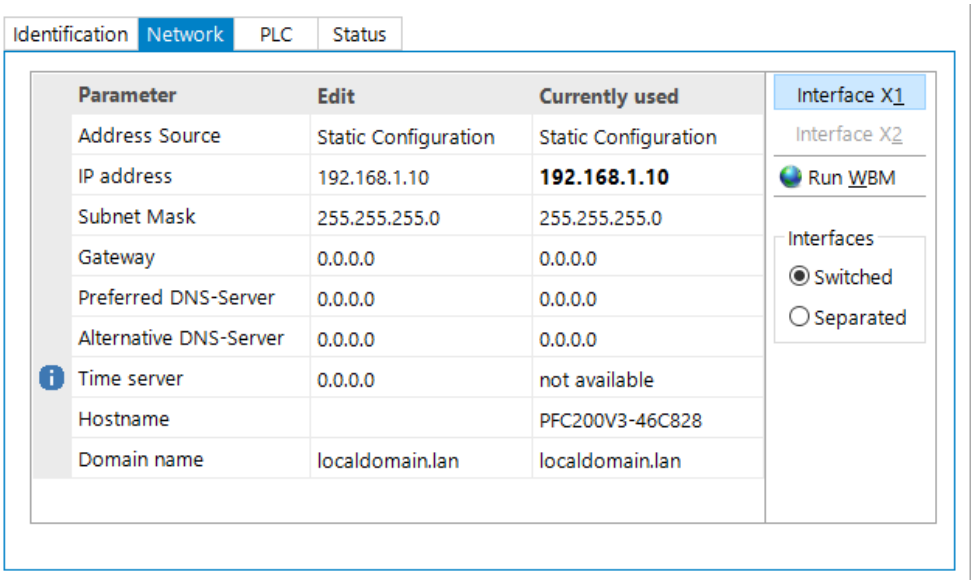

Figure 14: “WAGO Ethernet Settings” – “Network” Tab (Example)

7. To assign a fixed address, select “Static configuration” on the “Source” line under “Input”. DHCP is normally activated as the default setting.

8. In the “Input” column, enter the required IP address and, if applicable, the address of the subnet mask and of the 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. Click the **[Run WBM]** button in the right in the pane.

8.4.3 Temporarily Setting a Fixed IP Address

This procedure temporarily sets the IP address for the X1 interface to the fixed address “192.168.1.17”.
When the switch is enabled, the fixed address is also used for interface X2.
When the switch is disabled, the original address setting for interface X2 is not changed.
No reset is performed.

To make this setting, proceed as follows:

1. Set the mode selector switch to STOP.

2. Press and hold the button “CFG/RST” for longer than 8 seconds.

Execution of the setting is signaled by the “SYS” LED flashing orange.

To cancel this setting, proceed as follows:

- Perform a software reset or
- Switch off the controller and then switch it back on.

8.4.4 Setting the IP Address via the WBM

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

1. Use a suitable network cable to connect the controller and your PC.
2. Open an internet browser on the PC.
3. Call up the WBM on the controller. To do this, enter the following in the input line of the browser: “https://<IP address>/wbm”.
4. If you do not know the IP address, determine the IP address as described above.
   You will then be asked to authenticate.
5. Enter the user name “user” and the corresponding password (“user” by default).
   If you have not already changed the default password, you are asked to change the password now.
6. Open the “Configuration” tab.
7. In the navigation, select the “Networking” item and “TCP/IP Configuration” subitem.
8. In the “TCP/IP Configuration” group, select the “Static IP” entry in the “IP Source” selection field.
9. Enter the required IP address in the “Static IP Address” input field.
10. Enter the required subnet mask in the “Subnet Mask” input field.
11. Click the **[Submit]** button to apply the changes.
    Changing the IP address interrupts the connection to the controller.
12. Establish a new connection with the new IP address.

8.4.5 Assigning an IP Address using DHCP

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

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

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

The following example shows the corresponding output of “Open DHCP”.

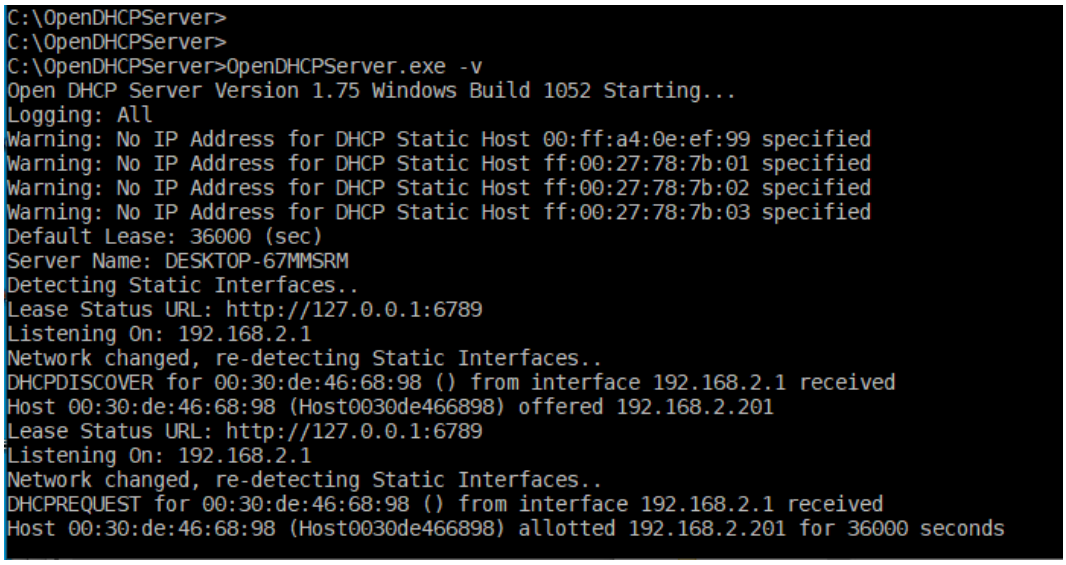

Figure 15: “Open DHCP”, Example Figure

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

The host name is “Host0030de466898”.

8.5 Initiating Reset Functions

You can initiate various reset functions using the mode selector switch and the button “CFG/RST”.

8.5.1 Warm Start Reset

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

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.

8.5.2 Cold Start Reset

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

To perform a cold start 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. You can then release the mode selector switch.

8.5.3 Software Reset

The controller is restarted on a software reset.

To perform a software reset, set the mode selector switch to RUN or STOP and then press the button “CFG/RST” for one to eight seconds.

Reset completion is indicated by the SYS LED, which lights up briefly red and then white. After a few seconds the SYS LED will indicate successful boot-up of the controller.

8.5.4 Factory 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!
All controller parameters and passwords are overwritten by a factory reset.
Stored boot projects are deleted, including existing web visualization data.
Subsequently installed firmware functions are not overwritten.
If you have any questions, contact WAGO Support.

The controller is restarted after the factory reset.
Proceed as follows to factory reset the controller:

1. Press the Reset button (CFG/RST).
2. Set the mode selector switch to the “RESET” position.
3. Press and hold both buttons until the “SYS” LED alternately flashes red/green after approx. 8 seconds.
4. When the “SYS” LED flashes red/green alternately, release the mode selector switch and Reset button.

Note

Do not interrupt the reset process!
If you release the Reset button (CFG/RST) too early, then the controller restarts without performing the factory reset.

8.6 Configuring in the Web-Based Management (WBM)

The HTML pages (from here on referred to as “pages”) of the Web-Based Management are used to configure the controller. Proceed as follows to access the WBM using a web browser:

1. Connect the controller to the ETHERNET network via the ETHERNET interface X1.

2. Start a Web browser on your PC.

3. Enter “https://” followed by the controller's IP address and “/wbm-ng” in the address line of your web browser, e.g., “https://192.168.1.17/wbm-ng”.
   Note that the PC and the controller must be located within the same subnet (see Section “Setting an IP Address”).
   If you do not know the IP address and cannot determine it, switch the controller temporarily to the pre-set address “192.168.1.17” (“Fixed IP address” mode, see Section “Commissioning” > … > “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. It is therefore important to stop the CODESYS application prior to performing complicated configurations using WBM.

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

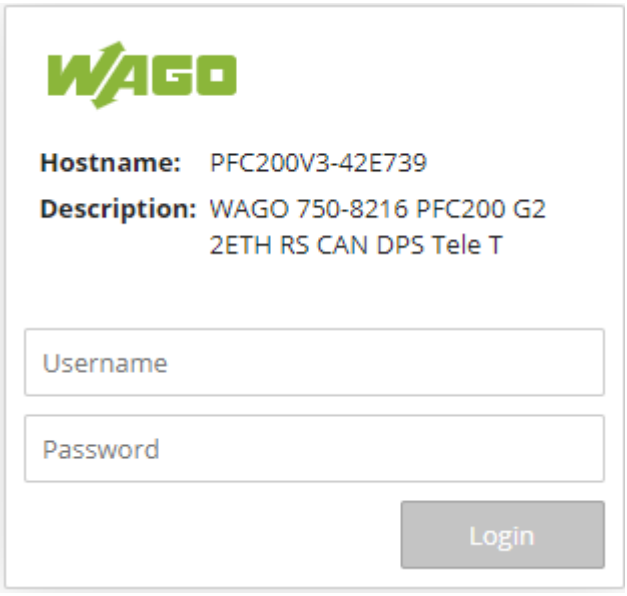

Figure 16: Entering Authentication

4. Enter the username and password.

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

→ Depending on the user selected, the navigation bar and the tabs of the WBM are displayed.

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.

8.6.1 WBM User Administration

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

Note

Change passwords
Default passwords are documented in these instructions and therefore do not offer adequate protection! Change the passwords to meet your particular needs.

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

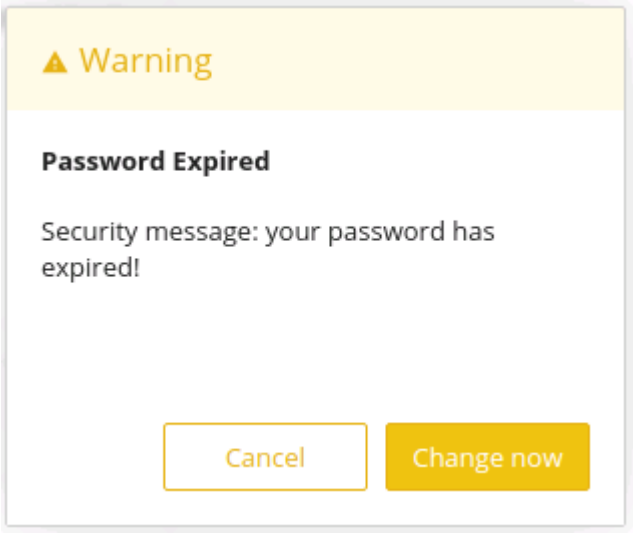

Figure 17: Password Reminder

Table 25:User Settings in the Default State

Users	Permissions	Default Password
root	All (administrator)	wago
admin	All (administrator)	wago
user	Supported to a limited extent	user

Note

General Rights of WBM Users
The WBM users “root”, “admin” and “user” have rights beyond the WBM to configure the system and install software.

User administration for controller applications is configured separately.

Access rights for the WBM pages are shown in the table below.
The “root” user has the same rights as the “admin” user and is therefore not listed separately.

Table 26: 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	Tademarks Information	user
WBM Version	WBM Version Info	user
Configuration		
PLC Runtime	PLC Runtime Configuration	user
Networking		
TCP/IP Configuration	TCP/IP Configuration	user
Ethernet Configuration	Ethernet Configuration	user
Host/Domain Name	Configuration of Host and Domain Name	user
Routing	Routing	user
STP/RSTP	Spanning Tree Protocol	user
Clock	Clock Settings	user
Administration		
Serial Interface	Configuration of Serial Interface RS232/RS485	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
DNS	Configuration of DNS Service	admin
Cloud Connectivity		

Table 26: Access Rights for WBM Pages

Tab/Navigation			WBM Page Title	User
	Status		Overview	admin
	Connection 1		Configuration	admin
	Connection 2		Configuration	admin
	SNMP			
		General Configuration	Configuration of general SNMP parameters	admin
		SNMP v1/v2c	Configuration of SNMP v1/v2c parameters	admin
		SNMP v3	Configuration of SNMP v3 Users	admin
	Browser Settings			
		Favorites	Favorites	user
		Autostart	Autostart	user
		Monitoring	Monitoring	user
		Browser Security	Browser Security	user
	Commissioning		Commissioning Settings	admin
	Docker		Docker Settings	admin
	Display			
		Font Upload	Fonts	user
		Display Orientation	Display Orientation	user
		Screensaver	Screensaver	user
	Users		WBM User Configuration	user
Fieldbus				
	OPC UA		OPC UA Configuration	admin
	BACnet			
		Status	BACnet Status	admin
		Configuration	BACnet Configuration	admin
		Data Link	BACnet Data Link	admin
		Storage Location	BACnet Storage Location	admin
Security				
	OpenVPN / 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

Table 26: Access Rights for WBM Pages

Tab/Navigation		WBM Page Title	User
	WAGO Device Access	WAGO Device Access	admin
Diagnostic			
	Log Message	Log Message Viewer	user
	Download	Download	admin
	Network Capture	Network Capture	admin

8.6.2 General Information about the Page

The IP address of the active device is displayed in the entry line of the browser window.

The WBM pages are only displayed after logging in. To log in, enter your username and password in the login window and click the **[Login]** button.

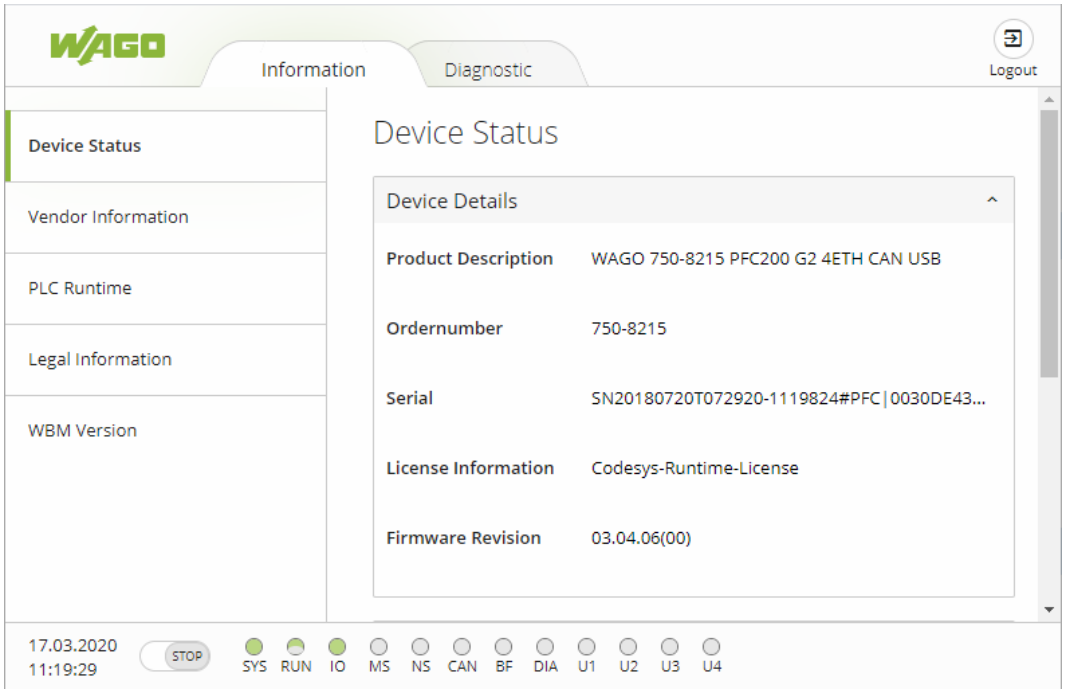

Figure 18: WBM Browser Window (Example)

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.

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

Figure 19: WBM Header with Tabs that Cannot be Displayed (Example)

The navigation tree is shown on the left 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, where provided, subpages included in these pages.

The current device status is displayed in the status bar.

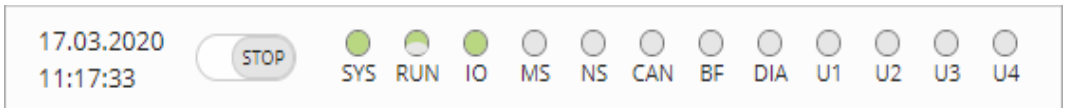

Figure 20: WBM Status Bar (Example)

- Date and Time - Local date and local time and on the device
- Setting of the mode selector switch
- LED status of the Device:
  All LEDs are graphically represented and are labeled with their particular designation (e.g., SYS, RUN, …). The following colors are possible:

  - gray: LED is off.
  - full color (green, red, yellow, orange): The LED is activated in the particular color.
  - half color:
    The LED is flashing in the corresponding color. The other half of the surface is then either gray or also colored. The latter case indicates that the LED is flashing sequentially in different colors.

  A tooltip containing more detailed information opens 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 shown.
  The states displayed in the WBM will not always correspond at the precise time to those on the controller. Data has a runtime during transmission and can only be queried at a certain interval. The time period between two queries is 30 seconds.

Note

Do not power cycle the controller after changing any parameters!
Some parameter changes require a controller restart for the changes to apply. Saving changes takes 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 the controller using the software reboot function. This ensures that all memory operations are completed correctly and completely.

A description of the WBM pages and the respective parameters can be found in the appendix in Section “Configuration Dialogs” > “Web-Based Management (WBM)”.

8.6.3 Reboot Function

Click the **[Reboot]** button. To restart, click the **[Reboot]** button. To cancel the restart, click **[Cancel]**.

9 Run-time System CODESYS V3

9.1 General Notes

Note

Additional Information
Information on the installation, startup and programming is provided in the CODESYS V3 documentation.

9.2 CODESYS V3 Priorities

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

Table 27: CODESYS V3 Priorities

Scheduler	Task	Linux® Priority	IEC Priority	Remark
Preemptive scheduling - Real-time range	Local bus or fieldbus - HIGH	-95 … -86		Local bus (-88)
	Mode selector 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 bus or 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 bus or fieldbus – LOW	-13 … -4		
Fair scheduling - None real-time range	CODESYS communication	Back-ground (20)		Communication with the CODESYS development environment
	Cyclic, event-controlled and freewheeling IEC task		15	Incl. standard priority of the visualization task

9.3 Memory Spaces under CODESYS V3

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

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

9.3.1 Program and Data Memory

The program memory (also code memory) has a maximum size of 32 MB.
The data memory has a maximum size of 128 MB.
Both areas are separate from each other and are requested when downloading to the system depending on the scope of the program. If the size limit is exceeded, it is displayed as an error.

9.3.2 Function Block Limitation

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

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

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

9.3.3 Remanent Memory

A total of 128 kbytes of remanent memory is available for the IEC-61131 application.
The remanent area is divided into the retain area and the persistence area. The areas are automatically distributed by CODESYS V3.

9.3.4 File Access from the IEC Application

Access to files via the IEC application is restricted to the following directories:

- /home/codesys
- /media/sd
- /tmp

9.3.5 Changing Network Settings from the IEC Application

To change network settings from an IEC application or via a fieldbus (e.g., PROFINET DCP), the “IP Source” parameter must be set to “external” (WBM “TCP/IP Configuration” page – “Bridge Interfaces” group).

The IEC application changes the network settings, for example, by enabling the “Adjust operating system settings” option in CODESYS (double-click the “ETHERNET (ETHERNET)” element in the device tree > “General” tab > “Adjust operating system settings” option).

9.3.6 EtherCAT

EtherCAT connection is possible via the CODESYS V3 functionality and the CODESYS V3 libraries.

To use the EtherCAT master function, the network interfaces must be switched from “switched” to “separated” (WBM “ETHERNET Configuration” page – “Bridge Configuration” group) and the controller or at least the runtime restarted so that the MAC addresses are assigned correctly.

To configure the EtherCAT master added to the project, the required AC adapter is selected in CODESYS (double-click the “EtherCAT_Master” element in the device tree > “General” tab > “Source address MAC” > **[Select]**).

10 Diagnostics

For diagnostic analysis, evaluate the indicator of the status LED on the front and read the error messages in the WBM under “Diagnostics”.
The possible indicators are explained as follows:

Table 28: LED Signaling

LED Display	Message
Green, steady	The product is ready to operate.
Red, flashing	There is an error. (The specific error message is displayed.)
Blue, flashing	There is a connection error to the controller. No communication

In the case of a connection error, check if:

- The controller is in operation.
- The network settings are correct.
- The controller URL is correct.

If the errors cannot be resolved, please contact WAGO Support.
support@wago.com
Disclose the color that is output.

Logbook

System messages, e.g., “Start of the controller” or “Communication interruptions”, are logged in the logbook.
In the tab “Diagnostic” in the WBM it is possible to read the logbook.

11 Service

11.1 Changing the Configuration with the WBM

The button “CFG/RST” is on top. The button calls up the Web-Based Management WBM to configure the device. The button must only be pressed using a pointed non-metallic object.
During the visualization run-time, the WBM is called up.
When starting up the device (Power ON), the autostart list is stopped and the device only starts the WBM. The button is not used to make any changes to the settings.

11.2 Firmware Changes

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

Obtain documentation appropriate for the firmware target version!
A firmware change 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.

Therefore, use only documentation appropriate for the target firmware after a firmware change.

If you have any questions, feel free to contact our WAGO Support.

You can update the firmware in two different ways using:

- WAGOupload
- Memory card and WBM

11.2.1 Use WAGOupload to Update/Downgrade the 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.

11.2.2 Perform Firmware Update/Downgrade

Proceed as follows if you want to update the controller to a later firmware version or to downgrade the controller to an earlier firmware version:

1. Copy the firmware image (*.img file) of the required firmware 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 new firmware image into the memory card slot. Use a special downgrade image if necessary (see above).
5. Switch on the controller.
6. After booting the controller, launch the WBM “Create Boot Image” page (you may have to temporarily change the IP address).
7. Create a new boot image on the internal memory.
8. Switch off the controller after completing the process.
9. Remove the memory card.
10. Switch on the controller.

The controller can now be started with the new firmware version.

12 Removal

12.1 Removal from the Rail

11. To remove, pull down the latch. Use a screwdriver or an operating tool for this.

2. Slide the product out at the lower edge of the rail.

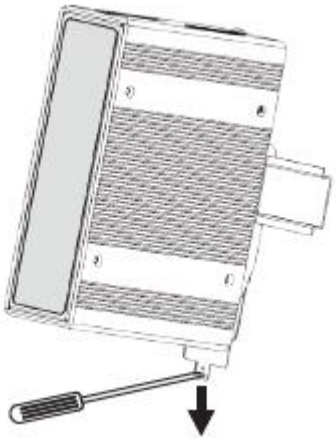

Figure 21: Removal from the Din-35 rail

13 Disposal

13.1 Electrical and electronic equipment

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

Electrical and electronic equipment contain materials and substances that can be harmful to the environment and health. Electrical and electronic equipment must be disposed of properly after use.
WEEE 2012/19/EU applies throughout Europe. Directives and laws may vary nationally.

Environmentally friendly disposal benefits health and protects the environment from harmful substances in electrical and electronic equipment.

- Observe national and local regulations for the disposal of electrical and electronic equipment.
- Clear any data stored on the electrical and electronic equipment.
- Remove any added battery or memory card in the electrical and electronic equipment.
- Have the electrical and electronic equipment sent to your local collection point.

Improper disposal of electrical and electronic equipment can be harmful to the environment and human health.

13.2 Packaging

Packaging contains materials that can be reused.
PPWD 94/62/EU and 2004/12/EU packaging guidelines apply throughout Europe. Directives and laws may vary nationally.

Environmentally friendly disposal of the packaging protects the environment and allows sustainable and efficient use of resources.

- Observe national and local regulations for the disposal of packaging.
- Dispose of packaging of all types that allows a high level of recovery, reuse and recycling.

Improper disposal of packaging can be harmful to the environment and wastes valuable resources.

14 Accessories

Several certified accessory items are available for the product.

Table 29: Accessories – Memory Cards

microSD memory card, 1 GB	758-879/000-002
microSD memory card, 2 GB	758-879/000-3102

Table 30: Accessories – Connecting Cable and connector

USB A-B connecting cable, 3 m	758-879/000-101
Connector for power supply	734-103
Fieldbus connector CANopen	750-963

15 Appendix

15.1 Configuration Dialogs

15.1.1 Web-Based-Management (WBM)

15.1.1.1 “Information” Tab

15.1.1.1.1 “Device Status” Page

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

“Device Details” Group

This group shows information about product identification.

Table 31: WBM “Device Status” Page – “Device Details” Group

Parameters	Explanation
Product Description	Product Designation
Order Number	Product Item Number
Serial	Unique Product Serial 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 32: WBM “Device Status” Page – “Network TCP/IP Details” Group

Parameter	Meaning	
Bridge <n>	Bridge currently configured; the properties are displayed in a separate area for each configured bridge.	
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 **Networking** > **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	

15.1.1.1.2 “Vendor Information” Page

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

15.1.1.1.3 “PLC Runtime Information” Page

All information about the enabled runtime system is provided on the “PLC Runtime Information” page. You will also find a link here to open WebVisu.

“Runtime” Group

Table 33: WBM “PLC Runtime Information” Page – “Runtime” Group

Parameter	Explanation
Version	The version of the enabled runtime system is shown. If the runtime system is disabled, “None” is displayed and the subsequent fields of this group are hidden.

“WebVisu” Group

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

15.1.1.1.4 “WAGO Software License Agreement” Page

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

15.1.1.1.5 “Open Source Licenses” Page

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

15.1.1.1.6 “WBM Third Party License Information” Page

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

15.1.1.1.7 “Trademarks Information” Page

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

15.1.1.1.8 “WBM Version” Page

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

15.1.1.2 “Configuration” Tab

15.1.1.2.1 “PLC Runtime Configuration” Page

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

“General PLC Runtime Configuration” Group

Table 34: WBM “PLC Runtime Configuration” Page – “General PLC Runtime Configuration” Group

Parameter	Meaning	
PLC runtime version	Select here the PLC runtime system to be enabled.	
	None	No runtime system is enabled.
	CODESYS V3	CODESYS V3 runtime system is enabled.
Home directory on memory card enabled	Define if the home directory for the runtime system should be moved to the memory card.	
	Disabled	The home directory is stored in the internal memory.
	Enabled	The home directory is moved to the memory card.

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

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

Click **[Submit]** to apply the change. 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!

“Webserver Configuration” Group

Table 35: WBM “PLC Runtime Configuration” Page – “Webserver Configuration” Group

Parameter	Meaning	
CODESYS V3 Webserver State	This displays the status (enabled/disabled) of the CODESYS V3 Webserver.	
Default Webserver	Choose here whether the Web-based Management or web visualization of the runtime system should be displayed when only entering the IP address of the controller.	
	Web-Based Management	The Web-based Management is displayed.
	WebVisu	The web visualization of the runtime system is displayed.

Click **[Submit]** to apply the change. The change takes effect immediately.

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

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

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

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

Note

Possible error messages when calling up the web visualization
The “500 − Internal Server Error” message indicates that the Webserver is not enabled.
A page with the header “WebVisu not available” means that no application has been loaded in the product using web visualization.

15.1.1.2.2 “TCP/IP Configuration” Page

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

“TCP/IP Configuration” Group

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

Table 36: WBM “TCP/IP Configuration” Page – “TCP/IP Configuration” Group

Parameter	Meaning	
Network Details Bridge <n>	Settings for the bridge currently configured	
Current IP Address	This displays the current IP address.	
Current Subnet Mask	This displays current subnet mask.	
Current Default Gateway	The IP address of the current default gateway is displayed.	
IP Source	You can specify whether to use a static or dynamic IP address.	
	Static IP	Static IP addressing
	DHCP	Dynamic IP addressing via DHCP
	BootP	Dynamic IP addressing via BootP
	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	Enter a static IP address. This is enabled if “Static IP” is enabled in the **IP Source** field.	
Subnet Mask	Enter the subnet mask. This is enabled if “Static IP” is enabled in the **IP Source** field.	
Default Gateway	Enter the IP address of the default gateway here.	

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“DNS Server” Group

Table 37: WBM “TCP/IP Configuration” Page – “DNS Server” Group

Parameters	Explanation
Active	The active DNS servers are displayed. Up to 3 active DNS servers can be used. The index reflects the query order. The first DNS server assigned via DHCP is given the highest priority.
Assigned by DHCP	The DNS servers assigned if necessary by DHCP (or BootP) are displayed. If no DNS server has been assigned by DHCP (or BootP), “No DNS Servers assigned by DHCP” is displayed.
Assigned by user	The addresses of the defined DNS servers are displayed. If no server has been entered, “No DNS Servers configured” is displayed.
New Server IP	Add additional DNS server addresses. You can enter a maximum of 3 addresses. The entries actually used result from an alternating combination of the “Assigned by DHCP” and ”Assigned by user” lists.

Click the **[Delete]** button to delete the selected DNS server. The change takes effect immediately.

Click the **[Add]** button to add the entered DNS server. The change takes effect immediately.

15.1.1.2.3 “Ethernet Configuration” Page

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

“Bridge Configuration” Group

Table 38: WBM “Ethernet Configuration” Page – “Bridge Configuration” Group

Parameter	Meaning
Bridge 1 … <n>	Assign the physical ports X1… X <n> to a logical bridge. To do so, click the respective option button. The assignment is marked in color. A port can only be assigned to one bridge at a time.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

“Switch Configuration” Group

This group only appears if parameter configuration is supported.

Table 39: WBM “Ethernet Configuration” Page – “Switch Configuration” Group

Parameters	Explanation	
Port Mirror	Enable or disable mirroring of the data traffic between the ports.	
	None	Both ETHERNET ports are operating normally.
	X1	The entire data traffic between X1 and the PFC system is mirrored at port X2.
	X2	The entire data traffic between X2 and the PFC system is mirrored at port X1.
Broadcast Protection	You can set the broadcast limit for protection against overloads.	
	Disabled	No broadcast packet limit
	1 % … 5 %	Limits incoming broadcast packets to the selected percentage of the total possible data throughput (10/100 Mbit)
Rate Limit	You can set the basic limitation of the incoming data traffic.	
	Disabled	No limitation of the incoming data traffic
	64 kbps … 99 mbps	Limits the incoming data traffic to the entered value

Click **[Submit]** to apply the change. The change takes effect immediately.

"Dummy Interfaces" Group

Table 40: WBM "Ethernet Configuration" Page – "Dummy Interfaces" Group

Parameter	Explanation
Name	Name of the selected dummy interface
Add dummy interface	Create a new dummy interface.
Name	Enter the name of the new dummy interface.

To delete a selected entry, click the **[Delete]** button. The changes take effect immediately.

To create a new entry, click the **[Add]** button. The changes take effect immediately.

"VLAN Interfaces" Group

Table 41: WBM "Ethernet Configuration" Page – "VLAN Interfaces" Group

Parameter	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
Add	Create a new VLAN interface.
Name	Enter the name of the new VLAN interface.
VLAN ID	Enter the VLAN ID; Permissible values are 3 … 4094.
Link	Select assigned bridge.

To delete a selected entry, click the **[Delete]** button. The changes take effect immediately.

To create a new entry, click the **[Add]** button. The changes take effect immediately.

“Ethernet Interface Configuration” Group

Table 42: WBM “Ethernet Configuration” Page – “Ethernet Interface Configuration” Group

Parameter	Meaning
Interface X<n>	A separate area is displayed for each interface in the controller.
Enabled	You can enable or disable the interface.
MAC Learning	You can disable or enable “MAC Learning”.
Speed/Duplex	Select the transmission speed and the transmission method. The drop-down menu is generated depending on the device and interface. When “Autonegotiation” is selected, the connection modalities are negotiated automatically between the peer devices.

Click **[Submit]** to apply changes. The changes take effect immediately.

15.1.1.2.4 Configuration of Host and Domain Name" Page

The settings for the hostname and domain are displayed on the "Configuration of Host/Domain Name" page.

"Hostname" Group

Table 43: WBM "Configuration of Host and Domain Name" Page – "Hostname" Group

Parameter	Explanation
Currently used	If you have selected dynamic assignment of an IP address via DHCP, the name of the host currently being used is displayed.
Configured	Enter the product hostname here; it is then used if the network interface is changed to a static IP address or if no hostname is assigned per DHCP response.

Click the **[Submit]** button to apply a change.

Click the **[Clear]** button to reset the input field.

The change takes effect immediately.

If the controller has been assigned a host name via DHCP, it is given preference and the manually configured host name is not used.
To accept the manually configured host name, the configuration of the DHCP server may have to be reduced by assigning the host name.

"Domain Name" Group

Table 44: WBM "Configuration of Host and Domain Name" Page – "Domain Name" Group

Parameter	Explanation
Currently used	If you have selected dynamic assignment of an IP address via DHCP, the name of the domain currently being used is displayed.
Configured	Enter the product domain name here; it is then used if the network interface is changed to a static IP address or if no domain name is assigned per DHCP response.

Click the **[Submit]** button to apply a change.

Click the **[Clear]** button to reset the input field.

The change takes effect immediately.

If the controller has been assigned a domain name via DHCP, it is given preference and the manually configured domain name is not used.
To accept the manually configured domain name, the configuration of the DHCP server may have to be reduced by assigning the domain name.

15.1.1.2.5 “Routing” Page

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

“IP Forwarding through multiple interfaces” Group

Table 45: WBM “Routing” Page – “IP Forwarding through multiple interfaces” Group

Parameter	Explanation
Enabled	Specify whether forwarding of IP data packets is allowed between different network interfaces. If the box is not checked, the settings under “Static Routes” are used, without allowing IP data packets that arrive at the controller on one network interface to leave the controller on different network interface. If the box is checked, IP packets can be forwarded between the interfaces. Other settings may be necessary on this WBM page.

Click the **[Submit]** button to apply the change. The changes take 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 46: WBM “Routing” Page – “Custom Routes“ Group

Parameter	Explanation	
Enabled	Specify whether the selected route should be used.	
	Disabled	The route is not used.
	Enabled	The route is used.
Destination Address	Specify whether any network devices or only a specific network device or device pool should be accessible.	
	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	Enter the subnet mask of the device. If “default” is entered for Destination Address, the value “0.0.0.0” must be entered.	
Gateway Address	Enter the 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	Set the number used as the metric. 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 = 4294967295.	
Interface	Enter an interface via which the packets sent to the destination address are routed. Bridges (br0-br3) as well as modems (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.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

To add a new route, click the **[Add]** button. The change takes effect immediately.

Click the **[Delete]** button to delete an existing route. The change takes effect immediately.

“Dynamic Routes” 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 47: WBM “Routing” Page – “IP-Masquerading” Group

Parameters	Explanation	
Enabled	Specify whether IP masquerading should be used.	
	Disabled	IP masquerading is not used.
	Enabled	IP masquerading is used.
Interface	You can select the specified name of a network interface. Alternatively, selecting “other” allows you to specify any network interface name.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

Click the **[Add]** button to add a new entry. The change takes effect immediately.

Click the **[Delete]** button to delete an existing entry. The change takes effect immediately.

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 48: WBM “Routing” Page – “Port Forwarding” Group

Parameters	Explanation	
Enabled	Specify whether port forwarding should be used.	
	Disabled	Port forwarding is not used.
	Enabled	Port forwarding is used.
Interface	You can select the specified name of a network interface. Alternatively, selecting “other” allows you to specify any network interface name.	
Port	Enter the port here on which the product receives network data packets to be forwarded.	
Protocol	You can select the protocol to be used for the port forwarding. The options are TCP, UDP or both protocols.	
Destination Address	Specify the network address of the destination device. This address replaces the original destination address of the network data packet.	
Destination Port	Specify the port number of the destination device. This value replaces the original destination port of the network data packet.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

Click the **[Add]** button to add a new entry. The change takes effect immediately.

Click the **[Delete]** button to delete an existing entry. The change takes effect immediately.

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

15.1.1.2.1 “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 49: 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.
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 Bpdu Guard	Current “Bpdu 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	Hier wird der aktuelle „Root Guard“-Status angezeigt.	
	☐	Root-Guard ist nicht aktiv.
	☑	Root-Guard ist aktiv.
Current Path Cost	Current path costs	
Current Priority	Current priority	

Table 49: WBM “Spanning Tree Protocol” Page – “Status” Group

Parameters	Explanation	
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 50: 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.
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	
Port X[n]	Each port X[n] has its own area. The port settings are only available after STP/RSTP has been successfully enabled.	

Table 50: WBM “Spanning Tree Protocol” Page – “Parameter Settings” Group

Parameters	Explanation	
Bpdu Filter	Enable/disable Bpdu filter.	
	☐	Bpdu filter is disabled.
	☑	Bpdu filter is enabled.
Bpdu 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.
Path Cost	Set Path Cost; Permissible Values: 0 ... 65535	
Priority	Set priority; Permissible values: 0 ... 15, Default = 8	

Click the **[Submit]** button to apply a change. The change takes effect immediately.

15.1.1.2.2 “Clock Settings” Page

The date and time settings are displayed on the “Clock Settings” page.

“Timezone and Format” Group

Table 51: WBM “Clock Settings” Page – “Timezone and Format” Group

Parameter	Explanation	
Timezone	Select the appropriate time zone for your location. 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	For time zones that cannot be selected with the “Time Zone” parameter, enter the name of the time zone or the country or city applicable to you. You can determine a valid name for the time zone here: http://www.timeanddate.com/time/map/	
Time Format	For switching between 12-hour and 24-hour time display	

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“UTC Time and Date” Group

Table 52: WBM “Clock Settings” Page – “UTC Time and Date” Group

Parameter	Explanation
UTC Date	Set the date.
UTC Time	Set GMT time.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“Local Time and Date” Group

Table 53: WBM “Clock Settings” Page – “Local Time and Date” Group

Parameter	Explanation
Local Date	Set the date.
Local Time	Set the local time.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

15.1.1.2.3 “Configuration of Serial Interface” Page

The settings for the serial interface are shown on the “Configuration of Serial Interface” page.

“Current Serial Interface Configuration” Group

Here, the application to which the serial interface is currently assigned and the interface mode are displayed.

Table 54: WBM “Configuration of Serial Interface” Page – “Current Serial Interface Configuration” Group

Parameters	Explanation	
Assigned to	Here, the application to which the serial interface is currently assigned is displayed.	
	Unassigned (usage by Applications, Libraries, PLC Runtime)	The serial interface is not assigned to any application and is available, so that the CODESYS program, for example, can access it via function blocks.
	Linux Console	The serial interface is assigned to the Linux console.
Mode	Here, the interface mode of the serial interface is displayed.	
	RS232	The serial interface is operated in the “RS-232” mode.
	RS485	The serial interface is operated in the “RS-485” mode.

NOTICE

Material damage due to a change of owner or mode!
Switching may damage connected RS-232/RS-485 devices.
Remove the devices before switching!

“Assign Owner of Serial Interface” Group

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

Table 55: WBM “Configuration of Serial Interface” Page – “Assign Owner of Serial Interface” Group

Parameters	Explanation
Linux® Console	Specify that the serial interface is assigned to the Linux® console.
Unassigned (usage by applications, libraries, CODESYS)	Specify that the serial interface is not to be assigned to any application and is available, so that the CODESYS program, for example, can access it via function blocks.

Click **[Submit]** to apply the change. The change only takes effect once the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

"Assign Mode of Serial Interface" Group

You can select the mode in which the serial interface is operated after the next controller reboot. The mode can only be changed if the serial interface is set to "Unassigned".

Table 56: WBM “Configuration of Serial Interface” Page – “Assign Owner of Serial Interface” Group

Parameter	Explanation
RS-232	Here, specify that the serial interface is to be operated in the "RS-232" mode.
RS-485	Here, specify that the serial interface is to be operated in the "RS-485" mode.

Click **[Submit]** to apply the change. The change only takes effect once the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

15.1.1.2.4 “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 57: WBM “Configuration of Service Interface” Page – “Assign Owner of Service Interface” Group

Parameters	Explanation
WAGO Service Communication	Specify that the service interface is used for the WAGO Service communication or runtime system communication.
Linux Console	Specify that the service interface is assigned to the Linux® console.
Unassigned (usage by applications, libraries, CODESYS)	Specify that the service interface is not to be assigned to any application and is available, so that the CODESYS program, for example, can access it via function blocks.

Click **[Submit]** to apply the change. The change only takes effect once the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

15.1.1.2.5 “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 58: WBM “Create Bootable Image” Page – “Create bootable image from active partition” Group

Parameters	Meaning		
Boot Device	The medium from which the boot was made is displayed.		
Destination	Depending on which medium has been booted, the following destination is available for selection after boot-up for the image to be generated:		
	System was booted from		Target partition for “bootable image”
	Memory Card	→	Internal Flash
	Internal memory	→	Memory Card

- Free space on target device:
  If the available memory space is less than 5% a warning is displayed. You can still start the copy process 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 copying procedure despite this warning.

Click **[Start Copy]** to start the copying procedure. 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.

15.1.1.2.6 “Firmware Backup” Page

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

“Firmware Backup” Group

Table 59: WBM “Firmware Backup” Page – “Firmware Backup” Group

Parameter	Explanation	
Boot Device	The storage medium from which the device was booted is displayed here.	
Destination	Select the storage location for the backup here.	
	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.
	Network	The data is saved in the file system and then made available as a download on the PC.
PLC runtime project	If you want to save the PLC runtime project (boot project, CODESYS settings), select this checkbox.	
Settings	If you want to save the device settings, select this checkbox.	
System	If you want to back up the operating system of the device and the root file system, select this checkbox.	
Encryption	If you want to save the data in encrypted form, select this button.	
Encryption passphrase	Enter the encryption password here. This input field only appears if the “Encryption” checkbox is selected.	
Confirm passphrase	Enter the encryption password again here to check it. This input field only appears if the “Encryption” checkbox is selected.	

Note

Note the firmware version!
Restoring the controller operating system (“System” selection) is only permissible and possible if the firmware versions at the backup and restore times are identical.
If necessary, skip restoring the controller operating system, or match the firmware version of the controller to the firmware version of the backup time 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 process.

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 procedure to help shorten the time required.

Click the **[Create Backup]** button to start the backup operation.

15.1.1.2.7 “Firmware Restore” Page

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

“Firmware Restore” Group

Table 60: WBM “Firmware Restore” Page – “Firmware Restore” Group

Parameter	Explanation	
Source	Select the data source for the restore here.	
	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.
	Network	The data is uploaded from the PC and restored.
Boot Device	The storage medium from which the device was booted is displayed here.	
PLC runtime project	Enter the name of the backup file for the CODESYS project here. The input field only appears if the network is selected as the data source.	
Settings	Enter the name of the backup file for the settings here. The input field only appears if the network is selected as the data source.	
System	Enter the name of the backup file for the system data and the root file system here. The input field only appears if the network is selected as the data source.	
Decryption	If you have backed up the data in encrypted form, select this checkbox.	
Decryption passphrase	Enter the encryption password here. This input field only appears if the “Decryption” checkbox is selected.	

Note

Note the firmware version!

Restoring the controller operating system (“System” selection) is only permissible and possible if the firmware versions at the backup and restore times are identical.

If necessary, skip restoring the controller operating system, or match the firmware version of the controller to the firmware version of the backup time 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 device 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 device. You must call the WBM again by entering the correct IP address of the device in the address line.

Note

Note the restore time!
The restore process takes approx. 2 … 3 minutes.
After the restore process, the controller is restarted and is then ready for use again.

Click the **[Restore]** button to start the restore operation.

15.1.1.2.8 “Active System” Page

The settings for specifying the partition from which the system is started are shown on the “Active System” page.

“Boot Device” Group

Table 61: WBM “Active System” Page – “Boot Device” Group

Parameter	Explanation
Boot Device	The storage medium from which the device was booted is displayed here.

“System <n> (Internal Flash)” Groups

Table 62: WBM “Active System” Page – “System <n> (Internal Flash)” Group

Parameter	Explanation	
Active	This shows whether the system is active.	
Configured	This shows whether the system should be active after the next reboot.	
State	The system status is displayed here.	
	good	The system is valid and can be used.
	bad	The system is not valid and cannot be used.

Click the respective **[Activate]** button to start the required system at the next reboot.

Note

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

15.1.1.2.9 “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 active partition, the text “Active Partition”.

“Devices” Group

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

Table 63: WBM “Mass Storage” Page – “Devices” Group

Parameter	Explanation
<Device>	The storage medium is displayed.
Boot device	This shows whether the device has booted from this storage medium.
Volume name	The name of the storage medium is displayed.

“Create new Filesystem on Memory Card” Group

Table 64: WBM “Mass Storage” Page – “Create new Filesystem on Memory Card” Group

Parameter	Meaning	
Filesystem type	You can select the format in which the filesystem should be created 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	Specify the name for the storage medium when formatted.	

Note

Data is deleted!
Any data stored in the storage medium is deleted during formatting!

To format the specified storage medium, click **[Start]**.

15.1.1.2.10 “Software Uploads” Page

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

Note

Install IPK files from trusted sources only!
IPK files are installed with extended rights (root rights), as long as not stated otherwise in the metadata.
Be careful when installing IPK files and install them from trusted sources only.

Table 65: WBM “Software Uploads” Page – “Upload New Software” Group

Parameters	Explanation
Software file	The file name of your selected software package is displayed, as long as you have not yet transferred it to the product. If you have not yet selected a package, “Choose ipk file...” appears. Click the input field and select a file with a software package on your PC.

To install the package, click **[Install]**.

The file with the software package is deleted from the device again after the installation process. If this is not possible due to a processing error, it is deleted no later than the next time the product restarts.

15.1.1.2.11 “Configuration of Network Services” Page

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

Note

Close any ports and services that you do not need!
Unauthorized persons may gain access to your automation system through open ports.
To reduce the risk of cyber attacks and thus increase cyber security, close all ports and services not required by your application in the control components (e.g., port 6626 for WAGO-I/O-*CHECK* and port 11740 for CODESYS V3).
Only open ports and services during commissioning and/or configuration.

“FTP” Group

Table 66: WBM “Configuration of Network Services” Page – “FTP” Group

Parameter	Explanation
Service active	Enable/disable the FTP service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“FTPES (explicit FTPS)” Group

Table 67: WBM “Configuration of Network Services” Page – “FTPES (explicit FTPS)” Group

Parameter	Explanation
Service active	Enable/disable the FTPS service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

“HTTP” Group

Table 68: WBM “Configuration of Network Services” Page – “HTTP” Group

Parameter	Explanation
Service active	Enable/disable the HTTP service. This service is disabled by default.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

Note

Disconnection abort on disabling
If the HTTP service is disabled, the connection to the product may be interrupted. In that case, reopen the page.

“HTTPS” Group

Table 69: WBM “Configuration of Network Services” Page – “HTTPS” Group

Parameter	Explanation
Service active	State of HTTPS service is displayed here.

“I/O-*CHECK*” Group

This group appears if the controller supports WAGO-I/O-*CHECK*.

Table 70: WBM “Configuration of Network Services” Page – “I/O-*CHECK*” Group

Parameter	Explanation
Service active	Enable/disable the WAGO-I/O-*CHECK*-Service.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

15.1.1.2.12 “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 71: WBM “Configuration of NTP Client” Page – “NTP Client Configuration” Group

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

To update the time regardless of interval, click the **[Update Time]** button.

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

15.1.1.2.13 “PLC Runtime Services” Page

The settings for various services of the runtime systems are displayed on the “PLC Runtime Services” page.

“CODESYS V3” Group

This group only appears if the controller supports the CODESYS V3 runtime system.

Table 72: WBM “PLC Runtime Services” Page – “CODESYS V3” Group

Parameter	Explanation
CODESYS V3 State	This displays the status (enabled/disabled) of the CODESYS V3 runtime system.
Webserver enabled	Enable or disable the Webserver for the CODESYS V3 web visualization.
Seperated WebVisu ports (8080/8081)	Enter here whether the CODESYS V3 web visualization is provided on ports 8080/8081. By default the web visualization is provided on WBM ports 80/443.
Port authentication enabled	Enter here whether a login is required for connecting to the device. The user name is admin and the password specified at “General Configuration.”

Click the **[Submit]** button to apply the change.
The change in authentication takes effect after the next restart.
All other changes take effect immediately.

15.1.1.2.14 “SSH Server Settings” Page

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

“SSH Server” Group

Table 73: WBM “SSH Server Settings” Page – “SSH Server” Group

Parameters	Explanation
Service active	You can enable/disable the SSH server.
Port Number	Enter the port number.
Allow root login	You can enable or inhibit root access.
Allow password login	Enable or disable the password query function.

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

15.1.1.2.15 “DHCP Server Configuration” Page

The “DHCP Server Configuration” page displays the DHCP service settings.

“DHCP Server Configuration Bridge <n>” Group

Table 74: WBM “DHCP Server Configuration” Page – “DHCP Configuration Bridge <n>” Group

Parameter	Explanation
Service active	Enable or disable the DHCP service for the interface X<n>.
Start IP for Range	Enter the start value of the available IP address range.
End IP for Range	Enter the end value of the available IP address range.
Lease time (min)	Specify the lease time here in seconds. 120 minutes are entered by default.
Static Hosts	This displays the static assignments of MAC IDs to IP addresses. If no assignment was defined, “No static hosts configured” is displayed.
Add Static Host	You can add static MAC addresses or host names and IP addresses.
MAC Address or Hostname	Enter a new static assignment, e.g., “01:02:03:04:05:06=192.168.1.20” or “hostname=192.168.1.20”. You can enter 15 assignments or host names.
Ip Address	Enter the IP address. You can enter 15 IP addresses.

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

To accept a new assignment click the **[Add]** button. The change takes effect immediately.

Click **[Delete]** to delete an existing assignment. The change takes effect immediately.

15.1.1.2.16 “Configuration of DNS Server” Page

The “Configuration of DNS Server” page displays the DNS service settings.

“DNS Server” Group

Table 75: WBM “Configuration of DNS Server” Page – “DNS Server” Group

Parameter	Explanation	
Service active	You can enable/disable the DNS server service.	
Mode	Select the operating mode of the DNS server.	
	Proxy	Requests are buffered to optimize throughput.
	Relay	All requests are routed directly.
Static Hosts	This displays the names for IP addresses. If no assignment was defined, “No static hosts configured” is displayed.	
Add Static Host	You can add static IP addresses and host names below.	
IP Address	Enter a new static assignment, e.g., “192.168.1.20:hostname”. You can enter 10 assignments.	
Hostname	Enter a host name.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

To accept a new assignment click the **[Add]** button. The change takes effect immediately.

Click **[Delete]** to delete an existing assignment. The change takes effect immediately.

15.1.1.2.17 “Status overview” Page

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

“Connection <n>” Group

A group is displayed for each cloud access.

Table 76: WBM “Status Overview” Page – “Connection <n>” Group

Parameter	Explanation
Is Active	The status of the cloud connectivity application is displayed.
Data from PLC Runtime	This shows how many data collections have been registered on the IEC application side for transfer to the cloud.
Cloud Connection	The status of the connection to the cloud service is shown.
Heartbeat	This shows the current heartbeat interval setting in seconds.
Telemetry Data Transmission	This indicates whether transfer of data is enabled or disabled.
Cache fill level (QoS 1 and 2)	This shows the fill level of the memory cache for outgoing messages as a percentage.

“Diagnosis” Group

This group is visible only when diagnostic information is available.

Warnings and errors are displayed here, along with information (when available) on how to potentially eliminate the error(s).

15.1.1.2.18 “Configuration of Connection <n>” Page

You can find settings and information for cloud access on the “Configuration of Connection <n>” 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 77: WBM “Configuration of Connection <n>” Page – “Configuration” Group

Parameter	Explanation
Enabled	You can enable/disable the cloud connectivity function.
Cloud platform	Select the cloud platform.
Hostname	Enter the host name or IP address for the selected cloud platform.
ID Scope	Enter the end point for the Azure Device Provisioning Service (DPS).
Registration ID	Enter the Registration ID for the Azure Device Provisioning Service (DPS).
Port number	Enter the port here to which a connection is to be established. Typical values are 8883 for encrypted connections and 1883 for unencrypted connections.
Device ID	Enter the device ID for the selected cloud platform.
Client ID	Enter the client ID for the selected cloud platform.
Authentication	Select the authentication method. Possible settings are “Shared Key Access” or “X.509 Certificate”.
Activation Key	Enter the activation key for the selected cloud platform.
Clean Session	Specify whether clean session should be enabled during the connection to the cloud service. If clean session is enabled, the information and messages on this connection are not stored persistently on the cloud service.
TLS	You can specify whether TLS encryption should be used for the connection to the cloud platform. Amazon Web Services (AWS) always uses TLS.

Table 77: WBM “Configuration of Connection <n>” Page – “Configuration” Group

Parameter	Explanation
CA file	Enter the path here to the file encoded in PEM format that contains the trusted CA certificate to use to establish an encrypted connection. The default value is the CA certificate /etc/ssl/certs/ca-certificates.crt that is already installed on the controller.
Users	Enter the user name for cloud service authentication.
Password	Enter the password for cloud service authentication.
Certification file	Enter the path here to the file encoded in PEM format that is used for cloud service authentication.
Key file	Enter the path to the file encoded in PEM format that contains the private key for cloud service authentication.
Use websockets	Here, you can specify whether the connection to the cloud platform is to be set up using the Websocket protocol via Port 443. If this checkbox is not selected, the connection to the cloud platform is set up using the MQTT protocol via Port 8883.
Proxy Type	Select which type of proxy should be used.
HTTP Proxy Host	Enter the host name or IP address of the proxy.
HTTP Proxy Port	Enter the port number of the proxy.
HTTP Proxy User	Enter the name of the proxy user.
HTTP Proxy Password	Enter the password for the proxy user.
Use compression	Here, you can set whether the data is to be compressed using GZIP compression.
Data Protocol	Here you can select the data protocol.
Cache mode	Specify in which memory the cache for the data telegrams should be created. This selection field is only enabled if a correctly formatted SD card is inserted (more information is available in Application Note A500920).
Last Will	You can specify whether a last will message should be enabled/disabled.
(Last Will) Topic	You can specify the topic under which the last will messages should be sent.
(Last Will) Message	You can enter the message you wish to use as the last will message.
(Last Will) QoS	You can specify the “Quality of Service” (QoS) of the last will message.
(Last Will) Retain	Here, you can set whether the previous last-will message sent under a topic from the broker is to be handled as a retained message.

Table 77: WBM “Configuration of Connection <n>” Page – “Configuration” Group

Parameter	Explanation
Device info	Specify whether a device info message should be generated that informs the cloud service of the basic configuration of the controller (more information is available in the Application Note A500920).
Device status	Specify whether device state messages should be generated that inform the cloud service about changes in the mode selector switch and the LEDs (more information is available in the Application Note A500920).
Standard commands	Specify whether the integrated standard commands should be supported (list of standard commands is available in the Application Note A500920). If the checkbox is disabled, only the commands defined in the IEC program are supported.
Application property template	You have the option of creating your own property for the individual MQTT messages to the Azure cloud. This parameter is optional; i.e., if the field is left blank, this property is not sent. The following placeholders are available to create this property: • <m>: Message type • <p>: Protocol version • <d>: Device ID Examples: • MyKey=HelloWorld_<m> • TestKey=<m>/<p>/<d> • DeviceId=<d>

Click the **[Submit]** button to apply a change.

The changes only take effect after the controller restarts. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

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

Table 78: Display of the Selection and Input Fields Depending on the Selected Cloud Platform

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	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

Table 78: Display of the Selection and Input Fields Depending on the Selected Cloud Platform

Selection or Input Field	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	Amazon Web Services	SAP IoT Services	Azure Device Provisioning Service (DPS)

X: Visible and enabled
(X): Visible, but disabled
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 disabled when “Last Will” is switched on
X4: Enabled if “Use websockets” is switched on.
X5: Visible and enabled if “Use websockets” is switched on and if “HTTP” is set as the “Proxy Type”.

Table 79: Choice of Data Protocol Depending on the Selected Cloud Platform

Data Protocol	Cloud Platform					
	WAGO Cloud	Azure	MQTT AnyCloud	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 80: Display of 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 81: Choice of 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 if “Compression” is not switched on
(X): Fixed setting

Table 82: Display of the Selection and Input Fields Depending on the Selected Authentication

Selection or Input Field	Authentication	
	Shared Access Key	**X.509 Certificate**
Activation Key	X	
Certification file		X
Key file		X

X: Visible and enabled

15.1.1.2.19 “Configuration of General SNMP Parameters” Page

The general settings for SNMP are given on the “Configuration of General SNMP Parameters” page.

“General SNMP Configuration” Group

Table 83: WBM “Configuration of General SNMP Parameters” Page – “General SNMP Configuration” Group

Parameter	Explanation
Service active	Activate/deactivate the SNMP service.
Name of Device	Enter here the device name (sysName).
Description	Enter here the device description (sysDescription).
Physical Location	Enter here the location of the device (sysLocation).
Contact	Enter here the email contact address (sysContact).
ObjectID	Enter here the object ID (sysOID).

Click the **[Submit]** button to apply the changes.

15.1.1.2.20 “Configuration of SNMP v1/v2c Parameters” Page

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

“Communities” Group

Table 84: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Communities” Group

Parameters	Explanation
Community <n>	Each configured community has its own area in the display. If no community has been configured, “(no Communities configured)” is displayed.
Name	The community name for the SNMP manager configuration is displayed. The community name can establish relationships between SNMP managers and agents who are respectively referred to as “Community” and who control identification and access between SNMP participants.
Access	This displays the access rights for the community. Possible values: “ReadOnly” or “ReadWrite”.
Add new Community	In this area, you can enter a new community.
Name	Specify the community name for the SNMP manager configuration. (See above) The community name can be up to 32 characters long and must not include spaces. To use the SNMP protocol, a valid community name must always be specified. The default community name is “public.”
Access	Specify the access rights for the new community. Possible values: “ReadOnly” or “ReadWrite”.

Click the corresponding **[Delete]** button to delete an existing community.

Click the **[Add]** button to add a new community.

“Trap Receivers” Group

Table 85: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Trap Receivers” Group

Parameters	Meaning
Trap Receiver <n>	Each configured trap receiver has its own area in the display. If no trap receiver has been configured, “(no Trap Receivers configured)” is displayed.
Host	The host name or the IP address for the trap receiver (management station) is displayed.
Community Name	This displays the community name for the trap receiver configuration. The community name can be evaluated by the trap receiver.
Version	This displays the SNMP version, via which the traps are sent.
Add new Trap Receiver	In this area, you can enter a new trap receiver.
Host	Specify the host name or the IP address for the new trap receiver (management station).
Community Name	Specify the community name for the new trap receiver configuration. (See above). The community name can be up to 32 characters long and must not include spaces.
Version	Specify the SNMP version that will send the traps. Possible values: “v1” or “v2c”.

Click the corresponding **[Delete]** button to delete an existing trap receiver.

Click the **[Add]** button to add a new trap receiver.

15.1.1.2.21 “Configuration of SNMP v3 Parameters” Page

The general settings for SNMP v3 are shown on the “Configuration of SNMP v3 Parameters” page.

“Users” Group

Table 86: WBM “Configuration of SNMP v3 Parameters” Page – “Users” Group

Parameters	Meaning
User <n>	Each configured v3 user has its own area in the display. If no v3 user has been configured, “(no Users configured)” is displayed.
Security Authentication Name	The user name is displayed.
Authentication Type	The authentication type for the SNMP v3 packets is displayed. Possible values: - Use no authentication (“None”) - Message Digest 5 (“MD5”) - Secure Hash Algorithm (“SHA”, “SHA224”, “SHA256”, “SHA384”, “SHA512”)
Authentication Key	The authentication key is displayed.
Privacy	The encryption algorithm for the SNMP message is displayed. Possible values: - No encryption (“None”) - Data Encryption Standard (“DES”) - Advanced Encryption Standard (“AES”, “AES128”, “AES192”, “AES192C”, “AES256”, “AES256C”)
Privacy Key	The key for encryption of the SNMP message is displayed. If nothing is displayed, the “authentication key” is automatically used.
Access	This displays the access rights for the user. Possible values: “ReadOnly” or “ReadWrite”.
Add new v3 User	In this area, you can enter a new v3 user. You can create up to 10 users.
Security Authentication Name	Enter the user name. This name must be unique; a pre-existing user name is not accepted when entered. The name must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Authentication Type	Specify the authentication type for the SNMP v3 packets. Possible values: - Use no authentication (“None”) - Message Digest 5 (“MD5”) - Secure Hash Algorithm (“SHA”, “SHA224”, “SHA256”, “SHA384”, “SHA512”)

Table 86: WBM “Configuration of SNMP v3 Parameters” Page – “Users” Group

Parameters	Meaning
Authentication Key	Specify the authentication key. The key must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Privacy	Specify the encryption algorithm for the SNMP message. Possible values: - No encryption (“None”) - Data Encryption Standard (“DES”) - Advanced Encryption Standard (“AES”, “AES128”, “AES192”, “AES192C”, “AES256”, “AES256C”)
Privacy Key	Enter the key for encryption of the SNMP message. If nothing is specified here, the “authentication key” is automatically used. The key must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Access	Specify the access rights for the new user. Possible values: “ReadOnly” or “ReadWrite”.

Click the respective **[Delete]** button to delete an existing user.

Click **[Add]** to add a new user.

“Trap Receivers” Group

Table 87: WBM “Configuration of SNMP v3 Parameters” Page – “Trap Receivers” Group

Parameters	Meaning
Trap Receiver <n>	Each configured v3 trap receiver has its own area in the display. If no v3 trap receiver has been configured, “(no Trap Receivers configured)” is displayed.
Security Authentication Name	The user name is displayed.
Authentication Type	The authentication type for the SNMP v3 packets is displayed. Possible values: - Use no authentication (“None”) - Message Digest 5 (“MD5”) - Secure Hash Algorithm (“SHA”, “SHA224”, “SHA256”, “SHA384”, “SHA512”)
Authentication Key	The authentication key is displayed.
Privacy	The encryption algorithm for the SNMP message is displayed. Possible values: - No encryption (“None”) - Data Encryption Standard (“DES”) - Advanced Encryption Standard (“AES”, “AES128”, “AES192”, “AES192C”, “AES256”, “AES256C”)
Privacy Key	The key for encryption of the SNMP message is displayed. If nothing is displayed, the “authentication key” is automatically used.
Host	The host name or the IP address of a trap receiver for v3 traps is displayed.
Add new Trap Receiver	In this area, you can enter a new v3 trap receiver. You can create up to 10 trap receivers.
Security Authentication Name	Enter the user name. This name must be unique; a pre-existing user name is not accepted when entered. The name must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Authentication Type	Specify the authentication type for the SNMP v3 packets. Possible values: - Use no authentication (“None”) - Message Digest 5 (“MD5”) - Secure Hash Algorithm (“SHA”, “SHA224”, “SHA256”, “SHA384”, “SHA512”)

Table 87: WBM “Configuration of SNMP v3 Parameters” Page – “Trap Receivers” Group

Parameters	Meaning
Authentication Key	Specify the authentication key. The key must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Privacy	Specify the encryption algorithm for the SNMP message. Possible values: - No encryption (“None”) - Data Encryption Standard (“DES”) - Advanced Encryption Standard (“AES”, “AES128”, “AES192”, “AES192C”, “AES256”, “AES256C”)
Privacy Key	Enter the key for encryption of the SNMP message. If nothing is specified here, the “authentication key” is automatically used. The key must be min. 8 and max. 32 characters long and contain lower case letters (a … z), upper case letters (A … Z), numbers (0 … 9), special characters !()*~'.-_ but no spaces.
Host	Specify the host name or the IP address for a trap receiver for v3 traps.

Click the respective **[Delete]** button to delete an existing trap receiver.

Click **[Add]** to add a new trap receiver.

15.1.1.2.22 “Favorites” Page

The “Favorites” page displays the product start page. This page also maintains a list of adjustable controllers for you.

For the start page, you can choose a specific controller from the available list that is displayed when the product is powered up.

If a website or controller has been selected as the start page, regardless of whether a boot project is available or not, the website or controller is displayed as the start page.

If the WBM or “Browser Favorites” has been activated as the start page and a boot project is available, the target visualization is displayed as the start page.

If the WBM or “Browser Favorites” has been activated as the start page and no boot project is available, the WBM or “Browser Favorites” are displayed as the start page.

Note

Start page cannot be set when target visualization has been started!
If a target visualization has been configured and started on the product, selecting a start page has no effect because the target visualization is started directly.

“WBM” Group

Here you enable/disable the WBM as the start page, which is displayed when the product is switched on.

Click the **[Submit]** button to apply a change.

“Browser Favorites” Group

Here you enable/disable the “Browser Favorites” selection list as the start page, which is displayed when the product is switched on.

Click the **[Submit]** button to apply a change.

“Favorite n” Groups

Each group describes the connection to a specific controller. If the name of a controller is changed, this name also becomes the new group label.

Here you enable/disable a favorite as the start page, which is displayed when the product is switched on.

Here you enable/disable the “MicroBrowser” for the specific controller.

Table 88: WBM “Favorites” Page – “Favorite n” Groups

Parameter	Meaning
Startpage	Enable/disable this favorite as the start page, which is displayed when the product is switched on.
Name	Enter any name for the controller.
URL	Enter the URL at which the controller’s Web visualization is reached.
Virtual Keyboard	Specify whether the virtual panel keyboard is to be used when displaying the URL of this controller. This is useful if, e.g., you want to display a WebVisu that requires its own virtual keyboard.
WebVisu	Specify whether the indicated URL is a WebVisu or not.
MircoBrowser	Enable/disable the “MicroBrowser” for the controller.

Click the **[Submit]** button to apply a change. To reset all input fields of the entry, click the **[Clear]** button. Click **[Submit]** to confirm the reset.

The activation/deactivation of the MicroBrowser only takes effect after restarting the product again. For this purpose, use the WBM reboot function. Do not switch off the product too early!

Note

CODESYS V3 application prevents web visualization in the MicroBrowser!
No CODESYS V3 application may be installed on the product to activate the MicroBrowser.

In the event of a faulty or interrupted connection from the browser to the controller, an orange rectangle with an exclamation mark is displayed in the MicroBrowser.

If the remote station (PLC) is not yet available when the product is started, a start screen is displayed.

The default login data applies to the MicroBrowser:

Table 89: MicroBrowser – Login Data

Users	Default password
admin	wago

15.1.1.2.23 “Autostart” Page

You can set the Autostart options for the Runtime on this page.

Group “Autostart Delay”

Set the countdown displayed when booting before displaying the start page. Within the time set, you have the option to prevent the panel from switching to the start page and to go to the WBM directly. A delay of “0” displays the start page immediately.

15.1.1.2.24 “Monitoring” Page

Make settings here for monitoring the product.

“Monitoring” Group

Table 90: WBM “Browser Settings > Monitoring” Page – “Monitoring” Group

Parameter	Explanation
Reconnect	Specify whether an attempt is made automatically to restore a connection if the connection to the product is interrupted.
Interval (s)	Specify an interval for the attempts.

15.1.1.2.25 “Browser Security” Page

Specify the browser security level.

“Browser Security” Group

Select the required security level (Low or High).

Table 91: WBM “Browser Settings > Browser Security” Page – “Browser Security” Group

Parameter	Explanation
Browser Security	• Low: At this security level, HTTPS connections are permitted with: •• Certificates that are not yet valid •• Certificates that have expired •• Certificates that are self-signed •• Certificates with host names that do not match • High: At this security level, the connections that are permitted at the “Low” low level and listed above are rejected.

15.1.1.2.1 “Commissioning Settings” Page

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

“Commissioning” Group

Table 92: 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.	

Click the **[Submit]** button to apply a change. The change takes effect immediately.

15.1.1.2.2 Page “Docker Settings”

On the page “Docker Settings”, see the settings for the "Docker®" service.

Group “Docker Status”

Table 93: WBM Page “Docker Settings” – group “Docker Status”

Parameter	Meaning	
Current State	The current status of the “Docker®” service is displayed.	
	stopped	The “Docker®” service is disabled.
	running	The “Docker®” service is enabled.
Service Enabled	If you want to enable the “Docker®” service, check this box.	

Click the **[Submit]** button to apply the changes. The changes take effect immediately.

15.1.1.2.3 “Fonts” Page

This page allows you to upload or delete fonts from a PC.

Click in the “Choose file ...” field. Select the required true-type font file (*.ttf).

Click the **[Upload]** button to upload the font. The uploaded font appears in the list above the “Choose file ...” field. The font is only available after restarting.

Click the **[Delete]** button to delete a font.

15.1.1.2.4 “Display Orientation” Page

You can make display orientation settings on the “Display > Display Orientation” page.

“Display Orientation” Group

Specify whether the display should appear in portrait or landscape mode. The options are landscape, portrait, landscape rotated and portrait rotated.

15.1.1.2.5 “Screensaver” Page

You can adjust the screensaver on the “Display > Screensaver” page.

“Screensaver Settings” Group

Specify whether and how a screensaver should be used.

Table 94: WBM “Screensaver” Page – “Screensaver Settings” Group

Parameter	Explanation
Enabled	You can enable or disable the screensaver here.
Setting	Specify whether an image, the time, a text or a backlight should be displayed or whether screen care should be performed. • Image: The screensaver with the WAGO logo is activated after a time set under “Duration.” • Text: Enter text here that is activated as the screensaver after the time set under “Duration” has elapsed. • Time: The current time is displayed as the screensaver. • Backlight: The brightness is reduced to the screensaver brightness and the WAGO logo displayed. • Screen care: For screen care, all pixels are inverted for a few milliseconds (not visible). • Off: No screensaver is displayed.
Text	Enter any text display as the text screensaver. (Can be adjusted in the “Text” option.)
Duration (s)	When the display is not in use, the screensaver is activated after the time set here has elapsed.

“Screen Care” Group

Set how long the display should be disabled for cleaning.

Table 95: WBM “Screensaver” Page – “Screen Care” Group

Parameter	Explanation
Enabled	You can enable or disable the screen care function here.
Time (hh:mm:ss)	Enter the time at which screen care should be performed. (Can be adjusted in the “Screen care” option.)

15.1.1.2.6 “WBM User Configuration” Page

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

“Change Password” Group

Note

Changing Passwords
The initial passwords as delivered are documented in this manual and therefore do not provide sufficient protection. Change the passwords to meet your particular needs!

Table 96: WBM “WBM User Configuration” Page – “Change Password” Group

Parameter	Explanation
Old Password	Enter the current password here for authentication.
New Password	Enter the new password here. Permitted characters for the password are the following ASCII characters: a … z, A … Z, 0 … 9, and special characters: !"#$%&'()*+,./:;<=>?@[]^_`{}|~-.
Confirm Password	Enter the new password again here for confirmation.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

Note

Note the permitted characters for WBM passwords!
If passwords with invalid characters are set for the WBM outside the WBM (e.g., from a USB keyboard), access to the pages directly on the display is no longer possible because only permitted characters are available from the virtual keyboard.

Note

General Rights of WBM Users
The WBM users “admin” and “user” have rights beyond the WBM to configure the system and install software.

User administration for controller applications is configured and managed separately.

15.1.1.3 “Fieldbus” Tab

15.1.1.3.1 “OPC UA Configuration” Page

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

“OPC UA Server Configuration” Group

Table 97: WBM “OPC UA Configuration” Page – “OPC UA Server Configuration” Group

Parameter	Explanation
Enabled	Enable or disable the WAGO OPC UA Server here.
Log level	Select the log level. The following values can be set: Info / Debug / Warning / Error. With log level “Error,” only error messages are read out; with log level “Info,” status messages are read out too. The specific log level selection affects server reaction time. Therefore, select the lowest level necessary; e.g., “Debug” for in-depth analyses.
Ctrl Configuration name	Enter the configuration names the controller contains in the PLC Open Device Set.

Click the **[Submit]** button to apply the changes.

“OPC UA Server Security Settings” Group

Table 98: WBM “OPC UA Configuration” Page – “OPC UA Server Security Settings” Group

Parameter	Explanation
Anonymous Access	Permit anonymous access to the server. This requires that runtime port authentication also be deactivated.
Allow Password On Plaintext	Transfer of password in readable format
Security Modes	Security Mode of the OPC UA Server Depending on the operating mode you select, different OPC UA endpoints for setting up the connection are available: None: Only the OPC UA endpoint **None** is activated. This allows an unsecured connection to the OPC UA server to be established. None + Sign + SignAndEncrypt: The enpoints **None, Sign and SignAndEncrypt** are available. **Sign** provides an endpoint that is password protected. **SignAndEncrypt** specifies an endpoint that povides both a password and encryption. Sign + SignAndEncrypt: The **Sign** and **SignAndEncrypt** endpoints are available. SignAndEncrypt: Only the **SignAndEncrypt** enpoint is available.
Security Policies	Selection of security policies Here, you can set the encryption level for the OPC UA server. The following options are available for this: Aes128Sha256RsaOaep and better, Basic256Sha256 and better, Aes256Sha256RsaPss.

Click the **[Submit]** button to apply the changes.

15.1.1.3.1 “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 99: 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 100: 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 101: WBM “BACnet Status” Page – “BACnet Data Link” Group

Parameters	Explanation
Connection Info	Display of the connection status

15.1.1.3.2 “BACnet Configuration” Page

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

“Restart” Group

Table 102: WBM “BACnet Data Link” Page – “BACnet Restart” Group

Parameters	Explanation
[Restart]	Restart the BACnet service

“BACnet Service” Group

Table 103: WBM “BACnet Configuration” Page – “BACnet Service” Group

Parameters	Explanation	
Service active	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.

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

“BACnet Data” Group

Table 104: 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.

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

“BACnet Log Level” Group

Table 105: WBM “BACnet Configuration” Page – “BACnet Log Level” Group

Parameters	Explanation
Error	Enable/disable error log outputs.
Warning	Enable/disable warning log outputs.
Info	Enable/disable info log output.
Debug	Enable/disable debug log output.

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

“BACnet Network Capture” Group

Table 106: WBM “BACnet Configuration” Page – “BACnet Network Capture” Group

Parameters	Explanation
Enable	Enable/disable logging of network traffic with the corresponding BACnet filters.
Log pre-master secrets	Enable/disable saving of secrets for decryption of BACnet/SC network traffic.
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.

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

15.1.1.3.3 “BACnet Data Link” Page

“BACnet Restart” Group

Table 107: WBM “BACnet Data Link” Page – “BACnet Restart” Group

Parameters	Explanation
[Restart]	Restart the BACnet service.

“BACnet/IP” Group

Table 108: WBM “BACnet Data Link” Page – “BACnet/IP” Group

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

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

“BACnet/SC” Group

Table 109: WBM “BACnet Data Link” Page – “BACnet/SC” Group

Parameters	Explanation	
Mode	Selection of the BACnet/SC operating mode	
	Node	The device is operated as a BACnet/SC node.
	Primary Hub	The device is operated as a BACnet/SC Primary HUB.
	Failover Hub	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.	
Accept any certificates	Enable/disable whether communication can be established via any certificates.	

Click the **[Submit]** button to apply a change. The change is only applied after the controller is restarted or after a BACnet restart.

“BACnet/SC Certificate Authority (CA)” Group

Table 110: 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 111: 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 112: WBM “BACnet Configuration” Page – “BACnet/SC Certificate Signing Request (CSR)” Group

Parameters	Explanation
[Generate]	Generate a CSR and a new private key on the device.
[Download]	Download CSR from device.

“BACnet/SC Default Certificates” Group

Table 113: WBM “BACnet Data Link” Page – “BACnet/SC Default Certificates” Group

Parameters	Explanation
[Generate]	Generation of a new certificate

15.1.1.3.4 “BACnet Storage Location” Page

You can specify settings for saving of BACnet-specific parameters on this page.

Changes are applied without having to restart.

“BACnet Persistence” Group

This group lets you select the storage location (SD card/internal flash) for the persistence data.

If the persistence settings are changed, a pop-up window warns that data loss may occur until the next persistence is completed.

Table 114: WBM Page “BACnet Storage Location” – “BACnet Persistence” Group

Parameter	Meaning	
Storage location	You can select the storage location for the persistence data. Selection is possible only when both storage options are available.	
	Internal-Flash	Data will be stored in the controller's internal memory.
	SD-Card	Data will be stored on the SD card. If “SD card” has been selected and the card is no longer inserted, this option is no longer enabled and only the “internal flash” option can be selected.

“BACnet Trendlog” Group

This group lets you select the storage location (SD card/internal flash) for the trend log data.

Table 115: WBM Page “BACnet Storage Location” – “BACnet Trendlog” Group

Parameter	Meaning	
Storage location	You can select the storage location for the trend log data. Selection is possible only when both storage options are available.	
	Internal-Flash	Data will be stored in the controller's internal memory.
	SD-Card	Data will be stored on the SD card. If “SD card” has been selected and the card is no longer inserted, this option is no longer enabled and only the “internal flash” option can be selected.

“BACnet Eventlog” Group

This group lets you select the storage location (SD card/internal flash) for the event log data.

Table 116: WBM Page “BACnet Storage Location” – “BACnet Eventlog” Group

Parameter	Meaning	
Storage location	Select the storage location for the event log data here. Selection is possible only when both storage options are available.	
	Internal-Flash	Data will be stored in the controller's internal memory.
	SD-Card	Data will be stored on the SD card. If “SD card” has been selected and the card is no longer inserted, this option is no longer enabled and only the “internal flash” option can be selected.

15.1.1.4 “Security” Tab

15.1.1.4.1 “OpenVPN / IPsec Configuration” Page

The “OpenVPN / IPsec Configuration” page displays the settings for OpenVPN and IPsec.

“OpenVPN” Group

Table 117: WBM “OpenVPN / IPsec Configuration” Page – “OpenVPN” Group

Parameter	Explanation	
Current State	The current status of the OpenVPN service is displayed.	
	stopped	The service is disabled.
	running	The service is enabled.
OpenVPN enabled	Enable or disable the OpenVPN service.	
openvpn.config	Select an OpenVPN configuration file to be transferred from PC to product or vice versa.	

Click the **[Submit]** button to apply a change.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file from the PC to the product, click **[Upload]** button.

To transfer a file from product to PC, click the **[Download]** button.

The changes only take effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

“IPsec” Group

Table 118: WBM “OpenVPN / IPsec Configuration” Page – “IPsec” Group

Parameter	Explanation	
Current State	The current status of the IPsec service is displayed.	
	stopped	The service is disabled.
	running	The service is enabled.
IPsec enabled	Enable or disable the IPsec service.	
ipsec.conf	Select an IPsec configuration file to be transferred from PC to product or vice versa.	
ipsec.secrets	Select an IPsec configuration file to be transferred from PC to product or vice versa.	

Click the **[Submit]** button to apply a change.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file from the PC to the product, click **[Upload]** button.

To transfer a file from product to PC, click the **[Download]** button.

The changes only take effect after the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

15.1.1.4.2 “General Firewall Configuration” Page

The “General Firewall Configuration” page displays the global firewall settings.

“Global Firewall Parameter” Group

Table 119: WBM “General Firewall Configuration” Page – “Global Firewall Parameter” Group

Parameter	Explanation
Firewall enabled entirely	Enables/disables the complete functionality of the firewall. This setting has the highest priority. If the firewall is disabled, all other settings have no direct effect. The configuration of the other parameters is possible nevertheless so that you can set the firewall parameters correctly before you enable the firewall. 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 or disable the “ICMP echo broadcast” protection.
Max. UDP datagrams per second	Specify the maximum number of datagrams per second with the same source ports and the same destination ports between hosts.
Max. TCP connections per second	You can specify the maximum number of TCP connections per second.

Click **[Submit]** to apply the change. The change takes effect immediately.

15.1.1.4.3 “Interface Configuration” Page

The individual interfaces for the firewall settings are displayed on the “Interface Configuration” page.

“Firewall Configuration Bridge <n> / VPN / WAN” 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 120: WBM “Interface Configuration” Page – “Firewall Configuration Bridge <n> / VPN / WAN” Group

Parameter	Explanation
Firewall enabled for Interface	Enable or disable the firewall for the respective bridge.
ICMP echo protection	Enable or disable the “ICMP echo” protection for the respective bridge. If you enable ICMP echo protection, all ICMP echo requests (pings) will be rejected and the ICMP echo limit per second and ICMP burst limit entries will be ineffective.
ICMP echo limit per second	You can specify the maximum number of “ICMP pings” per second. Input is only effective when ICMP echo protection is disabled. “0” = “Disabled”
ICMP burst limit (0 = disabled)	You can specify the maximum number of “ICMP echo bursts” per second. Input is only effective when ICMP echo protection is disabled. “0” = “Disabled”
Service Configuration	Enable or disable the firewall for the respective service.
FTP/FTPES	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)	
DNP3 (port 20000)	
IEC60870-5-104 (port 2404)	
IEC61850 (port 102)	

Click the **[Submit]** button to apply the change. The change takes effect immediately.

15.1.1.4.4 “Configuration of MAC Address Filter” Page

The “Configuration of MAC address filter” page displays the firewall configuration on the ETHERNET level.

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 devices 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 device via the ETHERNET. This also applies to other services that are used by your device, e.g., the IP configuration via DHCP.
If the “MAC Address Filter Whitelist” does not contain the MAC address of your DHCP server, your device will lose its IP settings after the next refresh cycle and is then no longer accessible.
If the “MAC Address Filter Whitelist” does not contain an entry, the activation of the filter is prevented.
If at least one enabled address is entered, you will receive an appropriate warning before activation, which you have to acknowledge.
The check described above is only performed in the WBM but not in the CBM!

“Global MAC address filter state” Group

Table 121: WBM “Configuration of MAC Address Filter” Page – “Global MAC address filter state” Group

Parameters	Explanation
Filter enabled	Enable or disable the global MAC address filter.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

“MAC address filter state Bridge <n>” Group

A separate group is displayed for each configured bridge.

Table 122: WBM “Configuration of MAC Address Filter” Page – “MAC address filter state Bridge <n>” Group

Parameter	Explanation
Filter enabled	Enable or disable here the MAC address filter for the specific bridge. This setting is independent of the “Firewall enabled entirely” setting on the General Firewall Configuration page.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

“MAC address filter whitelist” Group

Each list entry has its own area in the display.

Table 123: 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 activating the filter when the firewall is generally enabled. The description is only visible for entries initially available in the factory default settings.
MAC address	Displays the MAC address of the relevant list entry.
MAC mask	This displays the MAC mask of the relevant list entry.
Filter enabled	Enable or disable the filter for the relevant list entry.
Add filter to whitelist	Create a new list entry.
MAC address	Enter here the MAC address for a new list entry. You can enter 10 filters.
MAC mask	Enter the MAC mask for the new list entry.
Filter enabled	Enable or disable the filter for the new list entry.

Click the **[Submit]** button to apply the change. The change takes effect immediately.

Click the appropriate **[Delete]** button to remove an existing list entry. The change takes effect immediately.

Click **[Add]** to accept a new list entry. You can enter 10 filters. The change takes effect immediately.

15.1.1.4.5 “Configuration of User Filter” Page

The “Configuration of User Filter” page displays the settings for custom firewall filters.

“User filter” Group

Each configured filter has its own area in the display.

Table 124: WBM “Configuration of User Filter” Page – “User Filter” Group

Parameters	Meaning	
Policy	This displays whether the network participant is permitted or excluded by the filter.	
Source IP address	The source IP address for the respective filter is displayed.	
Source Netmask	This displays the source netmask for the respective filter.	
Source Port	The source port number for the respective filter is displayed.	
Destination IP address	The destination IP address for the respective filter is displayed.	
Destination Netmask	The destination netmask for the respective filter is displayed.	
Destination Port	The destination port number for the respective filter is displayed.	
Protocol	The permitted protocols for the respective filter is displayed.	
Input interface	The permitted interfaces for the respective filter are displayed.	
Add new user filter	You can create up to 10 filters. You only have 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.	
Policy	Select here whether the network devices is to be allowed or excluded by the filter.	
	Allow	The network device is permitted.
	Drop	The network device is excluded.
Source IP address	Enter here the source IP address for the new filter.	
Source netmask	Enter here the source network mask for the new filter.	
Source port	Enter here the source port address for the new filter.	
Destination IP address	Enter here the destination IP address for the new filter.	
Destination subnet mask	Enter here the destination network mask for the new filter.	
Destination port	Enter here the destination port address for the new filter.	

Table 124: WBM “Configuration of User Filter” Page – “User Filter” Group

Parameters	Meaning	
Protocol	Enter here the protocols for the new 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	Enter here the interfaces for the new 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.

Click **[Add]** to apply the new filter. The change takes effect immediately.

Click the **[Delete]** button to delete an existing filter. The change takes effect immediately.

15.1.1.4.6 “Certificates” Page

On the “Certificates” page, you will find options to install or delete certificates and keys.

“Installed Certificates” Group

Table 125: WBM “Certificates” Page – “Certificate List” Group

Parameters	Explanation
<certificate name>	The loaded certificates are displayed. If no certificate has been loaded. “No certificates existing” is displayed.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file PC to the product, click the **[Upload]** button. The changes take effect immediately.

The certificates are stored in the directory “/etc/certificates/” and the keys in the directory “/etc/certificates/keys/”.

Click **[Delete]** to delete an entry. The changes take effect immediately.

“Installed Private Keys” Group

Table 126: WBM “Certificates” Page – “Private Key List” Group

Parameters	Meaning
<private key name>	The loaded keys are displayed. If no key has been loaded, “No private keys existing” is displayed.

To select a file on the PC, click the **Choose file …** selection field.

To transfer the selected file PC to the product, click the **[Upload]** button. The changes take effect immediately.

The certificates are stored in the directory “/etc/certificates/” and the keys in the directory “/etc/certificates/keys/”.

Click **[Delete]** to delete an entry. The changes take effect immediately.

15.1.1.4.7 “Boot mode configuration” Page

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

“Force internal boot” Group

Table 127: WBM Page “Boot mode configuration” – “Force internal boot” Group

Parameter	Meaning	
Boot mode	You 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.

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”.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

15.1.1.4.8 “Security Settings” Page

The network security settings are found on the “Security Settings” page.

“TLS Configuration” Group

Table 128: “Security Settings” WBM Page – “TLS Configuration” Group

Parameters	Explanation	
TLS Configuration	You can set what TLS versions and cryptographic methods are allowed for HTTPS.	
	Standard	The Webserver allows TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.3, as well as cryptographic methods that are no longer considered secure.
	Strong	The Webserver only allows TLS Version 1.2 and 1.3 and strong algorithms. Older software and older operating systems may not support TLS 1.2 and TLS 1.3.

Click the **[Submit]** button to apply a change. The change takes effect immediately.

Note

BSI TR-02102 Technical Guidelines
The rules for the “Strong” setting are based on the TR-02102 technical guidelines of the German Federal Office for Information Security (BSI).
You can find the guidelines on the Internet at: https://www.bsi.bund.de > “Publications” > “Technical Guidelines.”

15.1.1.4.9 “Advanced Intrusion Detection Environment (AIDE)” Page

The network security settings are available on the “Advanced Intrusion Detection Environment (AIDE)” page.

“Run AIDE check at startup” Group

Table 129: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Run AIDE check at startup” Group

Parameter	Explanation
Service active	Here, you can activate/deactivate the “AIDE check” when the controller is started.

Click the **[Submit]** button to apply the changes. The changes only take effect when the controller restarts.

“Refresh Options” group

Table 130: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Control AIDE and show log” Group

Parameter	Explanation	
Select Action	Select here 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	Activate display of only the last n messages. You also specify the number of messages to be displayed.	
Automatic refresh interval (sec)	Select the checkbox to enable cyclic refresh. Enter the cycle time in seconds in which a cyclic refresh is performed. The label of the button (“Refresh”/“Start“/“Stop”) changes depending on status.	

Click **[Refresh]** to update the display. The button is only displayed if the cyclic refresh is not enabled.

To enable cyclic refresh, click the **[Start]** button. The button is only displayed if cyclic refresh is enabled and has not yet started.

To stop cyclic refresh again, click the **[Stop]** button. The button only appears if cyclic refresh 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

update is stopped until you call up the “Advanced Intrusion Detection Environment (AIDE)” page again.

The messages are displayed below the settings.

15.1.1.4.10 “WAGO Device Access” Page

On the “WAGO Device Access” page you will find settings for authentication when scanning the node.

Note

Beta Status
In the present firmware version, the “WAGO Device Access” functionality is still in beta!

“Unauthenticated Requests” Group

Table 131: WBM Page “WAGO Device Access” – “Unauthenticated Requests” Group

Parameter	Meaning
Allow unauthenticated Device Scan	You set whether the node can be scanned without authentication. In the default setting, authentication is switched off. To increase the security level, you can enforce authentication for node scanning. In the current beta status, only head stations but no I/O modules are recognized when scanning!

Click the **[Submit]** button to apply a change. The change takes effect immediately.

15.1.1.5 “Diagnostic” Tab

15.1.1.5.1 “Log Message Viewer” Page

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

“Refresh Options” Group

Table 132: WBM “Log Message Viewer” Page – “Refresh Options” Group

Parameters	Meaning	
Read only the last	Activate display of only the last n messages. You also specify the number of messages to be displayed.	
Automatic refresh interval (sec)	Select the checkbox to enable cyclic refresh. Enter the cycle time in seconds in which a cyclic refresh is performed. The label of the button (“Refresh”/“Start“/“Stop”) changes depending on status.	
Source	Select the source of the diagnostic messages. The drop-down list depends on the user who is logged in.	
	user	Default diagnostic messages only
	admin	Default diagnostic messages and all log files in the folder `/var/log/*`

To refresh the display or to enable cyclic refresh, click the **[Refresh]** button. This button is only displayed if the cyclic refresh is not enabled.

To enable cyclic refresh, click the **[Start]** button. The button is only displayed if cyclic refresh is enabled and has not yet started.

To stop cyclic refresh again, click the **[Stop]** button. The button only appears if cyclic refresh is enabled.

The cyclical refresh is performed for as long as the “Diagnostic Information” page is open. If you change the WBM page, the refresh is stopped until you call up the “Diagnostic Information” page again.

The messages are displayed below the settings.

15.1.1.5.2 “Download” Page

“Diagnostic Information” Group

Click the **[Download]** button to download diagnostic information from the device. An archive file is then created that contains the log messages, the firmware version and a list of the installed packages. This file is saved to the Downloads folder on your computer.

15.1.1.5.3 “Network Capture” Page

All the settings required for logging the network traffic on the device and downloading these logs are available on the “Network Capture” page.
The current status of network traffic logging is displayed.

“State” Group

Table 133: “Network Capture” Page – “State” Group

Parameter	Explanation
Current State	The current status of network traffic logging is displayed here.
Last Captured Package Count	Network packages already logged are displayed here.
Last Refresh Time	The last refresh time for Current State and Last Captured Package Count is displayed here.

“Configuration” Group

Table 134: “Network Capture” Page – “Configuration” Group

Parameter	Explanation	
Enable	Here, you can activate or deactivate logging.	
Rotate Log Files	Here, you can activate or deactivate rotating logging. When this option is activated, network traffic is recorded in up to three files of 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. Filesize	Specify the maximum file size for the data log file.	
Storage Location	Select the storage location for the logged data. Selection is possible only when both storage options are available.	
	Internal Flash	Data will be stored in the controller's internal memory.
	SD Card	Data will be stored on the SD card. If “SD card” has been selected and the card is no longer inserted, this option is no longer enabled and only the “Internal flash” option can be selected.
Listen On Network Interface	Here, select the network interface from which network traffic is to be logged. Any of the available network interfaces of the device can be selected.	

Click **[Submit]** to apply the change. The change takes effect immediately.

“Filter Configuration” Group

Table 135: “Network Capture” Page – “Filter Configuration” Group

Parameter	Explanation
Capture Filter	You can set capture filters here. These filters are used to log only the relevant or required data traffic. This enables you to record only the communication for one port, for example, or only from a defined IP address. More information on possible filter settings is given in the “Capture Filter” notes in the “Wireshark” documentation.

Click the **[Check]** button to check the specified “Capture Filter” for correctness.

Click **[Submit]** to apply the change. The change takes effect immediately.

“Log Download” Group

Table 136: “Network Capture” Page – “Log Download” Group

Parameter	Explanation
Select Log File	Select a log here that can be downloaded using the **[Download]** button.

Click the **[Download]** button to download the selected log from the device.

Click the **[Download All]** button to download all the logs from the device.

List of Figures

Figure 1: Front view 20
Figure 2: View on top 20
Figure 3: Labeling (Example) 21
Figure 4: Type plate (Example) 22
Figure 5: Termination with DTE-DCE Connection (1:1) 25
Figure 6: Termination with DCE-DCE Connection (Cross-Over)....25
Figure 7: RS-485 Bus Termination 26
Figure 8: Connections DIO X11 (Example)....29
Figure 9: Schematic Diagram 34
Figure 10: Example for Linux® Password 43
Figure 11: Start Behavior 47
Figure 12: Browser process....48
Figure 13: “WAGO Ethernet Settings” – Starting Screen (Example)....56
Figure 14: “WAGO Ethernet Settings” – “Network” Tab (Example)....57
Figure 15: “Open DHCP”, Example Figure 59
Figure 16: Entering Authentication 62
Figure 17: Password Reminder 64
Figure 18: WBM Browser Window (Example)....68
Figure 19: WBM Header with Tabs that Cannot be Displayed (Example)....68
Figure 20: WBM Status Bar (Example)....69
Figure 21: Removal from the Din-35 rail 80

List of Tables

Table 1: Number Notation 13
Table 2: Font Conventions 13
Table 3: Labeling....21
Table 4: Type plate 22
Table 5: Connectors on the front 23
Table 6: Connectors on top 23
Table 7: Function of RS-232 Signals for DTE/DCE 25
Table 8: X5 Pin Assignment 27
Table 9: X11 Pin Assignment 29
Table 10: SYS LED 32
Table 11: RUN LED 32
Table 12: CAN LED....32
Table 13: Positions Mode Selector Switch....33
Table 14: Technical Data – Device....35
Table 15: Technical Data – Climatic Environmental Conditions....35
Table 16: Technical Data – Power Supply....35
Table 17: Technical Data – Hardware 36
Table 18: Technical Data – Communication 36
Table 19: Technical Data – Interfaces Hardware....36
Table 20: Technical Data – Connections Hardware....37
Table 21: WBM Users 42
Table 22: Linux® User 43
Table 23: Default IP Addresses for ETHERNET Interfaces 55
Table 24: Network Mask 255.255.255.0 55
Table 25:User Settings in the Default State....64
Table 26: Access Rights for WBM Pages....65
Table 27: CODESYS V3 Priorities....72
Table 28: LED Signaling....75
Table 29: Accessories – Memory Cards....83
Table 30: Accessories – Connecting Cable and connector....83
Table 31: WBM “Device Status” Page – “Device Details” Group 84
Table 32: WBM “Device Status” Page – “Network TCP/IP Details” Group 85
Table 33: WBM “PLC Runtime Information” Page – “Runtime” Group 87
Table 34: WBM “PLC Runtime Configuration” Page – “General PLC Runtime Configuration” Group....93
Table 35: WBM “PLC Runtime Configuration” Page – “Webserver Configuration” Group....94
Table 36: WBM “TCP/IP Configuration” Page – “TCP/IP Configuration” Group ..95
Table 37: WBM “TCP/IP Configuration” Page – “DNS Server” Group....96
Table 38: WBM “Ethernet Configuration” Page – “Bridge Configuration” Group .97
Table 39: WBM “Ethernet Configuration” Page – “Switch Configuration” Group .98
Table 40: WBM "Ethernet Configuration" Page – "Dummy Interfaces" Group....99
Table 41: WBM "Ethernet Configuration" Page – "VLAN Interfaces" Group 99
Table 42: WBM “Ethernet Configuration” Page – “Ethernet Interface Configuration” Group....100
Table 43: WBM “Configuration of Host and Domain Name” Page – “Hostname” Group....101

Table 44: WBM “Configuration of Host and Domain Name” Page – “Domain Name” Group 101
Table 45: WBM “Routing” Page – “IP Forwarding through multiple interfaces” Group 103
Table 46: WBM “Routing” Page – “Custom Routes“ Group 104
Table 47: WBM “Routing” Page – “IP-Masquerading” Group 106
Table 48: WBM “Routing” Page – “Port Forwarding” Group 107
Table 49: WBM “Spanning Tree Protocol” Page – “Status” Group 108
Table 50: WBM “Spanning Tree Protocol” Page – “Parameter Settings” Group 109
Table 51: WBM “Clock Settings” Page – “Timezone and Format” Group 111
Table 52: WBM “Clock Settings” Page – “UTC Time and Date” Group 111
Table 53: WBM “Clock Settings” Page – “Local Time and Date” Group 112
Table 54: WBM “Configuration of Serial Interface” Page – “Current Serial Interface Configuration” Group 113
Table 55: WBM “Configuration of Serial Interface” Page – “Assign Owner of Serial Interface” Group 113
Table 56: WBM “Configuration of Serial Interface” Page – “Assign Owner of Serial Interface” Group 114
Table 57: WBM “Configuration of Service Interface” Page – “Assign Owner of Service Interface” Group 115
Table 58: WBM “Create Bootable Image” Page – “Create bootable image from active partition” Group 116
Table 59: WBM “Firmware Backup” Page – “Firmware Backup” Group 117
Table 60: WBM “Firmware Restore” Page – “Firmware Restore” Group 119
Table 61: WBM “Active System” Page – “Boot Device” Group 121
Table 62: WBM “Active System” Page – “System <n> (Internal Flash)” Group . 121
Table 63: WBM “Mass Storage” Page – “Devices” Group 122
Table 64: WBM “Mass Storage” Page – “Create new Filesystem on Memory Card” Group 122
Table 65: WBM “Software Uploads” Page – “Upload New Software” Group 123
Table 66: WBM “Configuration of Network Services” Page – “FTP” Group 124
Table 67: WBM “Configuration of Network Services” Page – “FTPES (explicit FTPS)” Group 124
Table 68: WBM “Configuration of Network Services” Page – “HTTP” Group 125
Table 69: WBM “Configuration of Network Services” Page – “HTTPS” Group .. 125
Table 70: WBM “Configuration of Network Services” Page – “I/O-*CHECK*” Group 125
Table 71: WBM “Configuration of NTP Client” Page – “NTP Client Configuration” Group 126
Table 72: WBM “PLC Runtime Services” Page – “CODESYS V3” Group 127
Table 73: WBM “SSH Server Settings” Page – “SSH Server” Group 128
Table 74: WBM “DHCP Server Configuration” Page – “DHCP Configuration Bridge <n>” Group 129
Table 75: WBM “Configuration of DNS Server” Page – “DNS Server” Group ... 130
Table 76: WBM “Status Overview” Page – “Connection <n>” Group 131
Table 77: WBM “Configuration of Connection <n>” Page – “Configuration” Group 132
Table 78: Display of the Selection and Input Fields Depending on the Selected Cloud Platform 135
Table 79: Choice of Data Protocol Depending on the Selected Cloud Platform 137

Table 80: Display of the Selection and Input Fields Depending on the Selected Data Protocol 137
Table 81: Choice of Cache Mode Depending on the Selected Data Protocol 137
Table 82: Display of the Selection and Input Fields Depending on the Selected Authentication 138
Table 83: WBM “Configuration of General SNMP Parameters” Page – “General SNMP Configuration” Group 139
Table 84: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Communities” Group 140
Table 85: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Trap Receivers” Group 141
Table 86: WBM “Configuration of SNMP v3 Parameters” Page – “Users” Group 142
Table 87: WBM “Configuration of SNMP v3 Parameters” Page – “Trap Receivers” Group 144
Table 88: WBM “Favorites” Page – “Favorite n” Groups 147
Table 89: MicroBrowser – Login Data 147
Table 90: WBM “Browser Settings > Monitoring” Page – “Monitoring” Group 149
Table 91: WBM “Browser Settings > Browser Security” Page – “Browser Security” Group 150
Table 92: WBM “Commissioning Settings” Page – “Commissioning” Group 151
Table 93: WBM Page “Docker Settings” – group “Docker Status” 152
Table 94: WBM “Screensaver” Page – “Screensaver Settings” Group 155
Table 95: WBM “Screensaver” Page – “Screen Care” Group 155
Table 96: WBM “WBM User Configuration” Page – “Change Password” Group 156
Table 97: WBM “OPC UA Configuration” Page – “OPC UA Server Configuration” Group 157
Table 98: WBM “OPC UA Configuration” Page – “OPC UA Server Security Settings” Group 158
Table 99: WBM “BACnet Status” Page – “BACnet Information” Group 159
Table 100: WBM “BACnet Status” Page – “BACnet License” Group 159
Table 101: WBM “BACnet Status” Page – “BACnet Data Link” Group 159
Table 102: WBM “BACnet Data Link” Page – “BACnet Restart” Group 160
Table 103: WBM “BACnet Configuration” Page – “BACnet Service” Group 160
Table 104: WBM “BACnet Configuration” Page – “BACnet Data” Group 160
Table 105: WBM “BACnet Configuration” Page – “BACnet Log Level” Group 161
Table 106: WBM “BACnet Configuration” Page – “BACnet Network Capture” Group 161
Table 107: WBM “BACnet Data Link” Page – “BACnet Restart” Group 162
Table 108: WBM “BACnet Data Link” Page – “BACnet/IP” Group 162
Table 109: WBM “BACnet Data Link” Page – “BACnet/SC” Group 162
Table 110: WBM “BACnet Data Link” Page – “BACnet/SC Certificate Authority (CA)” Group 163
Table 111: WBM “BACnet Data Link” Page – “BACnet/SC Certificate” Group 163
Table 112: WBM “BACnet Configuration” Page – “BACnet/SC Certificate Signing Request (CSR)” Group 163
Table 113: WBM “BACnet Data Link” Page – “BACnet/SC Default Certificates” Group 163

Table 114: WBM Page “BACnet Storage Location” – “BACnet Persistence” Group....164
Table 115: WBM Page “BACnet Storage Location” – “BACnet Trendlog” Group 164
Table 116: WBM Page “BACnet Storage Location” – “BACnet Eventlog” Group 165
Table 117: WBM “OpenVPN / IPsec Configuration” Page – “OpenVPN” Group 166
Table 118: WBM “OpenVPN / IPsec Configuration” Page – “IPsec” Group 167
Table 119: WBM “General Firewall Configuration” Page – “Global Firewall Parameter” Group 168
Table 120: WBM “Interface Configuration” Page – “Firewall Configuration Bridge <n> / VPN / WAN” Group 170
Table 121: WBM “Configuration of MAC Address Filter” Page – “Global MAC address filter state” Group....171
Table 122: WBM “Configuration of MAC Address Filter” Page – “MAC address filter state Bridge <n>” Group 172
Table 123: WBM “Configuration of MAC Address Filter” Page – “MAC address filter whitelist” Group 172
Table 124: WBM “Configuration of User Filter” Page – “User Filter” Group 173
Table 125: WBM “Certificates” Page – “Certificate List” Group....175
Table 126: WBM “Certificates” Page – “Private Key List” Group....175
Table 127: WBM Page “Boot mode configuration” – “Force internal boot” Group 176
Table 128: “Security Settings” WBM Page – “TLS Configuration” Group....177
Table 129: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Run AIDE check at startup” Group....178
Table 130: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Control AIDE and show log” Group 178
Table 131: WBM Page “WAGO Device Access” – “Unauthenticated Requests” Group....180
Table 132: WBM “Log Message Viewer” Page – “Refresh Options” Group 181
Table 133: “Network Capture” Page – “State” Group....183
Table 134: “Network Capture” Page – “Configuration” Group....184
Table 135: “Network Capture” Page – “Filter Configuration” Group 185
Table 136: “Network Capture” Page – “Log Download” Group 185

WAGO GmbH & Co. KG
Postfach 2880 • D - 32385 Minden
Hansastraße 27 • D - 32423 Minden
Phone: +49 571 887 – 0
Fax: +49 571 887 – 844169
E-Mail: info@wago.com
Internet: www.wago.com