TECHDOCS

Manual

WAGO Edge Controller

752-8303/8000-0002

Version 1.2.0

WAGO GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Phone: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 1 69

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 22
4.3.1 Connectors on the front 22
4.3.2 Connectors on top 22
4.3.3 “X1” and “X2” ETHERNET Interfaces 23
4.3.4 “X3” – RS-232/485 Serial Interface 23
4.3.4.1 Operating as an RS-232 Interface 24
4.3.4.2 Operating as an RS-485 Interface 24
4.3.5 “X4” – CAN Interface 25
4.3.6 “X5” Supply Voltage 26
4.3.7 “X6” and “X7” USB-2.0 Interfaces 26
4.3.8 “X8” – Line-out Audio Output (Headphones) 26
4.3.9 “X9” – HDMI Interface Type A 27
4.3.10 ”X10” – USB-C Interface 27
4.3.11 “X11” – Four Digital Inputs and Outputs DIO 27
4.3.12 “microSD” Memory Card Slot 28
4.4 Real-Time Clock 30
4.5 Display Elements 31
4.5.1 Status LED 31
4.6 Operating Elements 32
4.6.1 Mode Selector Switch 32
4.6.2 “CFG/RST” Button 32
4.7 Schematic Diagram 33
4.8 Technical Data 34

4.8.1 Device 34
4.8.2 Climatic Environmental Conditions 34
4.8.3 Power Supply 34
4.8.4 Hardware 35
4.8.5 Communication 35
4.8.6 Interfaces 35
4.8.7 Connectors 36
4.9 Approvals 37
4.10 Standards and Guidelines 37

5 Functions 38

5.1 Web Browser 38
5.2 Connection Monitoring 39
5.3 WBM for Configuration/Parameterization 39
5.4 Network 39
5.4.1 Interface Configuration 39
5.4.1.1 Operation with Separate Network Interfaces 39
5.4.2 Network Security 39
5.4.2.1 Users and Passwords 39
5.4.2.2 Services and Users 41
5.4.2.3 WBM User Group 41
5.4.2.4 Linux® User Group 41
5.4.2.5 SNMP User Group 42
5.4.2.6 Web Protocols for WBM Access 43
5.4.2.7 TLS Encryption 43
5.4.3 Network Configuration 43
5.4.3.1 Host Name/Domain Name 43
5.4.3.2 Default Gateways 44
5.5 Memory Card Functions 44
5.5.1 Backup 44
5.5.2 Restore 45
5.5.3 Create Image 45
5.6 Downloading Software 45
5.7 Booting 46
5.8 Licensed Software Components 48

6 Mounting 49

6.1 Assembly Guidelines/Standards 49
6.2 Mounting position 49
6.3 Mount to the Rail 50

7 Connecting 51

7.1 Earthing 51
7.2 Connecting Devices 51
7.3 Connecting the Power Supply 52

8 Commissioning 53

8.1 Switching ON 53
8.2 Login 53
8.3 Determining the IP Address of the Host PC 53
8.4 Setting an IP Address 53

8.4.1 Setting the IP Address via the WBM 54
8.4.2 Assigning an IP Address using DHCP....55
8.4.3 Changing an IP Address using “WAGO Ethernet Settings” 56
8.4.4 IP Connection via USB....57
8.4.5 Temporarily Setting a Fixed IP Address 58
8.5 Initiating Reset Functions 58
8.5.1 Warm Start Reset 58
8.5.2 Cold Start Reset....58
8.5.3 Software Reset 59
8.5.4 Factory Reset 59
8.6 Configuring in the Web-Based Management (WBM) 60
8.6.1.1 WBM User Administration....62
8.6.1.2 General Information about the Page....66
8.6.2 Reboot Function....68

9 *e!RUNTIME* Runtime Environment....69

9.1 General Notes 69
9.2 CODESYS V3 Priorities....70
9.3 Memory Spaces under *e!RUNTIME*....71
9.3.1 Program and Data Memory....71
9.3.2 Function Block Limitation 71
9.3.3 Remanent Memory 71

10 Diagnostics....72

11 Service....73

11.1 Changing the Configuration with the WBM 73
11.2 Firmware Changes 74
11.2.1 Use *e!COCKPIT* to Update/Downgrade the Firmware....75
11.2.2 Use WAGOupload to Update/Downgrade the Firmware....76
11.2.3 Perform Firmware Update/Downgrade....77

12 Removal....78

12.1 Removal from the Rail 78

13 Disposal....79

13.1 Electrical and electronic equipment 79
13.2 Packaging....79

14 Accessories....81

15 Appendix 82

15.1 Configuration Dialogs 82
15.1.1 Web-Based-Management (WBM) 82
15.1.1.1 “Information” Tab....82
15.1.1.1.1 “Device Status” Page 82
15.1.1.1.2 “Vendor Information” Page....84
15.1.1.1.3 “PLC Runtime Information” Page 85
15.1.1.1.4 “WAGO Software License Agreement” Page 87
15.1.1.1.5 “Open Source Licenses” Page 88
15.1.1.1.6 “WBM Third Party License Information” Page 89
15.1.1.1.7 “WBM Version” Page 90
15.1.1.2 “Configuration” Tab....91

15.1.1.2.1 “PLC Runtime Configuration” Page 91
15.1.1.2.2 “TCP/IP Configuration” Page 94
15.1.1.2.3 “Ethernet Configuration” Page 96
15.1.1.2.4 “Configuration of Host and Domain Name” Page 99
15.1.1.2.5 “Routing” Page 101
15.1.1.2.6 “Clock Settings” Page 106
15.1.1.2.7 “Configuration of Serial Interface RS232/RS485” Page 108
15.1.1.2.8 “Create Bootable Image” Page 109
15.1.1.2.9 “Firmware Backup” Page 110
15.1.1.2.10 “Firmware Restore” Page 112
15.1.1.2.11 “Active System” Page 114
15.1.1.2.12 “Mass Storage” Page 115
15.1.1.2.13 “Software Uploads” Page 116
15.1.1.2.14 “Configuration of Network Services” Page 117
15.1.1.2.15 “Configuration of NTP Client” Page 119
15.1.1.2.16 “PLC Runtime Services” Page 120
15.1.1.2.17 “SSH Server Settings” Page 122
15.1.1.2.18 “TFTP Server” Page 123
15.1.1.2.19 “DHCP Server Configuration” Page 124
15.1.1.2.20 “Configuration of DNS Server” Page 125
15.1.1.2.21 “Status overview” Page 126
15.1.1.2.22 “Configuration of Connection <n>” Page 127
15.1.1.2.23 “Configuration of General SNMP Parameters” Page 131
15.1.1.2.24 “Configuration of SNMP v1/v2c Parameters” Page 132
15.1.1.2.25 “Configuration of SNMP v3 Users” Page 134
15.1.1.2.26 “Favorites” Page 136
15.1.1.2.27 “Autostart” Page 138
15.1.1.3 “Monitoring” Page 139
15.1.1.4 “Browser Security” Page 140
15.1.1.5 “Fonts” Page 141
15.1.1.6 “Display Orientation” Page 142
15.1.1.7 “Screensaver” Page 143
15.1.1.7.1 “WBM User Configuration” Page 144
15.1.1.8 “Fieldbus” Tab 145
15.1.1.8.1 “OPC UA Status” Page 145
15.1.1.8.2 “OPC UA Configuration” Page 146
15.1.1.8.3 “OPC UA Information Model” Page 149
15.1.1.8.4 “MODBUS Services Configuration” Page 150
15.1.1.8.5 “BACnet …” Page 151
15.1.1.9 “Security” Tab 152
15.1.1.9.1 “OpenVPN / IPsec Configuration” Page 152
15.1.1.9.2 “General Firewall Configuration” Page 154
15.1.1.9.3 “Interface Configuration” Page 155
15.1.1.9.4 “Configuration of MAC Address Filter” Page 156
15.1.1.9.5 “Configuration of User Filter” Page 158
15.1.1.9.6 “Certificates” Page 160
15.1.1.9.7 “Security Settings” Page 161
15.1.1.9.8 “Advanced Intrusion Detection Environment (AIDE)” Page 162
15.1.1.10 “Diagnostic” Tab 164
15.1.1.10.1 “Diagnostic Information” Page 164

List of Figures **165**

List of Tables **166**

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
- WAGO Software, “***e!****COCKPIT*” manual (2759-0101)
- “Industrial ETHERNET” technology manual

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

1.3 Copyright

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.
- The hardware or software has been modified by the user or a third party.

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

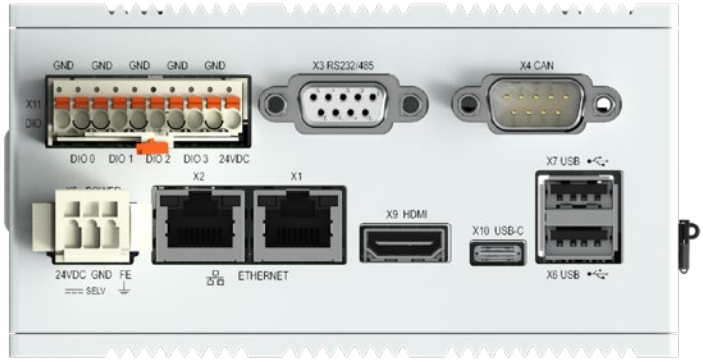

Figure 1: Front view

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

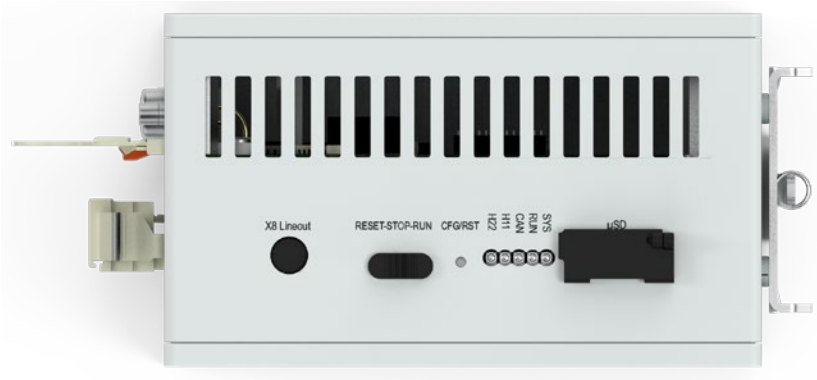

Figure 2: View on top

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 type plate is attached on the bottom side.

Table 3: Type Plate

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

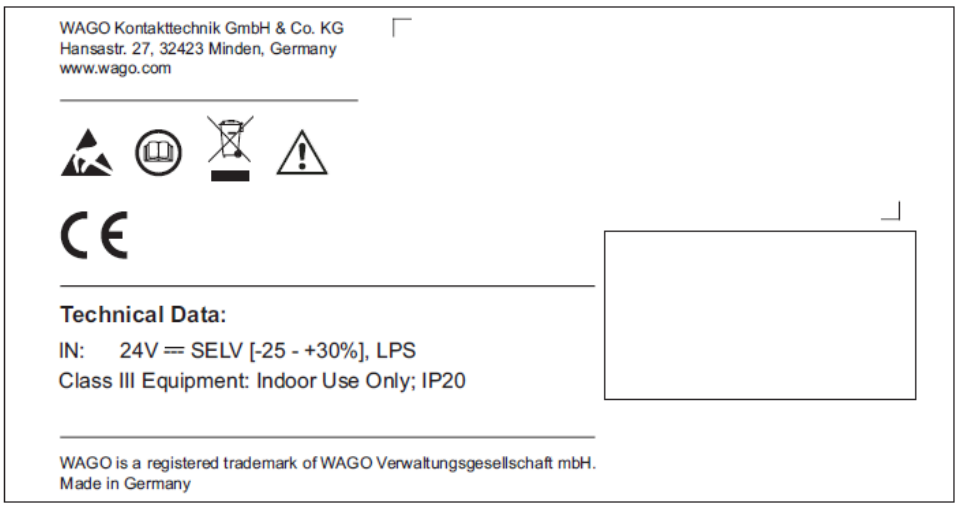

Figure 3: Type plate (Example)

4.3 Connectors

4.3.1 Connectors on the front

Table 4: 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 5: 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	RTS (request to send)	-
8	CTS (clear to send)	RXTX-N (signal neg.)
9	-	-

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 6: 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	---	---
7	RTS	Output	Input
8	CTS	Input	Output

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

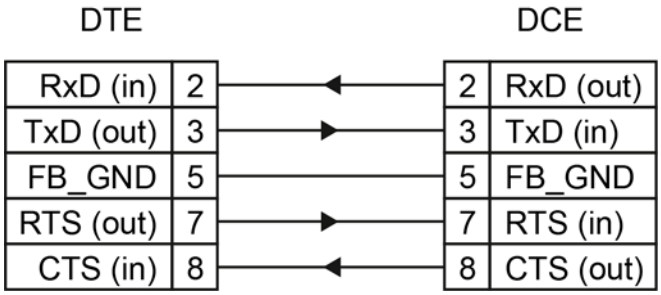

Figure 4: Termination with DTE-DCE Connection (1:1)

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

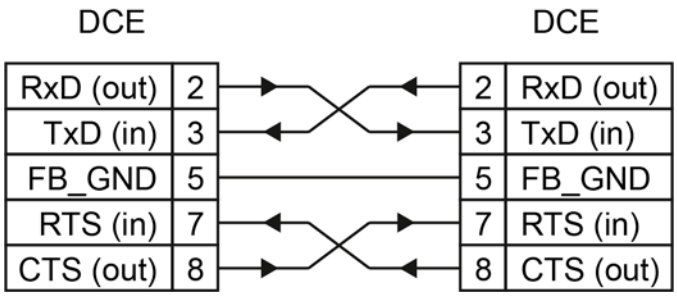

Figure 5: Termination with DCE-DCE Connection (Cross-Over)

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.

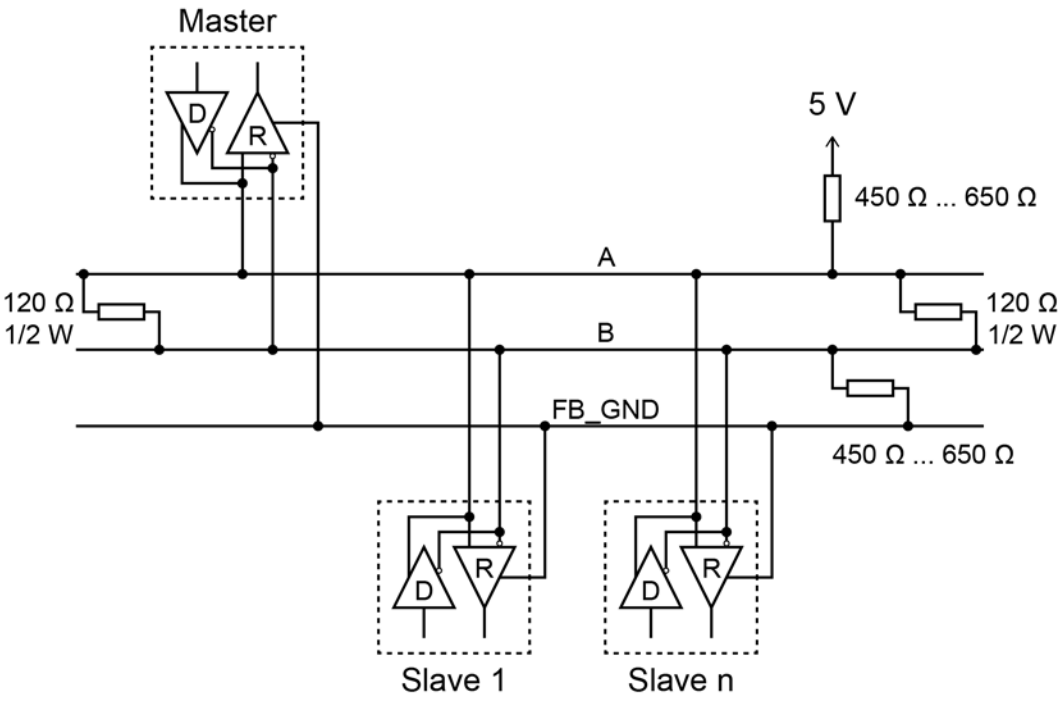

Figure 6: RS-485 Bus Termination

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 7: 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

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 8: 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.

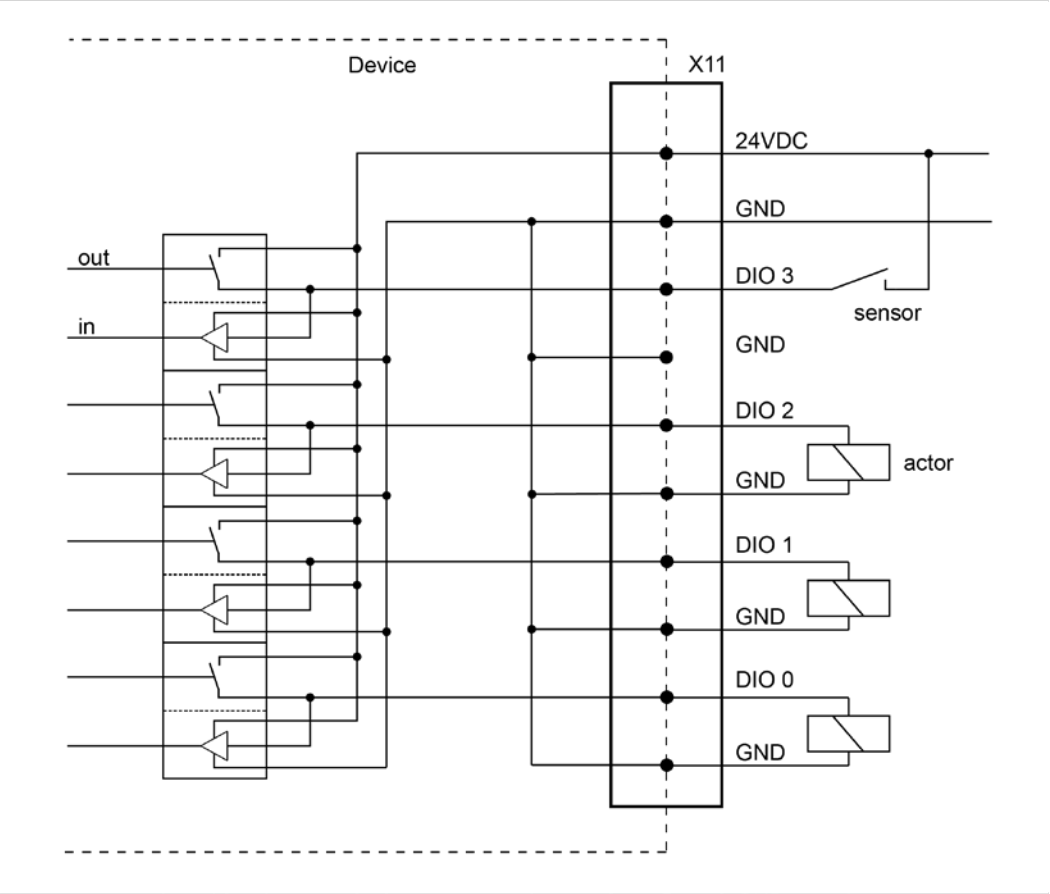

Figure 7: Connections DIO X11 (Example)

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

One three-color LED and four two-color LEDs are located on the left side. The meaning of the three-color SYS LED is analogous to that of the status LED on the front.

The RUN LED indicates the program status.

Table 9: RUN LED

LED Display	Explanation
Green flashing	No application and no boot project loaded.
Green, steady	***e!****RUNTIME* applications running.
Red, steady	All ***e!****RUNTIME* applications have stopped.

The CAN LED indicates the CANopen status.

Table 10: 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 11: 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 ***e!****RUNTIME* applications have stopped.
RUN	Latching	**Normal operation** ***e!****RUNTIME* 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.

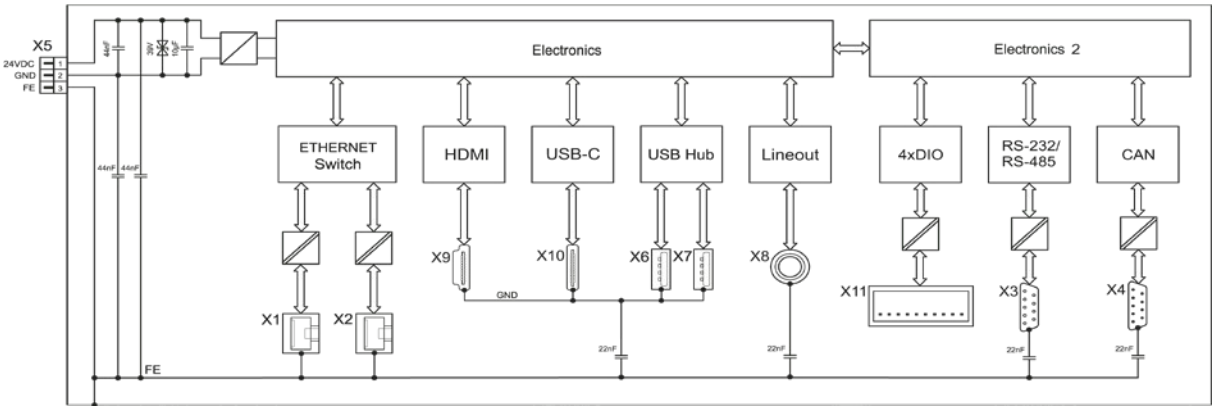

Figure 8: Schematic Diagram

4.8 Technical Data

4.8.1 Device

Table 12: 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 13: 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 14: 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 15: 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 16: 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 17: 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 x D-Sub-9
CAN Interface	1 x 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 18: 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:

CE Conformity Marking

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 ***e!****COCKPIT*, is then displayed with ***e!****RUNTIME* 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.

Table 19: Service and Users

Service	Users						
	WBM			Linux®			SNMP
	admin	user	guest	root	admin	user	
Web-Based Management (WBM)	X	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 20: WBM Users

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

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 21: 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.

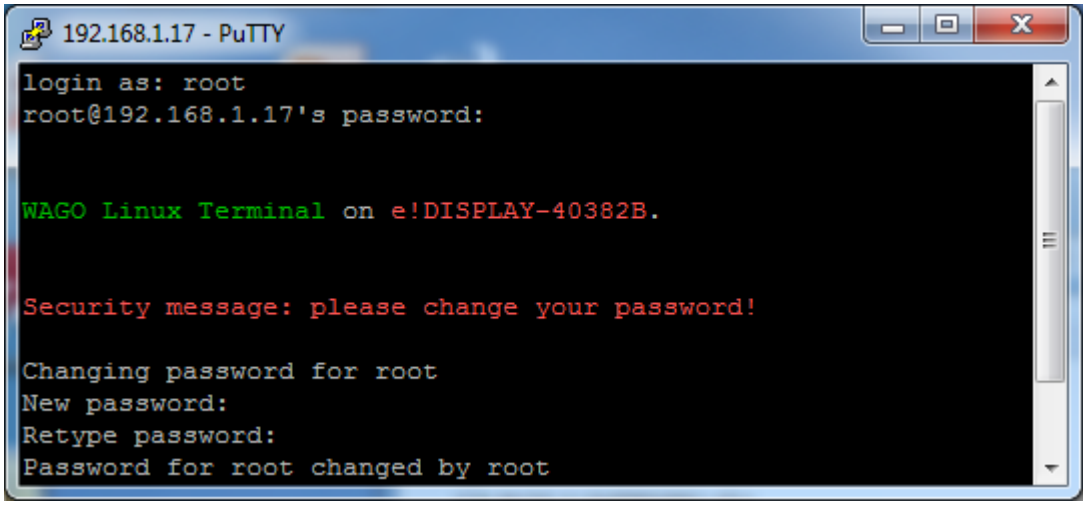

Figure 9: Example for Linux® Password

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 strong algorithms.
Older software and older operating systems may not support TLS 1.2 and encryption algorithms.
If “Standard” is set, TLS 1.0, TLS 1.1 and TLS 1.2 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
The German Federal Office for Information Security guidelines on migration to TLS 1.2 contain “compatibility matrices” that show what software is comparable with TLS 1.2.
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 or USB memory 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 USB memory 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

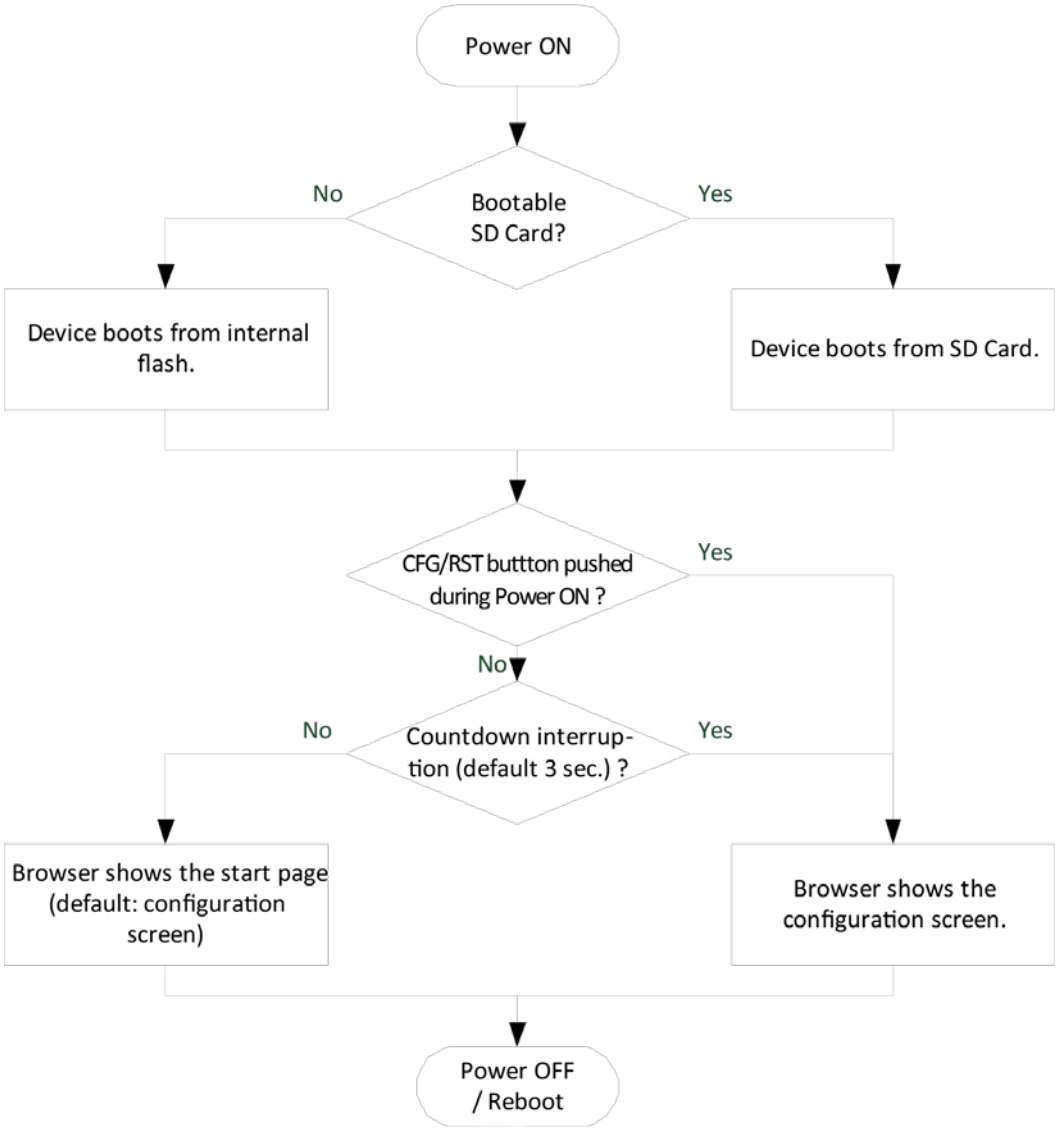

Figure 10: Start Behavior

Browser

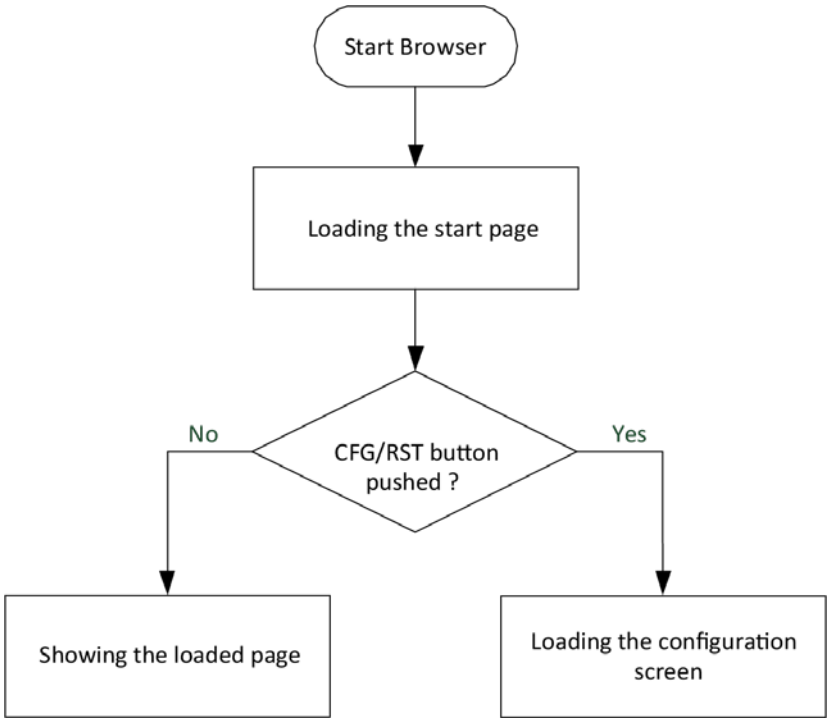

Figure 11: Browser process

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 ***e!****RUNTIME* runtime system software components that are subject to license verification is available for the product.

The ***e!****COCKPIT* software can be used for licensing. You can find corresponding instructions in the documentation of ***e!****COCKPIT*.

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 key for 30 days. This trial period only includes the days of 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.

When loading a program with licensed components, ***e!****COCKPIT* displays the number of days remaining.

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,” “user” or “guest.” 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 22: 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 23: 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 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.

8.4.2 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”.

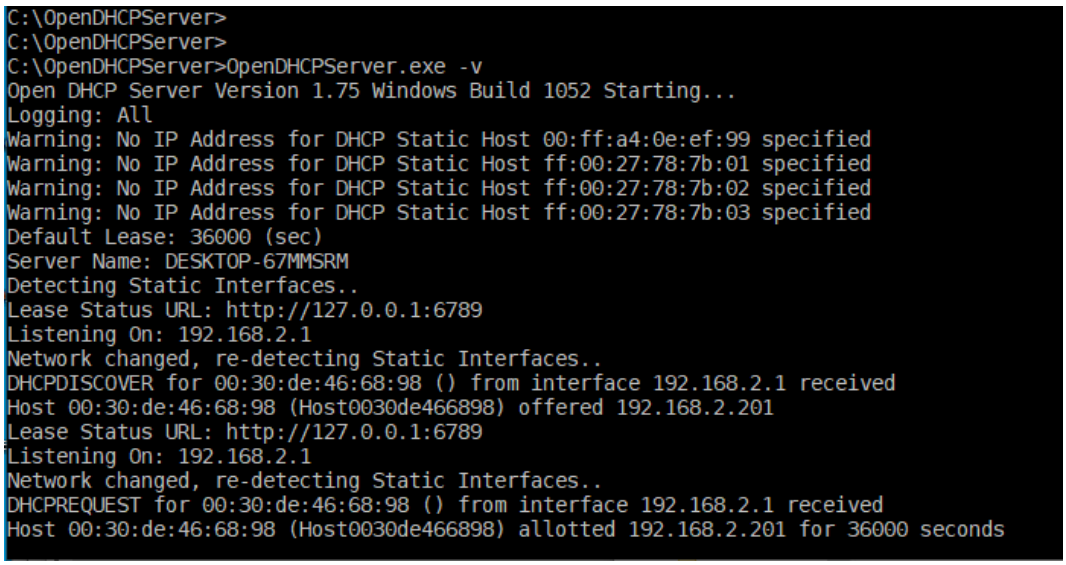

Figure 12: “Open DHCP”, Example Figure

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

The host name is “Host0030de466898”.

8.4.3 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 the WAGO USB service cable (Item No. 763-401) 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.

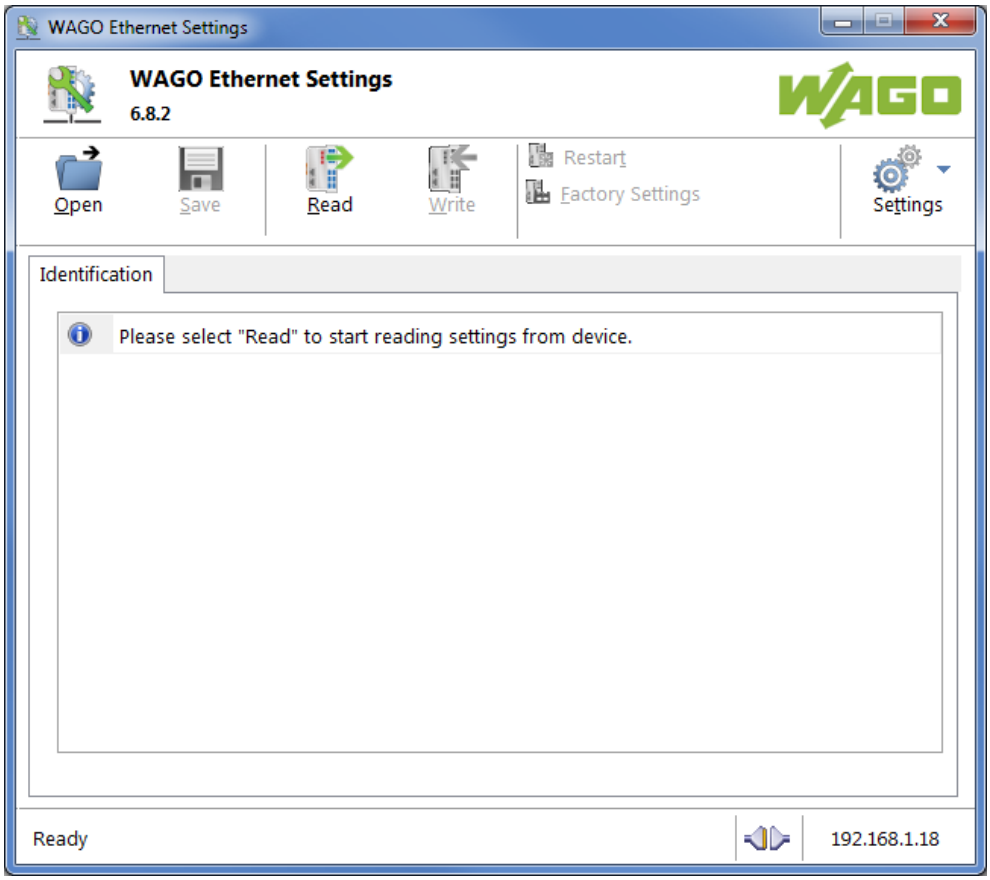

Figure 13: “WAGO Ethernet Settings” – Starting Screen (Example)

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

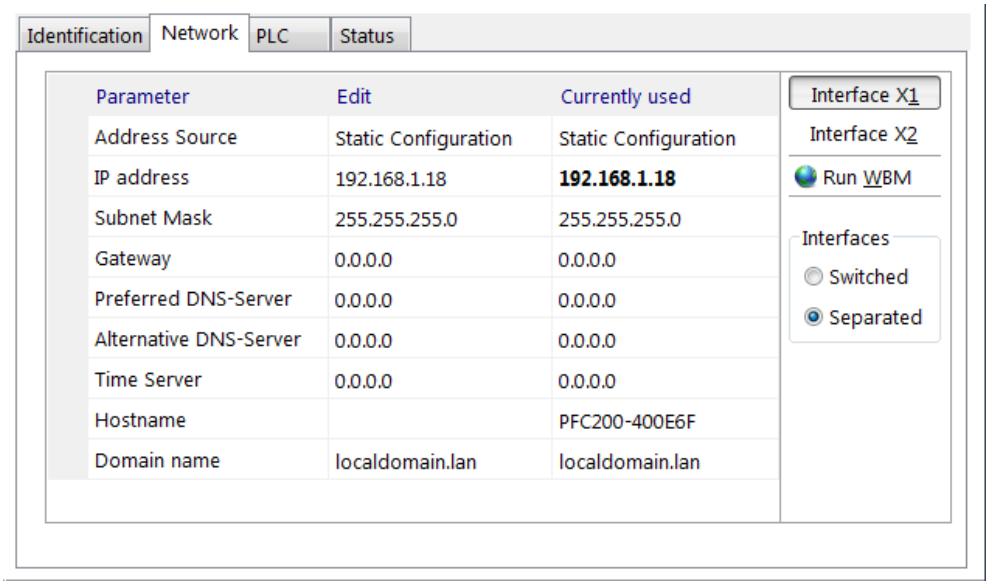

Figure 14: “WAGO Ethernet Settings” – “Network” Tab

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.

8.4.4 IP Connection via USB

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

1. Connect the controller to your PC via the USB service interface and a USB service cable.

2. If you are using Windows 10, go to step 4.
In Windows 7, the controller behaves like an external drive after connection. A driver for the IP connection via USB is stored on the drive.

3. Install this driver.
Communication is then possible via the IP connection via USB.

4. Call up the fixed IP address 192.168.42.42 in the browser.
The Web-Based Management of the controller opens. You can use it to make all the necessary settings on the controller.

8.4.5 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.

8.5 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 ***e!****RUNTIME* applications are reset with a warm start reset. All global data is set to its initialization values. This corresponds to the ***e!****COCKPIT* 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 ***e!****RUNTIME* 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 ***e!****COCKPIT* 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 a brief orange flashing of all LEDs. 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.

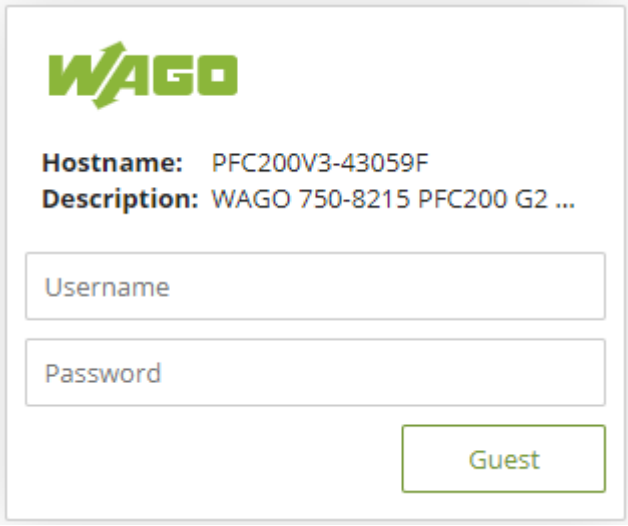

Figure 15: Entering Authentication

4. Enter the username and password.

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

6. If you only want to log in as a guest, click the **[Guest]** 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.

8.6.1.1 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.

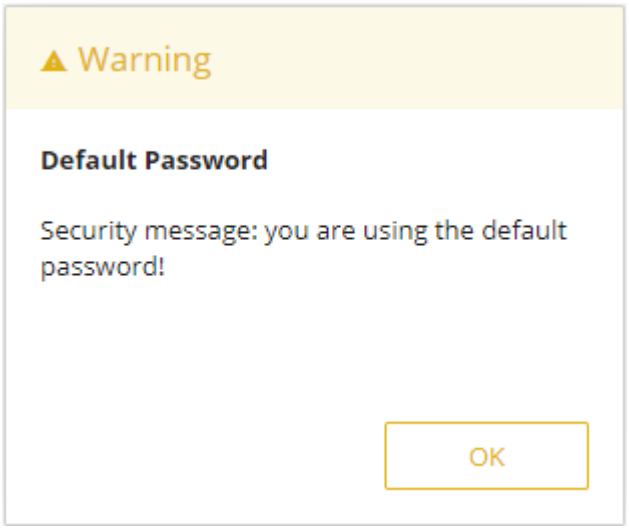

Figure 16: Password Reminder

Table 24:User Settings in the Default State

Users	Permissions	Default Password
admin	All (administrator)	wago
user	Supported to a limited extent	user
guest	Display only	---

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 separately.

Access to the WBM pages is as follows:

Table 25: Access Rights for WBM Pages

Tab/Navigation	WBM Page Title	User
Information		
Device Status	Device Status	guest
Vendor Information	Vendor Information	guest
PLC Runtime	PLC Runtime Information	guest
Legal Information		
WAGO Licenses	WAGO Software License Agreement	guest
Open Source Licenses	Open Source Licenses	user
WBM Licenses	WBM Third Party License Information	user
WBM Version	WBM Version Info	guest
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
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
TFTP	TFTP Server	admin
DHCP Server	DHCP Server Configuration	admin
DNS	Configuration of DNS Service	user
Cloud Connectivity		
Status	Overview	admin
Connection 1	Configuration	admin

Table 25: Access Rights for WBM Pages

Tab/Navigation			WBM Page Title	User
	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
	Display			
		Clean Display	Clean Display	user
		Touchscreen Calibration	Touchscreen Calibration	user
		Front Led	Front Led	user
		Font Upload	Fonts	user
		Brightness	Brightness	user
		Acoustic Signal	Acoustic Signal	user
		Display Orientation	Display Orientation	user
		Screensaver	Screensaver	user
	Users		WBM User Configuration	admin
Fieldbus				
	OPC UA			
		Status	OPC UA Status	admin
		Configuration	OPC UA Configuration	admin
		Information Model	OPC UA Information Model	admin
	Modbus		Modbus Services Configuration	user
	BACnet			
		Status	BACnet Status	admin
		Configuration	BACnet Configuration	admin
		Storage Location	BACnet Storage Location	admin
		Files	BACnet Files	admin
		Diagnostic	BACnet Diagnostic	admin
Security				
	OpenVPN / IPsec		OpenVPN / IPsec Configuration	admin
	Firewall			
		General Configuration	General Firewall Configuration	admin
		Interface Configuration	Interface Configuration	admin

Table 25: Access Rights for WBM Pages

Tab/Navigation		WBM Page Title	User
	MAC Address Filter	Configuration of MAC Address Filter	admin
	User Filter	Configuration of User Filter	admin
Certificates		Certificates	admin
TLS		Security Settings	admin
Integrity		Advanced Intrusion Detection Environment (AIDE)	admin
Diagnostic		Diagnostic Information	guest

8.6.1.2 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.

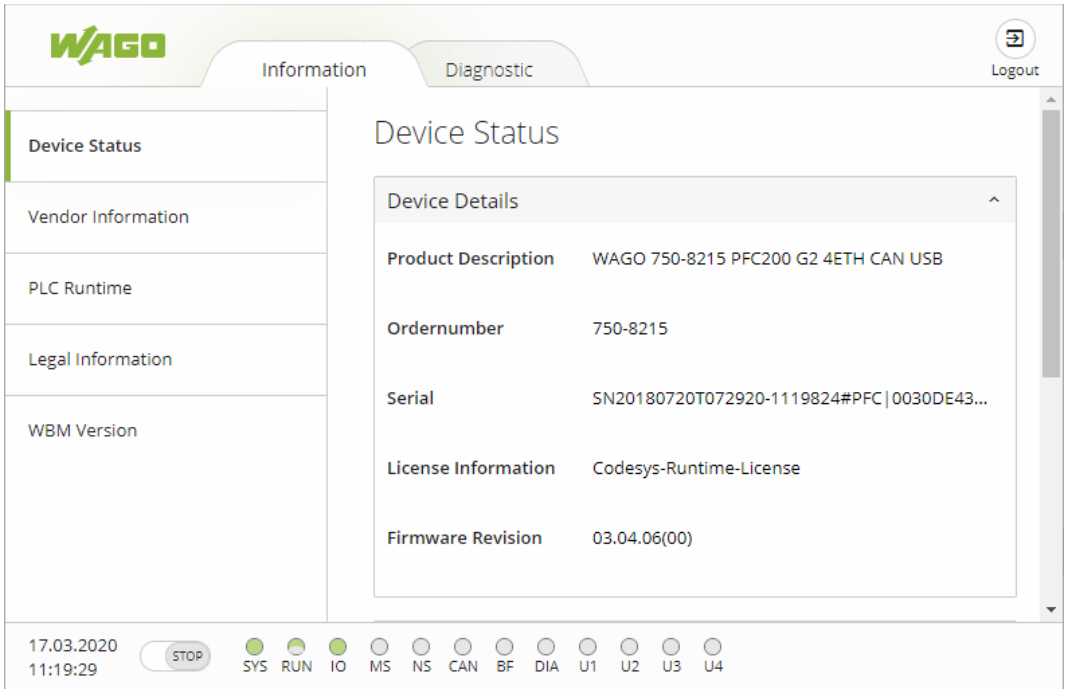

Figure 17: WBM Browser Window (Example)

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.

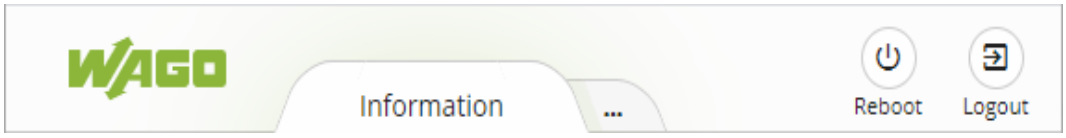

Figure 18: WBM Header with Tabs that Cannot be Displayed (Example)

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.

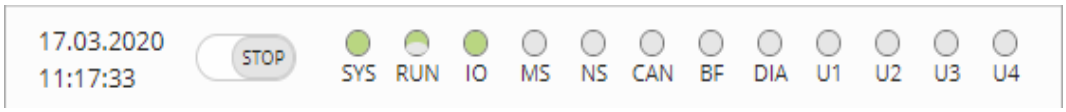

Figure 19: WBM Status Bar (Example)

- 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)”.

8.6.2 Reboot Function

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

9 *e!RUNTIME* Runtime Environment

9.1 General Notes

Note

Additional Information
Information on the installation and startup of ***e!****COCKPIT* is provided in the corresponding manual.
Information on programming is provided in the CODESYS 3 documentation.

9.2 CODESYS V3 Priorities

A list of priorities implemented for the controller is provided below as supplementary information to the CODESYS 3 documentation.

Table 26: 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 *e!RUNTIME*

The memory spaces in the controller under ***e!****RUNTIME* have the following sizes:

- Program memory: 32 Mbytes
- Data memory: 128 Mbytes
- Input data: 64 kbytes
- Output data: 64 kbytes
- Flags: 24 kbytes
- Retain: 104 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 section is subdivided into the flag area (memory) and the retain area.

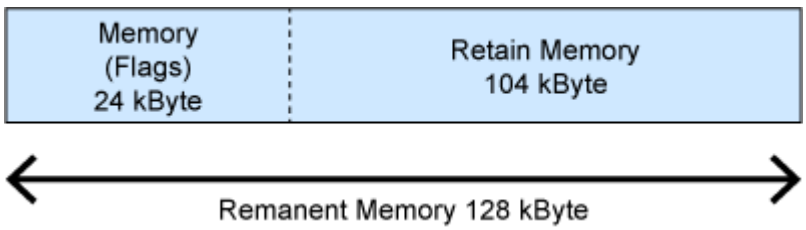

Figure 20: Remanent Main Memory

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 27: 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:

- ***e!****COCKPIT*
- WAGOupload
- Memory card and WBM

11.2.1 Use *e!COCKPIT* to Update/Downgrade the Firmware

1. Launch ***e!****COCKPIT*.
2. Create a new project or open an existing project.
3. Add at least one controller to your ***e!****COCKPIT* project either by scanning the network or going to the device catalog and entering the IP address of your controller in the settings dialog.

   Your controller is now displayed in the Device View of the project.
4. Select the displayed controller and click “Apply Selection” in the “SCAN” tab.
5. Click **[Add]** in the dialog.
6. Then click **[Replace Firmware]**. in the “DEVICE” tab.

   The “Replace Firmware” dialog opens.
7. In the “Replace Firmware” dialog, select the required firmware under “Available firmware on the PC” or click the “Select File” entry and select the * .wup firmware file for the required firmware.
8. Click **[Replace Firmware]** to transfer the firmware to the controller.
9. Wait until the operation ends with a status message and only then click **[OK]** to close the window.

The newly installed firmware is now available on your controller.

11.2.2 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.

11.2.3 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. Save your application and the controller settings.
2. Switch off the controller.
3. Insert the memory card with the new firmware image into the memory card slot. Use a special downgrade image if necessary (see above).
4. Switch on the controller.
5. After booting the controller, launch the WBM “Create Boot Image” page (you may have to temporarily change the IP address).
6. Create a new boot image on the internal memory.
7. Switch off the controller after completing the process.
8. Remove the memory card.
9. Switch on the controller.

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

12 Removal

12.1 Removal from the Rail

10. 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.

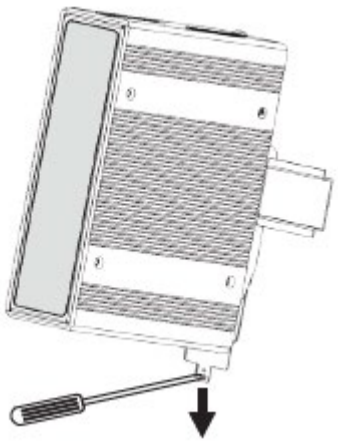

Figure 21: Removal from the Din-35 rail

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 28: Accessories – Memory Cards

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

Table 29: 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 30: 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 31: 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 PROFINET 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 and PLC program created in the programming software is provided on the “PLC Runtime Information” page. You will also find a link here to open WebVisu.

“Runtime” Group

Table 32: WBM “PLC Runtime Information” Page – “Runtime” Group

Parameter	Explanation	
Version	The version of the currently enabled runtime system is shown. If the runtime system is disabled, “None” is displayed and the subsequent fields of this group are hidden.	
Webserver Version	This shows the version number of the Webserver. This field appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.	
State	The PLC operating state is displayed. This field appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.	
	STOP	PLC program is not executed.
	RUN	PLC program is executed.
Number of Tasks	The number of tasks in the PLC program is shown. This field appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.	

“WebVisu” Group

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

“Project Details” Group

This group appears if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.

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

Parameter	Explanation
Date	The last save date of the project is displayed.
Title	The project information that the programmer has entered in the PLC program is displayed here (in the programming software under Project > Project Information ...). The information only appears in an executed PLC program. Descriptive texts up to 1024 characters long are given under “Description.”
Version	
Author	
Description	
Checksum	The calculated checksum of the project is displayed.

“Task <n>” Group(s)

One dedicated group is displayed for each task when the PLC program is executed. As a rule, only the group title is displayed with the task number, the task name and the task ID.

This group(s) appear(s) if the controller supports the CODESYS V2 runtime system and CODESYS V2 is set as the runtime system.

Table 34: WBM “PLC Runtime Information” Page – “Task n” Group(s)

Parameter	Explanation
Cycle count	Number of task cycles since the system start
Cycle time (µsec)	Currently measured task cycle time for the task
Cycle time min (µsec)	Minimum task cycle time for the task since the system start
Cycle time max (µsec)	Maximum task cycle time for the task since the system start
Cycle time avg (µsec)	Average task cycle time since the system start
Status	Task status (e.g., RUN, STOP)
Mode	Task execution mode (e.g., in cycles)
Priority	Set task priority
Interval (msec)	Set task interval

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 “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 35: 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 2	CODESYS V2 runtime system is enabled. This value only appears if the controller supports the CODESYS V2 runtime system.
	e!*RUNTIME*	***e!****RUNTIME* runtime system is enabled. This value only appears if the controller supports the ***e!****RUNTIME* runtime system.
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 36: WBM “PLC Runtime Configuration” Page – “Webserver Configuration” Group

Parameter	Meaning	
CODESYS V2 Webserver State	This displays the status (enabled/disabled) of the CODESYS V2 Webserver. This field only appears if the controller supports the CODESYS V2 runtime system.	
e!*RUNTIME* Webserver State	This indicates the status (enabled/disabled) of the ***e!****RUNTIME* Webserver. This field only appears if the controller supports the ***e!****RUNTIME* runtime system.	
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 37: 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.	
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
IP Address	Enter a static IP address. This is enabled if “Static IP” is enabled in the **Configuration Type** field.	
Subnet Mask	Enter the subnet mask. This is enabled if “Static IP” is enabled in the **Configuration Type** field.	

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

“DNS Server” Group

Table 38: WBM “TCP/IP Configuration” Page – “DNS Server” Group

Parameters	Explanation
New Server IP	Add additional DNS addresses. You can enter 10 addresses.
Manually Assigned	The addresses of the defined DNS servers are displayed. If no server has been entered, “No DNS Servers configured” is displayed.
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.

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

Click the **[Delete]** button to delete the selected 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 39: 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 40: 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.
Fast Aging	Set here the aging time of unused entries in the list of MAC addresses with a port assignment to external network stations. This field is only enabled in “switched” mode. Fast aging is only effective in this mode.	
	Disabled	An unused address entry becomes obsolete after 200 seconds.
	Enabled	An unused address entry becomes obsolete after 800 microseconds.
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.

“Ethernet Interface Configuration” Group

Table 41: 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.	
Autonegotiation on	When Autonegotiation is enabled, the connection modalities are negotiated automatically with the peer devices.	
Speed/Duplex	Select the transmission speed and the duplex method:	
	10 Mbit half-duplex	Information can only be sent or received.
	100 Mbit half-duplex	
	10 Mbit full-duplex	Information can be sent and received simultaneously.
	100 Mbit full-duplex	

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 42: 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 a hostname is supplied via a DHCP response, this is enabled in the system. If there are several network interfaces with DHCP, the last received hostname is always valid.
If only the hostname configured here is to be valid, the configuration of the DHCP server must be adapted so that no hostnames are transferred in the DHCP response.

“Domain Name” Group

Table 43: 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 a domain name is supplied via a DHCP response, this is enabled in the system. If there are several server network interfaces with DHCP, the last received domain name is always valid.

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

15.1.1.2.5 “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 44: 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 45: 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 46: 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 47: 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.

15.1.1.2.6 “Clock Settings” Page

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

“Timezone and Format” Group

Table 48: 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 49: 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 50: 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.

15.1.1.2.7 “Configuration of Serial Interface RS232/RS485” Page

The settings for the serial interface are shown on the “Configuration of Serial Interface RS232/485” page.

“Serial Interface assigned to” Group

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

“Assign Owner of Serial Interface” Group

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

Table 51: WBM “Configuration of Serial Interface RS232” 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.

NOTICE

Remove RS-485 devices before switching to “Linux Console”!
Connected RS-485 devices can be damaged when switching to “Linux Console”. Remove these devices before switching!

Click **[Change Owner]** 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!

15.1.1.2.8 “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 52: 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.

15.1.1.2.9 “Firmware Backup” Page

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

“Firmware Backup” Group

Table 53: 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, 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, 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.

15.1.1.2.10 “Firmware Restore” Page

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

“Firmware Restore” Group

Table 54: 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 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

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.

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

15.1.1.2.11 “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 55: 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 56: 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!

15.1.1.2.12 “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 57: 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 58: 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]**.

15.1.1.2.13 “Software Uploads” Page

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

Table 59: 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.

15.1.1.2.14 “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*, port 2455 for CODESYS V2 and port 11740 for ***e!****COCKPIT*).
Only open ports and services during commissioning and/or configuration.

“Telnet” Group

Table 60: WBM “Configuration of Network Services” Page – “Telnet” Group

Parameters	Explanation
Telnet	Enable/disable the Telnet service. This service is disabled by default.

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

“FTP” Group

Table 61: WBM “Configuration of Network Services” Page – “FTP” Group

Parameters	Explanation
FTP	Enable/disable the FTP service. This service is disabled by default.

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

“FTPS” Group

Table 62: WBM “Configuration of Network Services” Page – “FTPS” Group

Parameters	Explanation
FTPS	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 63: WBM “Configuration of Network Services” Page – “HTTP” Group

Parameters	Explanation
HTTP	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 64: WBM “Configuration of Network Services” Page – “HTTPS” Group

Parameters	Explanation
HTTPS	Enable/disable the HTTPS service.

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

Note

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

“I/O-*CHECK*” Group

Table 65: WBM “Configuration of Network Services” Page – “I/O-*CHECK*“ Group

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

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

15.1.1.2.15 “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 66: 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.

15.1.1.2.16 “PLC Runtime Services” Page

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

“General Configuration” Group

Table 67: WBM “PLC Runtime Services” Page – “General Configuration” Group

Parameter	Explanation
Port Authentication Password	Specify the new password for port authentication.
Confirm Password	Enter the new password again for confirmation.

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

“CODESYS V2” Group

This group only appears if the controller supports the CODESYS V2 runtime system.

Table 68: WBM “PLC Runtime Services” Page – “CODESYS V2” Group

Parameter	Explanation
CODESYS 2 State	This displays the status (enabled/disabled) of the CODESYS V2 runtime system.
Webserver enabled	Enable or disable the CODESYS V2 Webserver for the CODESYS web visualization.
Communication enabled	Enable or disable the communication between the CODESYS V2 runtime system and the CODESYS V2 programming system.
Communication Port Number	Enter here the port number for communication with the CODESYS V2 programming system. The default value is 2455.
Port authentication enabled	Define here whether port authentication is enabled. If this is enabled, the password specified under “General Configuration” must be entered when logging in via CODESYS V2 IDE.

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

“*e!RUNTIME*” Group

This group only appears if the controller supports the ***e!****RUNTIME* runtime system.

Table 69: WBM “PLC Runtime Services” Page – “***e!****RUNTIME*” Group

Parameter	Explanation
e!*RUNTIME* State	This displays the status of the ***e!****RUNTIME* system (enabled/disabled).
Webserver enabled	Enable or disable the Webserver for the ***e!RUNTIME*** web visualization.
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.

15.1.1.2.17 “SSH Server Settings” Page

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

“SSH Server” Group

Table 70: 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.

15.1.1.2.18 “TFTP Server” Page

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

“TFTP Server” Group

Table 71: WBM “TFTP Server” Page – “TFTP Server” Group

Parameters	Explanation
Service active	Activate or deactivate the TFTP server.
Download directory	Specify the path for downloading the server directory.

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

15.1.1.2.19 “DHCP Server Configuration” Page

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

“DHCP Server Configuration Bridge <n>” Group

Table 72: WBM “DHCP Server Configuration” Page – “DHCP Configuration Bridge <n>” Group

Parameter	Explanation
Service active	Enable or disable the DHCP service for the interface Xn.
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 10 assignments or host names.
Ip Address	Enter the IP address. You can enter 10 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.

15.1.1.2.20 “Configuration of DNS Server” Page

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

“DNS Server” Group

Table 73: 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.

15.1.1.2.21 “Status overview” Page

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

“Service” Group

Table 74: WBM “Status Overview” Page – “Service” Group

Parameter	Explanation
Version	The cloud plug-in version is displayed.

“Connection <n>” Group

A group is displayed for each cloud access.

Table 75: WBM “Status Overview” Page – “Connection <n>” Group

Parameter	Explanation
Operation	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.

15.1.1.2.22 “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 76: 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.
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.
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.

Table 76: WBM “Configuration of Connection <n>” Page – “Configuration” Group

Parameter	Explanation
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.
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.
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.

Table 76: WBM “Configuration of Connection <n>” Page – “Configuration” Group

Parameter	Explanation
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 table shows the dependencies of the selection and input fields for the selected cloud platform.

Table 77: Dependencies of the Selection and Input Fields for the Selected Cloud Platform

Selection or Input Field	Cloud Platform						Authentication		Data Protocol				Last Will
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services	Shared Access Key	X.509 Certificate	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B	
Enabled	X	X	X	X	X	X							
Cloud platform	X	X	X	X	X	X							
Hostname	X	X	X	X	X	X							
Port number			X	X	(X)	X							
Device ID	X	X											
Client ID			>	>	>	X			X	X	X		
Authentication		X											
Activation Key	X	>					X						
Clean Session			X	(X)	(X)	X							
TLS			X	X	(X)	X							
CA file			X	X	X	X							
User			X	X									

Table 77: Dependencies of the Selection and Input Fields for the Selected Cloud Platform

Selection or Input Field	Cloud Platform						Authentication		Data Protocol				Last Will
	WAGO Cloud	Azure	MQTT AnyCloud	IBM Cloud	Amazon Web Services	SAP IoT Services	Shared Access Key	X.509 Certificate	WAGO Protocol	WAGO Protocol 1.5	Native MQTT	Sparkplug payload B	
Password			X	X									
Certification file		>	X		X	X		X					
Key file		>	X		X	X		X					
Use websockets	X	X											
Use compression	X	X	>						X	X	X		
Data Protocol			X	X	X	(X)							
• WAGO Protocol			X	X	X								
• WAGO Protocol 1.5			X	X	X								
• Native MQTT			X	X	X	(X)							
• Sparkplug payload B			X		X								
Cache mode	X	X	X	X	X	X							
Last Will			X	X	X	X							
• Last Will Topic			>	>	>	>							X
• Last Will Message			>	>	>	>							X
• Last Will QoS			>	>	>	>							X
• Last Will Retain			>	>	(>)	>							X
Device info		X	>	>	>				X	X			
Device status		X	>	>	>				X	X			
Standard commands		X	>		>				X	X			
Application property template		X											

X: Visible and active
(X): Visible, but not active
>: Visible and active; dependent on other settings
(>): Visible, but not active; dependent on other settings

15.1.1.2.23 “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 78: 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).
Object ID	Enter here the object ID (sysOID).

Click the **[Submit]** button to apply the changes. The changes only take effect after restarting the controller. For this purpose, use the WBM reboot function. Do not shut down the controller too early!

15.1.1.2.24 “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.

“SNMP v1/v2c Manager Configuration” Group

Table 79: WBM “Configuration of SNMP v1/v2c Parameters” Page – “SNMP v1/v2c Manager Configuration” Group

Parameters	Explanation
Protocol enabled	It is displayed the SNMP protocol for v1/v2c is enabled. The local community name is deleted when the protocol is disabled.
Local Community Name	Specify the community name for the SNMP manager configuration. 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. 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.”

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

“Actually configured Trap Receivers” Group

Table 80: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Actually Configured Trap Receivers” Group

Parameters	Meaning
Each configured trap receiver has its own area in the display. If no trap receiver has been configured, “(no trap receivers configured)” is displayed.	
IP Address	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: v1 or v2c (traps higher than v3 are displayed in a separate form).
Add new Trap Receiver	In this area, you can enter a new trap receiver.
IP Address	Specify the IP address for the new trap receiver (management station).
Community Name	Specify the community name for the new trap receiver configuration. The community name can be evaluated by the trap receiver. 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: v1 or v2c (traps higher than v3 are configured in a separate form).

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

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

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!

15.1.1.2.25 “Configuration of SNMP v3 Users” Page

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

“Actually configured v3 Users” Group

Table 81: WBM “Configuration of SNMP v3” Page – “Actually configured v3 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 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”)
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”)
Privacy Key	The key for encryption of the SNMP message is displayed. If nothing is displayed, the “authentication key” is automatically used.
Notification Receiver IP	The IP address of a trap receiver for v3 traps is displayed. If no v3 traps are to be sent for this user, this field remains blank.
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.

Table 81: WBM “Configuration of SNMP v3” Page – “Actually configured v3 Users” Group

Parameters	Meaning
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”)
Authentication Key (min. 8 char.)	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”)
Privacy Key (min. 8 char.)	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.
Notification Receiver IP	Specify an IP address for a trap receiver for v3 traps. If no v3 traps are to be sent for this user, this field remains blank.

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

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

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!

15.1.1.2.26 “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 82: 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 the product restarts. For this purpose, use the WBM reboot function. Do not switch off the product too early!

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

e!*RUNTIME* **application prevents web visualization in the MicroBrowser!**
No ***e!****RUNTIME* 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 83: MicroBrowser – Login Data

Users	Default password
admin	wago

15.1.1.2.27 “Autostart” Page

You can set the Autostart options 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.

15.1.1.3 “Monitoring” Page

Make settings here for monitoring the product.

“Monitoring” Group

Table 84: 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.

15.1.1.4 “Browser Security” Page

Specify the browser security level.

“Browser Security” Group

Select the required security level (Low or High).

Table 85: 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.

15.1.1.5 “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.

15.1.1.6 “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.

15.1.1.7 “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 86: 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 87: 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.)

15.1.1.7.1 “WBM User Configuration” Page

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

“Change Passwords” 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 88: WBM “WBM User Configuration” Page – “Change Passwords” Group

Parameter	Explanation
Select User	Select the user (“User” or “Admin”) to whom you want to assign a new password.
Old Password	Enter the current password here for authentication.
New Password	Enter the new password here for the user selected under “Select User.” Permitted characters for the password are the following ASCII characters: a … z, A … Z, 0 … 9, blank spaces 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.

15.1.1.8 “Fieldbus” Tab

15.1.1.8.1 “OPC UA Status” Page

You can find the status information on the OPC UA service on the “OPC UA Status” page.

“OPC UA Server” Group

Table 89: WBM “OPC UA Status” Page – “OPC UA Server” Group

Parameter	Explanation
State	The current status (enabled / disabled) of the WAGO OPC UA server is displayed.
Version	The installed version of the WAGO OPC UA Server is displayed here.
License	Any existing OPC UA server license is displayed. Some features of the WAGO OPC UA server require a paid special license.

15.1.1.8.2 “OPC UA Configuration” Page

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

“General OPC UA Server Configuration” Group

Table 90: WBM “OPC UA Configuration” Page – “General OPC UA Server Configuration” Group

Parameter	Explanation	
Service enabled	Enable or disable the WAGO OPC UA Server here.	
Ctrl Configuration name	Enter the configuration names the controller contains in the PLC Open Device Set.	
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.	
Unlimited anonymous access	Access rights to the data provided by the server are set here.	
	Enabled	An unregistered user can view, read and write all variables.
	Disabled	Complete access to the data requires user logon with the appropriate rights.

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

“OPC UA Endpoints” Group

Table 91: WBM “OPC UA Configuration” Page – “OPC UA Endpoints” Group

Parameter	Meaning
Security Policy - None	Enable or disable the OPC UA endpoint “None”. This allows an unsecured connection to the OPC UA server to be established.
Security Policy - Basic128Rsa15	Enable or disable the “Basic128Rsa15” security policy. **Note:** This policy is no longer classified as secure.
Security Policy - Basic256Sha256	The “Basic256Sha256” security policy allows a secure connection to be established with the OPC UA server.

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

“OPC UA Security Settings” Group

Table 92: WBM Page “OPC UA Configuration” – “OPC UA Security Settings” Group

Parameter	Explanation	
Trust all clients	The verification is enabled or disabled here.	
	Enabled	A connection to all clients is permitted. → No security!
	Disabled	Connection is only allowed to clients with secure certificates.
URI Check Application	The URI check can be enable or disable here. A disabled URI check enables connection to an OPC server even if the URI on the server URI is different from the URI in the certificates.	
Error Certificate Time	The time can be enabled or disabled here. Certificates may have an expiration date. This date is checked against the current usage time on the device. The check cannot be run successfully if the time is incorrectly set on the device.	
Certificate Issuer Time Invalid	The time stamp check can be enabled or disabled here. CA certificates contain a validity time stamp from the manufacturer. This stamp is used when checking the time on the server hardware. If the time setting on the server hardware is incorrect or is missing entirely, the certificate may be indicated as invalid.	
Certificate Revocation Unknown	The accessibility check of the saving location for withdrawn certificates can be enabled or disabled here. Each certificate can have a location for withdrawn certificates. If network problems or other causes prevent access to the specified location, the certificate is not accepted.	
Certificate Issuer Revocation Unknown	The accessibility check of the storage location for withdrawn certificates can be enabled or disabled here. Each certificate of a certification location (CA certificate) can contain an entry for the withdrawn certificate saving location. If the location cannot be reached, the server will refuse the certificate.	

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

15.1.1.8.3 “OPC UA Information Model” Page

You can find the settings for the OPC UA information module on the “OPC UA Information Model” page.
The page is only visible on products that support software components that are subject to a license check (runtime licenses).

“OPC UA Server Information Model” Group

Table 93: WBM “OPC UA Information Model” Page – “OPC UA Server Information Model” Group

Parameter	Meaning
Feature enabled	Enable or disable the OPC UA Server information model.
informationmodel.xml	Select an XML description file for the information model to be used. Using a specific information model requires an extended OPC UA license!

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

To transfer the selected description file to the controller, click the **[Upload]** button.

To delete the installed description file from the controller, click the **[Delete]** button. After deletion, the default PLC Open information model is used again.

15.1.1.8.4 “MODBUS Services Configuration” Page

The “Modbus Services Configuration” page displays the settings for various Modbus® services. The groups only appear if the ***e!****RUNTIME* system is enabled. Otherwise an information text is displayed.

“Modbus TCP Slave” Group

Table 94: WBM “Modbus Services Configuration” Page – “Modbus TCP” Group

Parameters	Explanation
Service active	Disable or enable the Modbus/TCP service.

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

“Modbus UDP Slave” Group

Table 95: WBM “Modbus Services Configuration” Page – “Modbus UDP” Group

Parameters	Explanation
Service active	Disable/enable the Modbus UDP service.

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

15.1.1.8.5 “BACnet …” Page

The WBM pages “BACnet Status”, “BACnet Configuration”, “BACnet Storage Location“, “BACnet Files” and “BACnet Diagnostic” are only fully functional for test purposes or with an installed license.

The BACnet functionality can only be used if the controller supports the ***e!****RUNTIME* runtime system and ***e!****RUNTIME* is used as the runtime system.

If you use the BACnet functionality for test purposes without a license, it is indicated by the “SYS” LED (see Section “Diagnostics” > “Fieldbus/System” Display Elements).

You can find a description of the WBM pages in the technical information on licensable “***e!****RUNTIME* BACnet/IP 300 (M)/600 (M)” functionality.

15.1.1.9 “Security” Tab

15.1.1.9.1 “OpenVPN / IPsec Configuration” Page

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

“OpenVPN” Group

Table 96: 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 97: 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!

15.1.1.9.2 “General Firewall Configuration” Page

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

“Global Firewall Parameter” Group

Table 98: 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.
ICMP echo broadcast protection	Enable or disable the “ICMP echo broadcast” protection.
Max. UDP connections per second	You can specify the maximum number of UDP connections per second.
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.

15.1.1.9.3 “Interface Configuration” Page

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

“Firewall Configuration Bridge <n> / VPN” Group

A separate group is displayed for each configured bridge.
The settings in this group are based on the firewall configuration on the IP level.

Table 99: WBM “Interface Configuration” Page – “Firewall Configuration Bridge <n> / VPN” 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.	
ICMP echo limit per second	You can specify the maximum number of “ICMP pings” per second. “0” = “Disabled”	
ICMP burst limit (0 = disabled)	You can specify the maximum number of “ICMP echo bursts” per second. “0” = “Disabled”	
Service enabled	Telnet: This button is only displayed if Telnet is supported.	Enable or disable the firewall for the respective service. The services themselves must be enabled or disabled separately on the “Ports and Services” page.
	FTP	
	FTPS	
	HTTP	
	HTTPS	
	I/O-CHECK	
	PLC Runtime	
	PLC WebVisu – direct link (port 8080)	
	SSH	
	TFTP	
	BootP/DHCP	
	DNS	
	Modbus TCP	
	Modbus UDP	
	SNMP	
	OPC UA	
	PROFINET IO	

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

15.1.1.9.4 “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 a default entry with the following values:

MAC address: 00:30:DE:00:00:00
MAC mask: ff:ff:ff:00:00:00

If you enable the 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 100: 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 101: 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.

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 102: WBM “Configuration of MAC Address Filter” Page – “MAC address filter whitelist” Group

Parameters	Explanation
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.

15.1.1.9.5 “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 103: 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 103: 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.

15.1.1.9.6 “Certificates” Page

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

“Installed Certificates” Group

Table 104: WBM “Configuration of OpenVPN and IPsec” 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 105: WBM “Configuration of OpenVPN and IPsec” 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.

15.1.1.9.7 “Security Settings” Page

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

“TLS Configuration” Group

Table 106: “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 and TLS 1.2, as well as cryptographic methods that are no longer considered secure.
	Strong	The Webserver only allows TLS Version 1.2 and strong algorithms. Older software and older operating systems may not support TLS 1.2.

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.”

15.1.1.9.8 “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 107: 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 108: 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.

15.1.1.10 “Diagnostic” Tab

15.1.1.10.1 “Diagnostic Information” Page

The settings for displaying diagnostic messages are shown on the “Diagnostic Information” page.

Table 109: WBM “Diagnostic Information” Page

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.

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.

List of Figures

Figure 1: Front view 20
Figure 2: View on top 20
Figure 3: Type plate (Example) 21
Figure 4: Termination with DTE-DCE Connection (1:1) 24
Figure 5: Termination with DCE-DCE Connection (Cross-Over) 24
Figure 6: RS-485 Bus Termination 25
Figure 7: Connections DIO X11 (Example) 28
Figure 8: Schematic Diagram 33
Figure 9: Example for Linux® Password 42
Figure 10: Start Behavior 46
Figure 11: Browser process 47
Figure 12: “Open DHCP”, Example Figure 55
Figure 13: “WAGO Ethernet Settings” – Starting Screen (Example) 56
Figure 14: “WAGO Ethernet Settings” – “Network” Tab 57
Figure 15: Entering Authentication 60
Figure 16: Password Reminder 62
Figure 17: WBM Browser Window (Example) 66
Figure 18: WBM Header with Tabs that Cannot be Displayed (Example) 66
Figure 19: WBM Status Bar (Example) 67
Figure 20: Remanent Main Memory 71
Figure 21: Removal from the Din-35 rail 78

List of Tables

Table 1: Number Notation 13
Table 2: Font Conventions 13
Table 3: Type Plate 21
Table 4: Connectors on the front 22
Table 5: Connectors on top 22
Table 6: Function of RS-232 Signals for DTE/DCE 24
Table 7: X5 Pin Assignment 26
Table 8: X11 Pin Assignment 27
Table 9: RUN LED 31
Table 10: CAN LED 31
Table 11: Positions Mode Selector Switch 32
Table 12: Technical Data – Device 34
Table 13: Technical Data – Climatic Environmental Conditions 34
Table 14: Technical Data – Power Supply 34
Table 15: Technical Data – Hardware 35
Table 16: Technical Data – Communication 35
Table 17: Technical Data – Interfaces Hardware 35
Table 18: Technical Data – Connections Hardware 36
Table 19: Service and Users 41
Table 20: WBM Users 41
Table 21: Linux® User 42
Table 22: Default IP Addresses for ETHERNET Interfaces 54
Table 23: Network Mask 255.255.255.0 54
Table 24:User Settings in the Default State 62
Table 25: Access Rights for WBM Pages 63
Table 26: CODESYS V3 Priorities 70
Table 27: LED Signaling 72
Table 28: Accessories – Memory Cards 81
Table 29: Accessories – Connecting Cable and connector 81
Table 30: WBM “Device Status” Page – “Device Details” Group 82
Table 31: WBM “Device Status” Page – “Network TCP/IP Details” Group 83
Table 32: WBM “PLC Runtime Information” Page – “Runtime” Group 85
Table 33: WBM “PLC Runtime Information” Page – “Project Details” Group 86
Table 34: WBM “PLC Runtime Information” Page – “Task n” Group(s) 86
Table 35: WBM “PLC Runtime Configuration” Page – “General PLC Runtime Configuration” Group 91
Table 36: WBM “PLC Runtime Configuration” Page – “Webserver Configuration” Group 93
Table 37: WBM “TCP/IP Configuration” Page – “TCP/IP Configuration” Group 94
Table 38: WBM “TCP/IP Configuration” Page – “DNS Server” Group 95
Table 39: WBM “Ethernet Configuration” Page – “Bridge Configuration” Group 96
Table 40: WBM “Ethernet Configuration” Page – “Switch Configuration” Group 97
Table 41: WBM “Ethernet Configuration” Page – “Ethernet Interface Configuration” Group 98
Table 42: WBM “Configuration of Host and Domain Name” Page – “Hostname” Group 99

Table 43: WBM “Configuration of Host and Domain Name” Page – “Domain Name” Group 99
Table 44: WBM “Routing” Page – “IP Forwarding through multiple interfaces” Group....101
Table 45: WBM “Routing” Page – “Custom Routes“ Group 102
Table 46: WBM “Routing” Page – “IP-Masquerading” Group....104
Table 47: WBM “Routing” Page – “Port Forwarding” Group 105
Table 48: WBM “Clock Settings” Page – “Timezone and Format” Group....106
Table 49: WBM “Clock Settings” Page – “UTC Time and Date” Group....106
Table 50: WBM “Clock Settings” Page – “Local Time and Date” Group....107
Table 51: WBM “Configuration of Serial Interface RS232” Page – “Assign Owner of Serial Interface” Group....108
Table 52: WBM “Create Bootable Image” Page – “Create bootable image from active partition” Group....109
Table 53: WBM “Firmware Backup” Page – “Firmware Backup” Group....110
Table 54: WBM “Firmware Restore” Page – “Firmware Restore” Group....112
Table 55: WBM “Active System” Page – “Boot Device” Group 114
Table 56: WBM “Active System” Page – “System <n> (Internal Flash)” Group.114
Table 57: WBM “Mass Storage” Page – “Devices” Group 115
Table 58: WBM “Mass Storage” Page – “Create new Filesystem on Memory Card” Group....115
Table 59: WBM “Software Uploads” Page – “Upload New Software” Group....116
Table 60: WBM “Configuration of Network Services” Page – “Telnet” Group....117
Table 61: WBM “Configuration of Network Services” Page – “FTP” Group....117
Table 62: WBM “Configuration of Network Services” Page – “FTPS” Group 117
Table 63: WBM “Configuration of Network Services” Page – “HTTP” Group 118
Table 64: WBM “Configuration of Network Services” Page – “HTTPS” Group..118
Table 65: WBM “Configuration of Network Services” Page – “I/O-*CHECK*“ Group 118
Table 66: WBM “Configuration of NTP Client” Page – “NTP Client Configuration” Group....119
Table 67: WBM “PLC Runtime Services” Page – “General Configuration” Group 120
Table 68: WBM “PLC Runtime Services” Page – “CODESYS V2” Group....120
Table 69: WBM “PLC Runtime Services” Page – “***e!****RUNTIME*” Group 121
Table 70: WBM “SSH Server Settings” Page – “SSH Server” Group....122
Table 71: WBM “TFTP Server” Page – “TFTP Server” Group 123
Table 72: WBM “DHCP Server Configuration” Page – “DHCP Configuration Bridge <n>” Group 124
Table 73: WBM “Configuration of DNS Server” Page – “DNS Server” Group ...125
Table 74: WBM “Status Overview” Page – “Service” Group 126
Table 75: WBM “Status Overview” Page – “Connection <n>” Group 126
Table 76: WBM “Configuration of Connection <n>” Page – “Configuration” Group 127
Table 77: Dependencies of the Selection and Input Fields for the Selected Cloud Platform 129
Table 78: WBM “Configuration of General SNMP Parameters” Page – “General SNMP Configuration” Group 131
Table 79: WBM “Configuration of SNMP v1/v2c Parameters” Page – “SNMP v1/v2c Manager Configuration” Group....132

Table 80: WBM “Configuration of SNMP v1/v2c Parameters” Page – “Actually Configured Trap Receivers” Group 133
Table 81: WBM “Configuration of SNMP v3” Page – “Actually configured v3 Users” Group 134
Table 82: WBM “Favorites” Page – “Favorite n” Groups....137
Table 83: MicroBrowser – Login Data 137
Table 84: WBM “Browser Settings > Monitoring” Page – “Monitoring” Group ...139
Table 85: WBM “Browser Settings > Browser Security” Page – “Browser Security” Group....140
Table 86: WBM “Screensaver” Page – “Screensaver Settings” Group 143
Table 87: WBM “Screensaver” Page – “Screen Care” Group 143
Table 88: WBM “WBM User Configuration” Page – “Change Passwords” Group 144
Table 89: WBM “OPC UA Status” Page – “OPC UA Server” Group 145
Table 90: WBM “OPC UA Configuration” Page – “General OPC UA Server Configuration” Group....146
Table 91: WBM “OPC UA Configuration” Page – “OPC UA Endpoints” Group .147
Table 92: WBM Page “OPC UA Configuration” – “OPC UA Security Settings” Group....148
Table 93: WBM “OPC UA Information Model” Page – “OPC UA Server Information Model” Group 149
Table 94: WBM “Modbus Services Configuration” Page – “Modbus TCP” Group 150
Table 95: WBM “Modbus Services Configuration” Page – “Modbus UDP” Group 150
Table 96: WBM “OpenVPN / IPsec Configuration” Page – “OpenVPN” Group .152
Table 97: WBM “OpenVPN / IPsec Configuration” Page – “IPsec” Group 153
Table 98: WBM “General Firewall Configuration” Page – “Global Firewall Parameter” Group 154
Table 99: WBM “Interface Configuration” Page – “Firewall Configuration Bridge <n> / VPN” Group 155
Table 100: WBM “Configuration of MAC Address Filter” Page – “Global MAC address filter state” Group....156
Table 101: WBM “Configuration of MAC Address Filter” Page – “MAC address filter state Bridge <n>” Group 157
Table 102: WBM “Configuration of MAC Address Filter” Page – “MAC address filter whitelist” Group 157
Table 103: WBM “Configuration of User Filter” Page – “User Filter” Group 158
Table 104: WBM “Configuration of OpenVPN and IPsec” Page – “Certificate List” Group....160
Table 105: WBM “Configuration of OpenVPN and IPsec” Page – “Private Key List” Group 160
Table 106: “Security Settings” WBM Page – “TLS Configuration” Group.....161
Table 107: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Run AIDE check at startup” Group....162
Table 108: WBM “Advanced Intrusion Detection Environment (AIDE)” Page – “Control AIDE and show log” Group 162
Table 109: WBM “Diagnostic Information” Page....164

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