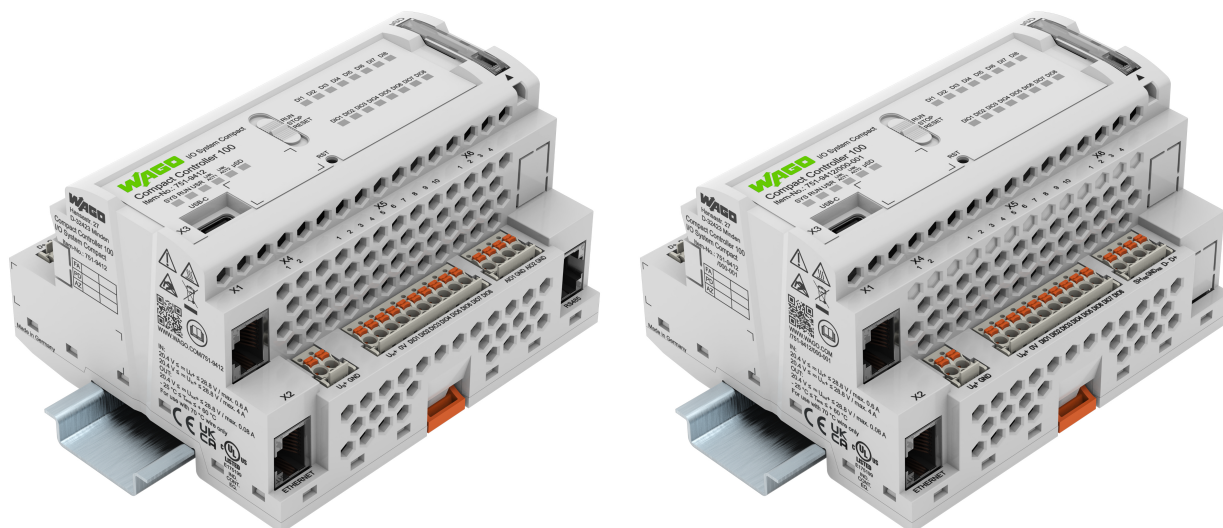


WAGO I/O System 751

SECURITY, Functional Description YOCTO Firmware

751-9412, 751-9412/000-001



© 2026 WAGO GmbH & Co. KG
All rights reserved.

WAGO GmbH & Co. KG

Hansastraße 27

D - 32423 Minden

Phone: +49 571/887 – 0

E-Mail: ✉ info@wago.com

Internet: 🌐 www.wago.com

Technical Support

Phone: +49 571/887 – 44555

E-Mail: ✉ support@wago.com

Internet: 🌐 www.wago.com/support

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

E-Mail: ✉ documentation@wago.com

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

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1 Provisions	7
1.1 Scope of Applicability	7
2 Cybersecurity	8
2.1 Threats	8
2.1.1 Cybersecurity Threat in General	8
2.1.1.1 Targets from a Product Perspective	8
2.1.1.2 Attack Vector from Product Perspective	8
2.1.2 Cybersecurity-Specific Threats	9
2.1.3 Vulnerability Assessment	9
2.2 Vulnerabilities in Network Access	9
2.2.1 Vulnerabilities in Network Access – Overview	9
2.2.2 PLC Functionality	10
2.2.3 Insecure Fieldbus	10
2.2.4 Insecure Local Bus	10
2.2.5 Root Privileges	10
2.2.6 Programmability	11
2.2.7 Engineering/Service Access	11
2.3 Vulnerabilities in Physical Access	11
2.3.1 Physical Access Vulnerabilities – Overview	11
2.3.2 Service Interface	12
2.3.3 Operating Mode Switch	12
2.3.4 Reset Button	12
2.3.5 Slot for SIM card	12
2.3.6 Slot for Memory Card	12
2.4 Potential Targets	13
2.4.1 Non-Monitored Indicators	13
2.5 Hardening and Cybersecurity Capabilities	13
2.5.1 Defense-in-Depth Principle	13
2.5.2 Reference Architecture	15
2.5.3 Hardening Measures	15
2.5.3.1 Secure Operating Environment	15
2.5.3.2 Secure Commissioning	16
2.5.3.3 Secure Operation	17
2.5.3.4 Secure Decommissioning	18
2.5.4 Cybersecurity Capabilities	19
2.5.5 Cybersecurity Service	19
3 Overview	21
4 Functions	22
4.1 Function Overview	22
4.2 System Functions	23
4.2.1 Standards Compliance	23
4.2.2 User Management	23
4.2.2.1 General Settings	24
4.2.2.1.1 Authentication Notice	24
4.2.2.1.2 Password Quality	24
4.2.2.1.3 Password Changes	24
4.2.2.2 System User Accounts	25
4.2.2.2.1 "admin" User Account	25
4.2.2.2.2 "root" User Account	25
4.2.2.3 Local User Management	26
4.2.2.3.1 Local User Accounts	26
4.2.2.3.2 Local User Roles	27

4.2.2.4	User Management via LDAP	27
4.2.2.5	User Login	28
4.2.2.5.1	Login Window	28
4.2.2.5.2	"OAuth2" Authentication Service	29
4.2.3	Event Logging	30
4.2.3.1	Internal Log Memory (Logging)	30
4.2.3.2	External Log Server (Remote Logging)	31
4.2.4	Product and system status	32
4.2.5	Real-Time Clock	32
4.2.5.1	Display/Manual Setting	32
4.2.5.2	Automatic Setting	33
4.2.6	CODESYS V3 Runtime Environment	33
4.2.6.1	Memory Areas under CODESYS V3	34
4.2.6.1.1	Program and Data Memory	34
4.2.6.1.2	Flag Area (Memory) and Retain Area	34
4.2.6.2	CODESYS Web Visualization	34
4.2.6.3	Security Settings in CODESYS	34
4.2.6.3.1	Secure Communication between Development Environment and Controller	34
4.2.6.3.2	Integrity of the Transferred Project Files	34
4.2.7	Firmware Update	35
4.2.7.1	Signatures and Certificates for Update Bundle	35
4.2.8	Certificate Management	35
4.2.8.1	Truststore	36
4.2.8.2	Device Certificates	37
4.2.9	Webserver	38
4.2.9.1	CORS Policy	39
4.2.10	Open Source Licenses	40
4.2.11	WAGO Device Access	40
4.2.11.1	Device Scan	40
4.2.12	Factory Reset	41
4.3	Hardware Functions	41
4.3.1	Mode Selector Switch/Reset Button	41
4.3.1.1	Operating Mode Switch	41
4.3.1.2	Reset Button	42
4.3.2	Communication Interface	42
4.3.3	USB-C Service Port	42
4.3.4	OnBoard I/O	43
4.3.4.1	Analog Inputs AI1, AI2	43
4.3.4.1.1	AI 0 ... 10 V	43
4.3.4.1.2	AI -10 ... 10 V	43
4.3.4.1.3	AI 0 ... 20 mA	43
4.3.4.1.4	AI 4 ... 20 mA	44
4.3.4.1.5	AI 3.6 ... 21 mA	44
4.3.4.2	Analog Inputs/Outputs AIO1, AIO2	44
4.3.4.2.1	AI 0 ... 10 V, -10 ... +10 V, 0 ... 20 mA, 4 ... 20 mA, 3.6 ... 21 mA	45
4.3.4.2.2	AO 0 ... 10 V	45
4.3.4.2.3	AO -10 ... +10 V	45
4.3.4.2.4	AO -12 ... +12 V	45
4.3.4.2.5	AO 0 ... 20 mA	45
4.3.4.2.6	AO 0 ... 22 mA	45
4.3.4.2.7	AO 4 ... 20 mA	46
4.3.4.3	Temperature Inputs PT1+/PT1-, PT2+/PT2-	46
4.3.4.3.1	Pt100, Pt200, Pt500, Pt1000	46
4.3.4.3.2	Ni100, Ni1000 (TK6180), Ni1000 (TK5000)	47
4.3.4.3.3	Ni120	47
4.3.4.3.4	Potentiometer 0 ... 1.2 kOhm	47
4.3.4.3.5	Potentiometer 0 ... 5 kOhm	48
4.3.4.4	Digital Inputs DI	48

4.3.4.5	Digital Inputs/Outputs DIO.....	48
4.3.4.5.1	DI 0/24 V	49
4.3.4.5.2	DO 0/24V.....	49
4.4	Configuration Functions	49
4.4.1	Web-based Management (WBM)	49
4.4.1.1	General Controls.....	49
4.4.1.2	Ribbon (Device Actions).....	50
4.4.1.3	Device	50
4.4.1.4	Workspace	51
4.4.1.4.1	I/O Check	51
4.4.1.4.2	Settings	54
4.4.1.4.3	Restart	59
4.4.1.4.4	Firmware	59
4.4.1.4.5	Backup/Restore.....	60
4.4.1.4.6	Device Log	61
4.4.1.5	Message Window	62
4.5	Network Functions.....	64
4.5.1	Network Configuration.....	64
4.5.1.1	Configuration for Security Requirements.....	64
4.5.1.2	Interface Configuration.....	64
4.5.1.2.1	Bridge and Port Configuration	64
4.5.1.3	Hostname/Domain Addresses.....	66
4.5.1.3.1	Hostname.....	67
4.5.1.3.2	Domain Addresses.....	67
4.5.2	Network Security	67
4.5.2.1	Providing a Secure Network Environment	67
4.5.2.2	Firewall.....	68
4.5.2.2.1	MAC Address Filter.....	68
4.5.2.2.2	ServiceRules	68
4.5.2.2.3	IP Address Filter	69
4.5.2.2.4	IP Forwarding Filter.....	69
4.5.2.2.5	Flood/Broadcast Protection.....	70
4.5.2.3	IPsec	70
4.5.3	Network Services.....	72
4.5.3.1	DHCP Client	72
4.5.3.2	SSH Service	72
4.6	Memory Functions	73
4.6.1	Automount	73
4.6.2	Data Backup	73
4.6.2.1	Backup Function	73
4.6.2.2	Restore Function	74
4.7	Diagnostic Functions	74
4.7.1	Diagnostics via Indicators.....	74
4.7.2	Diagnostics via WBM or WAGO Device Manager	74
4.7.2.1	Illustration of LEDs	74
4.7.2.2	Wiring Test (I/O Check)	74
4.7.2.3	Event Log (Device Log).....	75
5	Commissioning	77
5.1	Switching On the Controller	77
5.2	Setting an IP Address.....	77
5.2.1	Setting an IP Address via the WBM	77
5.2.2	Assigning an IP Address with DHCP	78
5.3	Changing Passwords	78
5.4	Managing Users	79
5.4.1	Managing Local User Roles and Accounts	79
5.4.1.1	Managing Local User Accounts.....	79

5.4.1.2	Managing Local User Roles	80
5.5	Switch Off/Restart.....	81
6	Configuration.....	82
6.1	Configuring in WBM	82
7	Service	84
7.1	Firmware Updates.....	84
7.1.1	Performing a Firmware Update with the WBM	84
7.2	Clearing Reset Functions.....	86
7.2.1	Warmstart Reset.....	86
7.2.2	Coldstart Reset	86
7.2.3	Software Reset (Restart)	86
7.2.4	Factory Reset	87
7.3	Starting/Stopping CODESYS Applications	88
7.3.1	Launching CODESYS Applications.....	88
7.3.2	Halting CODESYS Applications.....	88
7.4	Backing Up and Restoring Data	88
7.4.1	Performing a Backup	88
7.4.2	Performing a Restore	89
7.5	WDX Methods for Production.....	89
7.6	Creating and Managing Certificates	90
7.6.1	Creating Device Certificates.....	90
7.6.1.1	Self-Signed Certificates	90
7.6.1.2	Certificates Signed via an External PKI.....	91
7.6.2	Loading Externally Created and Signed Device Certificates.....	92
8	Diagnostics.....	93
8.1	Diagnostics via Indicators.....	93
8.2	Diagnostics via WBM	93
8.2.1	Testing the Wiring.....	93
8.2.2	Viewing the Device Log.....	94
8.3	Checking System Integrity	95

1 Provisions

1.1 Scope of Applicability

This document applies to the following products:

751-9412 (Compact Controller 100) (Compact Controller 100; 8DI 8DIO 2AI 2AIO 2RTD 2RS 2ETH; SD)

Version Firmware	01.02.03(03)
Product detail page	www.wago.com/751-9412

751-9412/000-001 (Compact Controller 100) (Compact Controller 100; 8DI 8DIO 2AI 2RTD 2RS 2ETH; SD)

Version Firmware	01.02.03(03)
Product detail page	www.wago.com/751-9412/000-001

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

Applicable document

□ **Product Manual** of the product used

Information

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

2 Cybersecurity

2.1 Threats

2.1.1 Cybersecurity Threat in General

Probability and Severity of Events

Products for industrial automation can be used in a wide variety of systems and applications. Depending on the application, the requirements for the **protection goals** of cybersecurity (integrity, availability or confidentiality of data) can vary. The incentives for potential attackers and the severity of cybersecurity incidents are just as varied.

As the manufacturer, we can describe the circumstances under which unauthorized access can be gained to which data areas, interfaces or functions of our product. Targets can be considered from the **product perspective**. As a manufacturer, we can provide instructions on how to use the product's cybersecurity capabilities to reduce the likelihood of unauthorized access.

From an **application point of view**, the operator must check what damage can occur, what level of security is required and whether additional measures are needed to increase security. One criterion for the appropriateness of the level of security, for example, is whether or not personal data is processed in the specific application. Only the operator can assess the actual effects of unauthorized access in the respective specific application.

2.1.1.1 Targets from a Product Perspective

From a product perspective, at least the following physical or logical objects can represent targets of an attack:

- Disrupt product function (restrict availability).
- Manipulate data (influencing evaluations, decisions or system behavior).
- Making data accessible to unauthorized persons (third parties).
- Access to connected other systems.

2.1.1.2 Attack Vector from Product Perspective

From a product perspective, at least the following basic mechanisms can represent targets of an attack:

- Power supply interruption:
Denial of Service (DoS) or planning of further attacks
- Access to Unsecured Interfaces:
Unauthorized operation of interfaces; multiple targets, potentially including the transmission of manipulated software/firmware
- Access to unencrypted data:
Unauthorized use, disclosure or manipulation of data
- Changes to the structure, configuration or programming of the product:
Multiple targets, potentially compromising other connected systems

2.1.2 Cybersecurity-Specific Threats

Specific threats can only be assessed with knowledge of the respective system and application. The operator must assess the threats arising from the significance of the data transmitted. Regardless of the assessment of transmitted data, basic types of threats to the specific product type can be identified.

Basic threat types specific to the product type: CC100 V2 Secure Controller

- Interference with communication in the network:
By manipulating the network address of the product, address conflicts can be created, communication interrupted or data misrouted.
- Acquisition of information about system processes:
By recording the process input or process output data, information about processes running in the system can be obtained. This knowledge makes it possible to identify additional vulnerabilities for cybersecurity attacks.
- Disrupting processes or causing damage to the system:
By manipulating process input data, the higher-level control system can be caused to generate incorrect setpoint values for decentralized automation devices. By manipulating process output data, field-level actuators can be caused to perform incorrect operations.

2.1.3 Vulnerability Assessment

Products have technical limits due to their product functions. These technical limits can represent a cybersecurity vulnerability.

If the operator compensates for these vulnerabilities with their own technical or organizational measures, the product can still be used safely.

The Cybersecurity Manual describes as targets which product features represent a known cybersecurity vulnerability if the operator does not take appropriate protective measures.

Note: The operator is responsible for evaluating all documented targets in terms of the probability of occurrence and severity of incidents and for taking appropriate measures. The vulnerability assessment must be extended to potential vulnerabilities that arise from the integration into the respective system and application.

The vulnerability assessment supports the achievement of the protection goals of data integrity, availability or confidentiality.

2.2 Vulnerabilities in Network Access

2.2.1 Vulnerabilities in Network Access – Overview

The product is intended for use in a protected network segment.

The following attacks are possible in an unprotected network segment through unauthorized access:

Data can be read out. Data can be manipulated. Data can be passed on to unauthorized persons (third parties).

The following data can be affected, for example:

- Product/device data, process data, configuration data, register data, local bus data

Configurations can be read out. Configurations can be manipulated. Configurations can be passed on to unauthorized persons (third parties).

The following configurations may be affected:

- Product/device configurations, project configurations, network configurations

Software/firmware can be read out. Software/firmware can be manipulated. Software/firmware can be passed on to unauthorized persons (third parties).

The following software/firmware can be affected:

- Product software/firmware, service/auxiliary software

Systems can be read out. Systems can be manipulated. Systems can be compromised.

The following systems may be affected:

- I/O system, other connected systems

2.2.2 PLC Functionality

The programmable logic controller (PLC) functionality supports recording of process data from sensors and control of actuators in networks.

The cybersecurity capabilities of the programmable logic controller (PLC) functionality depend on many factors.

If the programmable logic controller (PLC) functionality is not sufficiently secure, product data can be read out or manipulated by unauthorized users and/or malware.

2.2.3 Insecure Fieldbus

The fieldbus provides a wired connection between the fieldbus coupler and the bus system's sensors and actuators and provides data exchange among the components.

An insecure fieldbus lacks cybersecurity capabilities like authentication, integrity protection and encryption.

Insecure fieldbuses include Modbus TCP and BACnet.

2.2.4 Insecure Local Bus

The local bus is an internal bus that establishes the data connection between the head stations (fieldbus coupler or controller) and the I/O modules. The data is transmitted unencrypted.

The local bus establishes a direct connection among the components of an I/O system. The local bus can be extended with a connecting cable (RJ45).

The local bus lacks cybersecurity capabilities like authentication, integrity protection and encryption.

2.2.5 Root Privileges

The "root" user account has unrestricted rights.

When enabled, a "root" user account can modify a product's firmware. When enabled, a "root" user account has access to and permission to modify all of a product's functions, configurations and certificates.

An enabled "root" user account is required for accessing the product's Linux operating system.

If access to the enabled “root” user account is not sufficiently secure, unauthorized users and/or malware may be able to read information from the product or manipulate it.

2.2.6 Programmability

Product programmability allows users to program and run applications themselves, either in a runtime environment or via an operating system.

The product’s factory settings allow user-programmed applications to utilize the system resources fully.

Whether a user-programmed application has access to the system functions depends on many factors.

- The runtime environment includes resource management.

Failure to use the runtime environment’s resource management can disrupt normal operation.

One example of a runtime environment is CODESYS.

2.2.7 Engineering/Service Access

Engineering/service access is used for configuration and parameterization.

Engineering/service access requires an engineering, configuration and parameterization tool running on an external engineering device (such as a desktop or laptop).

An engineering device’s cybersecurity capabilities depend on many factors.

In particular, these include:

- The operating system
- The user rights
- If it connects to various different networks (e.g., publicly accessible networks)
- If it connects to portable data storage devices

If the engineering device is not sufficiently secure, the product data can be read out or manipulated via unauthorized users and/or malware.

2.3 Vulnerabilities in Physical Access

2.3.1 Physical Access Vulnerabilities – Overview

The product is intended for use in an area with physical access protection.

In areas without physical access protection, unauthorized access can permit the following attacks:

Connections can be interrupted or rendered inoperative, affecting product accessibility.

The following connections may be affected:

- Network connection, local bus, service interfaces

Data can be read out. Data can be manipulated. Data can be passed on to unauthorized persons (third parties).

The following data can be affected, for example:

- Product/device data, process data, configuration data, register data, local bus data

The product can be reset to the factory settings, This allows access to the product. The following settings may be affected:

- Product/device settings

Components of the modular I/O system can be switched out. Components that have been manipulated can be inserted into the system.

The following components may be affected:

- Components of the I/O system

The software/firmware can be switched out. Software/firmware that has been manipulated can be introduced into the system.

The following software/firmware may be affected:

- Software/firmware of the I/O system components

2.3.2 Service Interface

The service interface serves as a configuration, programming and firmware interface.

The configuration and programming can be read out and modified, and network settings can be made.

2.3.3 Operating Mode Switch

The operating mode switch is used to set the operating mode (STOP, RUN and RESET). STOP stops the application that is loaded. RESET resets the application.

When it is used in combination with the reset button, device settings and login credentials are reset to factory settings.

All applications and parameters are deleted.

2.3.4 Reset Button

The reset button can be used to restart the firmware.

Settings and credentials can be reverted to factory values.

When it is used in combination with the operating mode switch, device settings and login credentials are reset to factory settings.

All applications and parameters are deleted.

2.3.5 Slot for SIM card

The SIM card slot is available for inserting a SIM card. The SIM card is used for the product's GPRS connection. The GPRS connection enables remote product maintenance.

This function is not currently supported.

2.3.6 Slot for Memory Card

The memory card slot contains a memory card with specific data. A memory card can be used to transfer data, boot projects or software/firmware to the product or system.

This function is not currently supported.

2.4 Potential Targets

2.4.1 Non-Monitored Indicators

The product is intended for use in a secure operating environment.

The product is not capable of recognizing indications that a cyber attack is being prepared or carried out.

The product is not able to take sufficient countermeasures of its own when such incidents occur or operations are carried out. The lack of self-diagnostics gives attackers an opportunity to find and exploit vulnerabilities through experimentation.

Examples of indicators for planning or execution of cybersecurity attack are:

- Changed – usually increased – network activity
- Changed – usually increased – utilization of hardware
- Frequent successive changes to configurations

2.5 Hardening and Cybersecurity Capabilities

2.5.1 Defense-in-Depth Principle

The product is a device with open interfaces and ports and is intended for use in a protected network segment.

Protective measures suitable for the specific application area and application must be implemented.

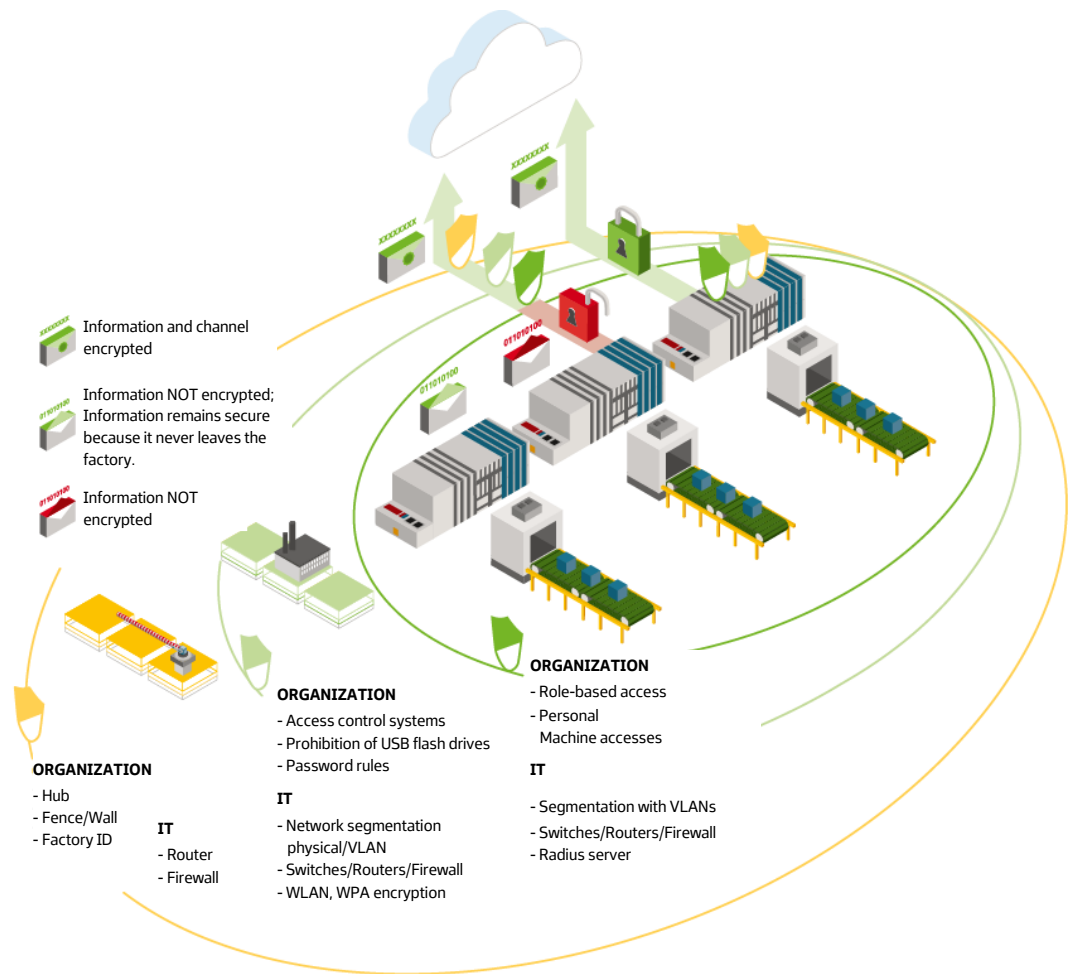


Figure 1: Onion Pattern (Example)

The system operator must combine organizational and technical security measures to successfully counter cybersecurity threats.

No single security measure offers comprehensive protection. For example, the hardness of a vault door (technical security measure) is irrelevant while the door for storage or retrieval is open (organizational security measure).

The function of some products requires that processes take place without protective measures ("safe door open") within trust boundaries or within certain periods of time. Any protective functions missing from the product must then be implemented by the operator in the operational environment for which they are responsible.

The organizational and technical security measures taken must, like the layers of an onion, envelop all vulnerable access points or transmission paths and cover all areas that could be attacked. The security measures taken must also be designed in such a way that if one measure is overcome, the other measures continue to provide protection.

To aid in the interpretation of the security architecture, this documentation contains information on the necessary measures that can be identified from the product's point of view:

 **Hardening Measures** [► 15].

2.5.2 Reference Architecture

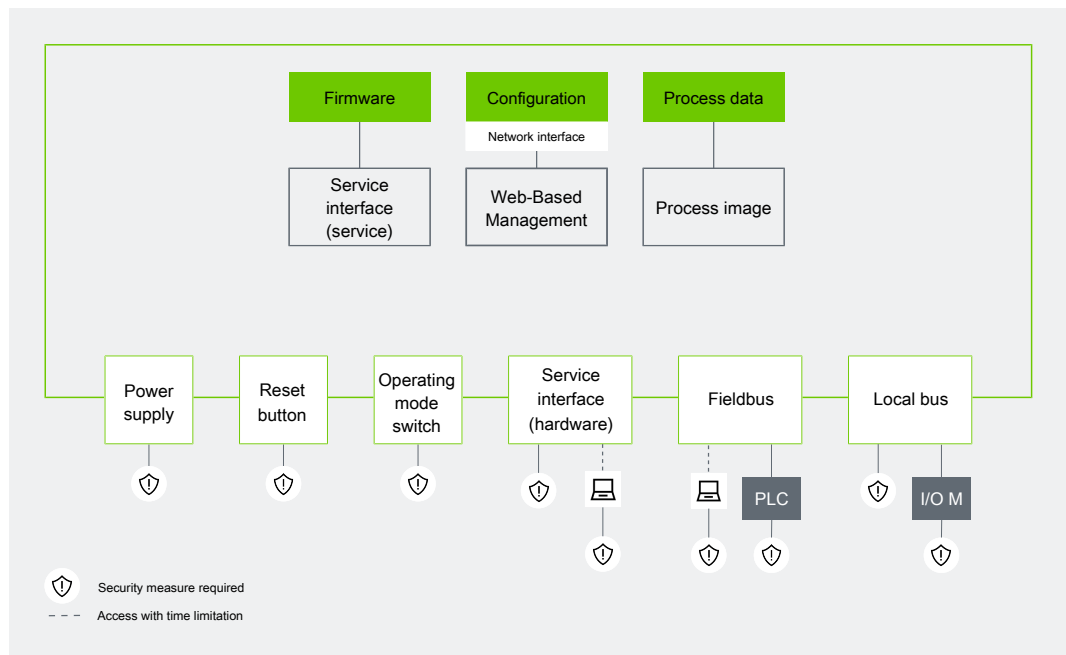


Figure 2: Reference Architecture

2.5.3 Hardening Measures

The hardening measures described are not alternatives to one another. To ensure good protection, the various hardening measures must be implemented in addition to each other.

2.5.3.1 Secure Operating Environment

The product must only be operated in a secure operating environment.

A secure operating environment helps prevent various attacks. A secure operating environment meets the following requirements at a minimum:

- Physically protected access
- Protected network segment
- Recorded access and entry
- Monitoring for suspicious events or processes

Physically protected access

The product is a device with accessible controls, ports and storage options.

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

- Access area is protected.
- Access is only granted to authorized persons.
- The extension of the local bus does not lead outside.
- Only necessary connections lead physically to the outside.

Protected Network Segment

The product is a device with open interfaces and network ports.

It may only be used in a protected network segment that meets the following requirements at a minimum:

- There is no unprotected connection to the Internet.
- There is no unprotected connection to other network segments.
- Access is authorized according to the reference architecture.
- All network devices are located in a protected network segment.

Recorded access and entry

In certain situations, the product requires temporarily reduced security. For example, temporarily reduced security may be necessary for engineering/service activities or in the event of a fault.

At a minimum, logging must capture the following events:

- Connecting an engineering device
- Access to the protected network segment (e.g., changing the limit of the protected network segment, disabling the firewall of the network)
- Access to the physically protected area (e.g., service personnel)

Monitoring for suspicious events or processes

Monitoring must cover at least the following events and processes:

- Changed, in particular suspiciously increased network activity

2.5.3.2 Secure Commissioning

Secure product commissioning helps prevent various attacks. Secure commissioning meets the following requirements at a minimum:

- Changed access data
- Protected network access
- Splitting the application program up appropriately into prioritized tasks

Access Data

- Change all freely accessible and documented access data.

The access data is freely accessible and documented in [□ Product Manual](#).

The following settings must be met at a minimum:

- Password for user account "admin" was assigned.
- Unused network ports are disabled.
- The network ports of used services are changed, provided that this can be reasonably implemented on the product itself and on the other side.
- Unused interfaces are disabled.
- Unused wireless technology is disabled.

Network Access

- Protect network access.

The following requirements must be met as a minimum:

- Functions for network protection of the product are used.
When available: e. g., MAC filter
- Secure protocol is used.
When available: e. g. HTTPS, SFTP
- Only required interfaces are enabled.
- Only required network ports are enabled.
- Only necessary services are enabled.

Splitting Up the Application Program

- Split your application program up into tasks.

The following requirements must be met as a minimum:

- Prioritization of parts of the application program
- Assignment of parts of the application program to task priorities (development environment)

2.5.3.3 Secure Operation

Secure operation of the product helps prevent various attacks. Secure operation meets the following requirements at a minimum:

- Time-limited physical access for engineering/service activities or in case of error
- Time-limited access and entry for engineering/service activities or in the event of a fault
- Security event/process logging
- Action following a security event/incident
- System integrity checks after changes
- Use of tested and current firmware/updates
- Use of tools to check cybersecurity

Access and entry for engineering/service activities or in the event of a fault

Engineering or service activities often require access to product data or configuration.

Therefore, the operator must ensure that the third-party devices used and the connection to the product are secure.

- Only grant access for a limited time.

The following forms of access must have time limitations:

- Access to communication software
- Access to interfaces
- Access with increased rights

Logging Security Incidents

- Log security events.

The following requirements for logging security events must be met as a minimum:

- The product's logging function is set up.
- Logging measures for security events that the product does not log have been set up.
- Logging measures for the network are set up.

WAGO recommends using "System Logging Protocol" (Syslog).

After a Security Incident

- Take action following a security event.

The following actions must be taken after a security event, as a minimum:

- Compare actual and setpoint configuration data.

System Integrity Checks

- Check the integrity of your system after any changes are made.

At a minimum, the following checks must be performed after configuration changes:

- Check configuration checksum

- Firewall check

Verified and current firmware (updates)

- Use only verified and current firmware (updates).

The following requirements are features of a tested and up-to-date firmware/update:

- Checksum was successfully verified (integrity check).

WAGO recommends using current firmware.

The current version of a firmware corresponds to the current state of the art and security. Previous firmware versions can present vulnerabilities in technology and security.

You can find verified current WAGO firmware (and firmware updates) and information on installation at:

🔗 <https://downloadcenter.wago.com>

For more information, please contact:

🔗 [Technical Support](#)

Aids

- Use additional tools to check security.

The following tools can help you check the cybersecurity of your system:

- System Logging Protocol (Syslog)
- Management of certificates
- WAGO IO Update 750 (upon request to Technical Support)

2.5.3.4 Secure Decommissioning

Secure product decommissioning helps prevent various attacks. Secure decommissioning meets the following requirements at a minimum:

- Deleted data in the product
- Deleted product data in the environment

Data in the Product

- Delete all data saved in the product.

The following requirements must be met as a minimum:

- Product is reset to factory settings.
- Data that cannot be deleted is overwritten (e.g., with "0").
- If there is any suspicion that sensitive data has not been deleted: Arrange for scrapping by a disposal service provider qualified in cybersecurity.

Product Data in the Environment

- Delete all data stored by the product in the environment.

The following requirements must be met as a minimum:

- Product configurations in the configuration environment must be deleted.

2.5.4 Cybersecurity Capabilities

Product Housing Protection

The product housing has a physical protection feature that indicates when it has been opened without authorization.

- The product housing comes from the factory sealed with a security seal.

Session Locking

Session locking protects against unauthorized access when inactive. A session can be locked after a configurable period of inactivity or by actively logging out. Access is restored once the user has been authenticated.

- The session lock is implemented via the operating system of the engineering device.
- The session lock on the engineering device is set up.

Secure-by-Default

Upon delivery, the firmware is secure by default. The factory settings and configurations are designed to provide the best possible protection for the product.

- The factory settings are documented.
- Settings that need to be made during commissioning are documented.

Encrypted Communication

The integrated Webserver enables encrypted communication with the product for access to the Web-Based Management.

Note: The encryption capability applies to this protocol; the product may have other protocols that do not support encryption.

Encrypted communication can be performed via the secure protocols:

- "Transport Layer Security" (TLS) allows secure HTTPS connections to be established in the network.
- "Secure Shell" (SSH) enables operation of secure shell connections (network services) in insecure networks.

Update Capability

Updates to the software/firmware can be provided that extend the product's features, improve the software/firmware or fix a security vulnerability.

- The product does not come with an automatic update function.

2.5.5 Cybersecurity Service

Current Security Vulnerabilities

- Find out more and report any current security vulnerabilities.

The following contact points can be used for information and reporting on current security vulnerabilities:

- Information about known and current security vulnerabilities can be viewed online: "Common Vulnerabilities and Exposures (CVE)," <https://cert.vde.com/de/advisories/vendor/wago/>.
- Information on Vulnerabilities of WAGO products is available from the WAGO Product Security Incident Response Team [PSIRT](#).

Cybersecurity Service Duration

- Find out the duration of the cybersecurity service for your product.

Information on the duration of the cybersecurity service can be found on the product detail page at: www.wago.com/<item number>.

3 Overview

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

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

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

4 Functions

4.1 Function Overview

The functions listed here are not included in all products.

The functions included are available in the function overview in the corresponding product manual.

The functions are described in the following sections.

System Functions

-  [User Management \[> 23\]](#)
-  [Event Logging \[> 30\]](#)
-  [Product and system status \[> 32\]](#)
-  [Real-Time Clock \[> 32\]](#)
-  [CODESYS V3 Runtime Environment \[> 33\]](#)
-  [Firmware Update \[> 35\]](#)
-  [Certificate Management \[> 35\]](#)
-  [Webserver \[> 38\]](#)
-  [Open Source Licenses \[> 40\]](#)
-  [WAGO Device Access \[> 40\]](#)
-  [Factory Reset \[> 41\]](#)

Hardware Functions

-  [Mode Selector Switch/Reset Button \[> 41\]](#)
-  [Communication Interface \[> 42\]](#)
-  [USB-C Service Port \[> 42\]](#)
-  [OnBoard I/O \[> 43\]](#)

Configuration Functions

-  [Web-based Management \(WBM\) \[> 49\]](#)

Network Functions

- Network configuration
 -  [Interface Configuration \[> 64\]](#)
 -  [Hostname/Domain Addresses \[> 66\]](#)
- Network security
 -  [Firewall \[> 68\]](#)
 -  [IPsec \[> 70\]](#)
- Network services
 -  [DHCP Client \[> 72\]](#)
 -  [SSH Service \[> 72\]](#)

Memory Functions

-  [Automount \[> 73\]](#)
-  [Data Backup \[> 73\]](#)

Diagnostic Functions

- [🔗 Diagnostics via Indicators \[► 74\]](#)
- [🔗 Diagnostics via WBM or WAGO Device Manager \[► 74\]](#)

4.2 System Functions

4.2.1 Standards Compliance

WAGO declares that the products covered by this document are IEC 62443-4-2-compliant if the requirements in section "Cybersecurity" are met.

Use of certain functions or user accounts with extensive rights (e.g., "root") may allow software modifications to be made that go beyond the declared product functions.

Therefore, WAGO revokes its declaration of compliance in such cases. Such revocation cannot be reversed.

Before it is revoked, a warning appears with a security prompt.

When the declaration is revoked, a flag is set permanently in the controller and cannot be deleted.

Note: The installer/operator is responsible for modifications to the product.

Setting the flag has the following consequences in particular:

- The controller is no longer guaranteed to be updateable.
- The installer/operator is responsible for modifying the firmware.
- The installer/operator is responsible for maintaining the controller's security features.

When the flag is set, this is indicated as follows:

- The controller is permanently marked as "non-compliant."
- This marking is indicated in the WBM or in WAGO Device Manager.

This setting can be made via WBM or WAGO Device Manager on the "Device" > "Security Compliance" page.

Table 1: "Device Status/Actions" – "Security"

Parameters/Button	Explanation	
[Resign IEC 62443-4-2]	WAGO revokes its declaration of IEC 62443-4-2 compliance. A security prompt appears. Revocation of the declaration of compliance cannot be reversed!	
IEC 62443-4-2 Compliance	Status indicator for the declaration of IEC 62443-4-2 compliance	
	false	The declaration of IEC 62443-4-2 compliance has been revoked.
	true	The declaration of IEC 62443-4-2 compliance is valid.

4.2.2 User Management

The controller lets you create user accounts with different roles and rights tailored to your operational requirements.

In order to meet security standards, each user must be an individual user account with its own password.

User accounts can be created, parameterized and managed locally or accessed from a central LDAP server.

User accounts that have been created can be disabled. This does not delete them, but prevents users from logging in.

An administrator with the appropriate role or rights can enable/disable accounts.

4.2.2.1 General Settings

4.2.2.1.1 Authentication Notice

A notice appears during authentication; the content of this notice is configurable.

It can be set by an administrator with corresponding roles and rights.

The operator must specify legally compliant notice content.

Therefore, the factory settings do not include default text.

Examples of message content:

- Only authorized persons are permitted to use this device.
- Unauthorized use of the system is prohibited and will be subject to criminal and/or civil legal penalties.
- System usage is monitored, recorded and reviewed.
- Use of the system constitutes acceptance of the above conditions.

The notice can be 2048 characters long and cannot contain any control characters besides line breaks.

4.2.2.1.2 Password Quality

For all local users, when a password is assigned, its quality is checked. Passwords that do not meet the password quality requirements are rejected.

The factory settings for password quality correspond to the guidelines and recommendations of the German Federal Office for Information Security (BSI).

You can configure the following password quality criteria according to your operational and security requirements:

- Minimum password length
- Minimum number of uppercase letters, lowercase letters, numbers and special characters

These settings can be made with the WBM or in WAGO Device Manager.

Table 2: "Settings" – "Account Management/PasswordQuality"

Parameters	Explanation
Min Length	Enter the minimum length of the password (6 ... 100; factory setting = 8)
Min Capital	Minimum number of uppercase letters (A ... Z) (0 ... 100, factory setting = 1)
Min Lowercase	Minimum number of lowercase letters (a ... z) (0 ... 100, factory setting = 1)
Min Digit	Minimum number of digits (0 ... 9) (0 ... 100, factory setting = 1)
Min Special	Minimum number of special characters () (0 ... 100, factory setting = 1)

4.2.2.1.3 Password Changes

Passwords for the following users can be changed in the WBM or in WAGO Device Manager on the "Account Management" > "Basic" page:

- Locally managed users
- Users managed via LDAP
- "admin" system user

To change these passwords, use the **[Change Password]** button in the "Device Status/Actions" area.

In the change dialog, enter the username, the old password and the new password and repeat the new password.

Table 3: "Device Status/Actions" – "Account Management"

Button	Explanation
[Change Password]	Change the password for the "admin" user or for created users The password for "root" can be changed via the [Enable Root] button.

4.2.2.2 System User Accounts

There are two permanent local "System" user accounts set up in the controller.

4.2.2.2.1 "admin" User Account

The "admin" user account is required for initial commissioning.

When the product is delivered, no password is assigned to the "admin" user account.

The first time a user logs in as "admin," a password must be assigned.

Because the "admin" user account is anonymous and not personalized, it must be disabled after initial commissioning.

The following setting can be made for the "admin" user account:

- Enable/Disabled

The account can be enabled/disabled through the WBM or in WAGO Device Manager on the "Account Management" > "Basic" page within the "Settings" area > "SystemUser 2 (admin)."

Table 4: "Settings" – "SystemUser 2 (admin)"

Parameters	Explanation
Enabled	Setting that determines whether the "admin" user account is enabled/disabled
☐	The user account is not enabled.
☒	The user account is enabled.

4.2.2.2.2 "root" User Account

The "root" user account has unrestricted rights.

By default, the "root" user account is locked and cannot be used.

To enable this account, it is necessary to revoke the declaration of IEC 62443-4-2 compliance.

Only an administrator with the corresponding role/rights can enable this user account.

This account must be assigned a password the first time it is enabled.

Since the "root" user account is anonymous and not personalized and has extensive rights, it must be disabled after use.

The following setting can be made for the "root" user account:

- Enabled/Disabled

This account can be enabled for the first time in the WBM or WAGO Device Manager on the "Account Management" > "Basic" page within the "Device Status/Actions" area.

Table 5: "Device Status/Actions" – "Account Management"

Button	Explanation
[Enable Root User].	A dialog appears with input fields for entering and repeating the password, as well as an [Enable Root User] button to activate the account.

You can also change the password later by using the [Enable Root User] button in the "Device Status/Actions" area.

You can enable/disable this account at any time in the future in the WBM or WAGO Device Manager on the "Account Management" > "Basic" page within the "Settings" area > "SystemUser 1 (root)."

Table 6: "Settings" – "SystemUser 1 (root)"

Parameters	Explanation
Enabled	Setting that determines whether the "root" user account is enabled/disabled
☐	The user account is not enabled.
☒	The user account is enabled.

If you try to enable it for the first time via "Settings," this is rejected with an error message.

4.2.2.3 Local User Management

Local user roles and user accounts are created, parameterized and managed in the controller.

They are only valid for this specific controller.

If a user is logged in and rights are assigned to them or revoked from them, the change does not take effect until the next time they log in.

4.2.2.3.1 Local User Accounts

The following settings can be made for each local user account:

- Name of the user account
- Status of the user account (enabled/disabled)
- User roles (selection from list of created user roles)
- Prompt to change password (Force Password Change)

The settings can be made with the WBM or WAGO Device Manager.

Table 7: "Settings" – "User List"

Parameters	Explanation
User list	Number of created local user accounts
User <n> (<Name>)	For each created local user account, a separate area is displayed.
Name	Enter the name of the user account
Enabled	Setting that determines whether the selected user account is enabled/disabled
☐	The user account is not enabled.
☒	The user account is enabled.

Parameters	Explanation
Roles	Assign user roles to the selected user account; list box with possible roles indicating the number of assigned user roles; when the list box is collapsed, the assigned roles appear below it. When it is expanded, a list of checkboxes for the available roles appears.
	☐ The user account does not have the selected role.
	☒ The user account has the selected role.
	<User role> Setting that determines whether the user account has the selected role
Force Password Change	Setting that determines whether the password for the selected user account must be changed during the next login
	☐ The password does not have to be changed during the next login.
	☒ The password must be changed during the next login.

4.2.2.3.2 Local User Roles

The following settings can be made for each local user role:

- Name of the user role
- Permissions (selection from list of predefined authorizations)

The settings can be made with the WBM or WAGO Device Manager.

Table 8: "Settings" – "UserRole List"

Parameters	Explanation
UserRole List	Number of local user roles that have been created
UserRole <n> (<Name>)	For each local user role that has been created, a separate area is displayed.
Name	Enter the user role name (maximum 48 characters); allowed characters: lowercase letters (a ... z), numbers (0 ... 9) and special characters (minus sign, underscore)
Permissions	Assign permissions to the selected role; list box with possible permissions indicating the number of assigned permissions; when the list box is collapsed, the assigned permissions appear below it. When it is expanded, an input field for searching and a list of checkboxes for the available permissions appear.
	☐ The user role does not have the selected permission.
	☒ The user role has the selected permission.
	<Permission> Setting that determines whether the user role has the selected permission

4.2.2.4 User Management via LDAP

LDAP user accounts are created, parameterized and managed by the LDAP administrator on a central server.

They are valid for all controllers connected to this server or a configurable subset of them.

LDAP user accounts must have at least one UID and a primary GID greater than or equal to 10000 to authenticate on the controller. This setting must be made by the LDAP administrator in the central user administration on the server.

If user management is enabled via the LDAP service, user accounts can be locked for a limited time, or locked permanently after too many failed login attempts.

The permitted number of failed attempts and the lock duration are configurable.

The LDAP administrator can configure and re-enable user accounts on the LDAP server.

LDAP user information is cached locally in the controller. Thus LDAP users can authenticate on the controller even in the event of a network failure.

Existing certificate revocation lists are not used to check the validity of the peer certificate.

The following settings can be made for the connection between the controller and the LDAP server:

- Enabled/Disabled
- Hosts
- Base DN
- Device Certificate
- Server CA
- Bind DN
- Auth Token

The settings can be made with the WBM or WAGO Device Manager.

4.2.2.5 User Login

User login is performed via a central authentication service.

All controller logins and login attempts are saved in the event log.

4.2.2.5.1 Login Window

The login window shows the device's hostname, the requesting application and the authentication notice.

The following information must be entered:

- Username
- Password

If the administrator has selected this requirement, a new password must be assigned the first time this account is logged into.

A corresponding notice appears: "Your password is expired. A password change is required."

In that case, the following information must be entered:

- Enter old password
- Enter new password
- Repeat new password

The choice of password must follow the rules from the "Password Quality" section.

During initial commissioning, a window opens for changing the "admin" account password with the following notice: "This device is in commissioning state. Please set the password for the user 'admin'."

Once a password is successfully assigned, the login window opens with the following notice: "Successfully updated password."

After a successful login attempt, the login window closes, and the application opens.

After a failed login attempt, the login window opens with the following message: "Invalid username and/or password"

To reduce the risk of attack, there is a short delay after a failed login attempt before another attempt is permitted.

The login window then reopens.

4.2.2.5.2 "OAuth2" Authentication Service

The following security settings are available for the "OAuth2" authentication service:

- Setting the validity period for newly issued refresh tokens
- Setting the validity period for newly issued access tokens
- Setting the validity period for newly issued authorization codes
- Enabling/disabling "Silent Mode"
- Invalidating all previously issued tokens
- Invalidating a specific token

The validity period and "Silent Mode" settings can be made in the WBM or in WAGO Device Manager on the "OAuth2Server" page within the "OAuth2Server" group.

Table 9: "Settings" – "OAuth2Server"

Parameters	Explanation
Auth Code Lifetime	Validity period of newly issued authorization codes (factory setting = 60 s)
Access Token Lifetime	Validity period of newly issued access tokens (factory setting = 28800 s)
Refresh Token Lifetime	Validity period of newly issued refresh tokens (factory setting = 2592000 s)
Silent Mode Enabled	Setting that determines whether the display in the login window is reduced to the fields required for login (silent mode)
	☐ Display is not reduced (factory setting).
	☒ Display is reduced to the necessary login fields.

If "Silent Mode" is enabled, the authentication service's login screen only displays the input fields required for login and does not show additional device information.

Tokens can be invalidated in the event of a problem, for example if you suspect that a token has been stolen or used elsewhere. To invalidate a specific token only, the token must be known (e.g., read out from network traffic).

It can be invalidated in the WBM or in WAGO Device Manager on the "OAuth2Server" page within the "Device Status/Actions" area.

Table 10: "Device Status/Actions" – "OAuth2Server"

Button	Explanation
[Revoke All Tokens]	Invalidates all tokens previously issued
[Revoke Token]	Invalidates a specific token The name of the token can be entered in a pop-up window. Clicking the [Revoke Token] button confirms the invalidation.

4.2.3 Event Logging

The system includes a log service which records system events in the form of log messages.

The logged events include the following:

- Actuation of the operating mode switch and reset button
- Logins and login attempts on the controller
- Write access and method calls via WdX

The event log indicates which user logged in, when they logged in, and what changes were made.

Each log message contains:

- The time
- The component name
- The log level
- The log message

The log messages are structured as follows:

Line 1: "Time # component name # log level"

Line 2: "Log message"

Example of log entries:

"Tue Sep 02 2025 09:10:09 GMT+0200 (Central European Summer Time) # xxx.service [nnn]
Informational(6)"

"OMS position: STOP"

"Tue Sep 02 2025 09:10:26 GMT+0200 (Central European Summer Time) # xxx.service [nnn]
Informational(6)"

"OMS position: RUN"

The controller's event log can be accessed in the WBM and in WAGO Device Manager via the "Device Log" item in the menu ribbon.

The event logging settings can be made in the WBM and in WAGO Device Manager on the "Logging" or "Remote Logging" page (see the following sections).

In order to provide a verifiable event log (audit log), the timestamps must correspond to the actual time. This requires correct settings for the controller's time and time zone.

The corresponding settings are described in section [Real-Time Clock \[► 32\]](#).

4.2.3.1 Internal Log Memory (Logging)

The size of the log memory must be adapted to the operational requirements during commissioning.

The following are configurable:

- The minimum log level
- The maximum log memory size

If the maximum size setting is exceeded, the oldest messages are discarded.

These logging settings can be modified in the WBM or in WAGO Device Manager under "Settings" on the "Logging" page.

Table 11: "Settings" – "Logging"

Parameters	Explanation	
Min Log Level	Minimum log level	
	Error	Only error messages are logged.

Parameters	Explanation	
	Warning	Warnings and error messages are logged.
	Notice	Notices, warnings and error messages are logged.
	Informational	Information messages, notes, warnings and error messages are logged; factory setting
	Debug	All events and messages are logged.
Disk Usage Limit	Maximum log memory size; (default: 50 MiB)	

"Device Status/Actions" shows the current size of the log memory.

4.2.3.2 External Log Server (Remote Logging)

The log system in the firmware cannot detect log message manipulation. If you need to protect the logging data (against change/deletion/loss), it can be sent via remote logging to a central log server that meets this requirement.

Storing log data on a central log server allows backup of large data volumes and analysis of log data (intrusion detection system, security information and event management, etc.).

The remote storage settings can be modified in the WBM or in WAGO Device Manager under "Settings" on the "Remote Logging" page.

Table 12: "Settings" – "RsyslogClientConfig 1"

Parameter	Meaning	
Enabled	Enable/disable remote logging	
	☐	Remote logging is disabled.
	☒	Remote logging is enabled.
Target	Destination address of the remote logging server	
Port	Destination port of the remote logging server	
Transport Protocol	Select protocol	
	UDP	UDP is enabled.
	TCP	TCP is enabled.
Device Certificate	Select device certificate; this drop-down menu is only enabled if the TCP protocol is enabled.	
CA Certificate	Select CA certificate; this drop-down menu is only enabled if the TCP protocol is enabled.	
Server TLS Enabled	Enable/disable server TLS	
	☐	Server TLS is disabled.
	☒	Server TLS is enabled.
Server TLS Authentication	Select authentication method; this drop-down menu is only enabled if Server TLS is enabled.	
	NoAuthentication	No server authentication
	Fingerprint	Authenticate server by certificate fingerprint
	SubjectAlternative-Name	Authenticate server by certificate subject alternative name (common name)
Server Certificate Fingerprint Hash Algorithm	Select hash algorithm; this drop-down menu is only enabled if Server TLS is enabled and "Fingerprint" is selected as the authentication method.	
	SHA1	SHA1 is enabled.

Parameter	Meaning	
	SHA256	SHA256 is enabled.
Server Certificate Fingerprint	Enter certificate fingerprint This input field is only enabled if Server TLS is enabled and "Fingerprint" is selected as the authentication method.	

4.2.4 Product and system status

Product and system status information is displayed on the WBM "Information" page:

The **[Calculate Config Checksum]** button starts the calculation of the checksum for the configuration. After the calculation, the checksum appears in a separate window.

The product properties appear in the "Device Status/Actions" area in the "Identity" group:

Table 13: "Device Status/Actions" – "Identity"

Parameters	Explanation
Order Number	Product item number
Description	Product designation
Serial Number (UII)	Unique product identification number

The product versions appear in the "Device Status/Actions" area in the "Versions" group:

Table 14: "Device Status/Actions" – "Version"

Parameters	Explanation
Firmware Version	Firmware version
Software Release Index	Software version
Hardware Release Index	Hardware version

4.2.5 Real-Time Clock

In order to provide a verifiable event log (audit log), the timestamps must correspond to the actual time. This requires the time and time zone to be set.

The corresponding settings are also required for the use of certificates.

To keep the time for timestamps on the device up to date, it is necessary to enable system time synchronization via time server (e.g., NTP). NTP is disabled by default.

NTP is an insecure protocol (no authentication and authorization required). Therefore, if NTP is used, the network must be protected accordingly to prevent manipulation of the time settings on the controller.

4.2.5.1 Display/Manual Setting

The time zone can be selected in the WBM or in WAGO Device Manager on the "System-Time" page within the "Settings" area.

Table 15: "Settings" – "Time Zone"

Parameters	Explanation
Time Zone	Select time zone; the list contains different locations / capital cities. Selecting one applies the correct time zone settings.

The current system date and time (UTC and local) appear in the WBM or WAGO Device Manager on the "SystemTime" page within the "Device Status/Actions" area. If no time server is available, the date and time can be set manually.

UTC

Table 16: "Device Status/Actions" – "UTC"

Parameters	Explanation	
System Time (UTC)	GMT date and time	
	[Change]	Opens a dialog for entering the date and time

Local Device Time

Table 17: "Device Status/Actions" – "Local Device Time"

Parameters	Explanation	
System Time (local device time)	Local date and time	
	[Change]	Opens a dialog for entering the date and time

4.2.5.2 Automatic Setting

Table 18: "Settings" – "NTPClient"

Parameters	Explanation	
Enabled	Enable/disable automatic time update	
	☐	Time update is disabled; default setting
	☒	Time update is enabled
Configured Time Server	Enter the IP addresses of the time servers; you can specify up to four time servers in a comma-separated list.	
Configured Pools	Enter the IP addresses of the time pools; you can specify up to four time pools in a comma-separated list.	

4.2.6 CODESYS V3 Runtime Environment

Note

Read CODESYS V3 documentation!

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

Note

Close any ports and services that you do not need!

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

1. To reduce the risk of cyber attacks and increase cybersecurity, close all ports and services not required by your application in the control components.
2. Only open ports and services during commissioning and/or configuration.

4.2.6.1 Memory Areas under CODESYS V3

4.2.6.1.1 Program and Data Memory

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

4.2.6.1.2 Flag Area (Memory) and Retain Area

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

4.2.6.2 CODESYS Web Visualization

The CODESYS Web visualization can be accessed at "https://<ip-address>/webvisu/web-visu.htm."

For security reasons, the port of the CODESYS Webserver (port 58080) cannot be addressed directly, but is redirected via the central Webserver.

4.2.6.3 Security Settings in CODESYS

Some security-related settings cannot be made in the controller and must instead be made in the CODESYS development environment.

4.2.6.3.1 Secure Communication between Development Environment and Controller

Communication between the CODESYS development environment and the controller is unencrypted by default and must be secured.

Configuration changes, such as adding certificates and forcing encryption, can secure communication between the development environment and controller.

These settings are not made in the WBM or in WAGO Device Manager, but rather in CODESYS.

For more information, see "Encrypting Communication, Changing Security Settings" in the online help for CODESYS.

Physical protection can be implemented through use in a secure environment or secure communication via VPN.

4.2.6.3.2 Integrity of the Transferred Project Files

Know-how protection and copy protection of a boot application can be achieved with the help of controller-specific license management and the app settings in the application's object properties.

The download code and boot application can be encrypted and signed.

These settings are not made in the WBM or WAGO Device Manager, but rather in CODESYS. For more information, see "Protecting an Application" in the online help for CODESYS.

4.2.7 Firmware Update

The device can be updated via the integrated WBM or the "WAGO Device Manager" software.

This process uses an update bundle, which is a file containing everything that will be updated.

The device must not be switched off during the update process; if it is, its functionality can no longer be guaranteed.

During the firmware update, the update bundle is copied to the device and checked for compatibility, integrity and authenticity.

The system update then begins.

During the firmware update, the "SYS" LED flashes, alternating between red and green.

When the firmware is updated, the configuration settings are retained as long as they are still compatible.

The event log records important events that occur during the firmware update (including start, end and possible causes of error).

If an error occurs during the firmware update, the device is rolled back to the state before the update.

4.2.7.1 Signatures and Certificates for Update Bundle

The update bundle is protected by digital signatures to ensure the authenticity and integrity of the update bundle:

- The authenticity check verifies that the update bundle originates from the entity that claims to have created it (e.g., from WAGO).
- The integrity check verifies that the update bundle has not been modified during transmission.

In the factory settings, the signatures for this check are set in such a way that only update bundles created by WAGO are accepted.

To ensure secure device operation, WAGO recommends retaining the factory settings and not changing them.

Any changes you make are at your own risk – WAGO assumes no liability in such cases!

If changes are required, e.g., to use update bundles or firmware versions not supplied by WAGO, the following settings can be made:

- Bundle – certificate used to check the update bundle as a whole
- Firmware – certificate used to check the firmware contained in the update bundle

These settings can be made with the WBM or WAGO Device Manager.

4.2.8 Certificate Management

When device certificates are uploaded, the key length or parameters of the EC curve are compared with the minimum requirements of the BSI-TR-02102-2.

The minimum requirements are:

- RSA key length:
 - 2048 bit (TPM and software)
 - 4096 bit (software only)

- Parameters of the EC curve:
 - SECP256R1 (= prime256V1)
 - secp384r1
 - secp521r1

An RSA key length of 2048 bits is accepted because the current TPM2 (per the TPM specification) only supports one 2048 bit RSA key.

Device certificates that do not meet the above requirements cannot be generated; if such certificates are uploaded, they are rejected.

4.2.8.1 Truststore

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

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

Table 19: "Settings" – "CertStore/CA"

Parameters	Explanation	
Trust Public	Determines whether publicly trusted certificates are trusted	
	☐	Publicly trusted certificates are not trusted.
	☒	Publicly trusted certificates are trusted.

Table 20: "Settings" – "CACertificate List"

Parameters	Explanation	
CACertificate List	Number of configured CA certificates	
CACertificate <n>	For each CA certificate, a dedicated group is displayed.	
Certificate	Add or remove a CA certificate	
	Not set	No CA certificate has been added yet.
	<certificate name>	Name of the added CA certificate
	Select	Download a CA certificate from the computer
	Remove file from device	Remove the CA certificate from the controller
Comment	Enter a comment to use as the certificate name	
Trusted	Setting that determines whether the CA certificate is trusted	
	☐	The CA certificate is not trusted.
	☒	The CA certificate is trusted.

Table 21: "Settings" – "CertificateRevocationList List"

Parameters	Explanation
CertificateRevocationList List	Number of configured lists
CertificateRevocationList <n>	For each CertificateRevocationList, a separate list is displayed.
URL	Enter the URL for the list

Table 22: "Device Status/Actions" – "CertificateRevocationList List"

Parameters	Explanation
CertificateRevocationList List	Number of configured lists
CertificateRevocationList <n>	For each CertificateRevocationList, a separate list is displayed.
Expiration	Expiration date of the list; if the list is not found or cannot be downloaded, "empty" appears here.

4.2.8.2 Device Certificates

Table 23: "Settings" – "DeviceCertificate List"

Parameters	Explanation	
DeviceCertificate list	Number of device certificates	
DeviceCertificate <n>	For each certificate, a separate area is displayed.	
Certificate	Add or remove a device certificate file	
	Not set	No device certificate file has been added yet.
	<certificate name>	Name of the added device certificate file
	Select	Download a device certificate file from the computer
	Remove file from device	Remove the device certificate file from the controller
Comment	Enter a comment to use as the certificate name	
Private Key	Add or remove an associated private key file	
	Not set	No key file has been added yet.
	<Key>	Name of the added key file
	Select	Download a key file from the computer
	Remove file from device	Remove the key file from the controller
Automatic Renewal	Setting that determines whether the certificate is automatically renewed	
	☐	The certificate is not automatically renewed.
	☒	The certificate is automatically renewed.

Table 24: "Settings" – "CertStore/EnrollmentServer"

Parameters	Explanation	
Host	Enter the hostname of the enrollment server	
Auth User	Enter the username for the connection to the enrollment server	
Auth Password	Enter the password for the connection to the enrollment server	
Verbose	Setting that determines whether extended information about the connection is logged	
	☐	Extended information is not logged.
	☒	Extended information is logged.
Verify Host	Setting that determines whether the hostname is verified	
	☐	The hostname is not verified.
	☒	The hostname is verified.
CA Certificate	Select the CA certificate for verification	

Table 25: "Device Status/Actions" – "CertStore/Device"

Parameters	Explanation	
CertStore/Device	[Create Certificate]	Generate a certificate on the device.
	[Create Certificate With Enrollment]	Generate a certificate on the device that can optionally be signed and/or updated by the enrollment server.

Table 26: "Device Status/Actions" – "DeviceCertificate List"

Parameters	Explanation	
DeviceCertificate list	Number of certificates generated on the device	
DeviceCertificate <n> (<Name>)	For each certificate, a separate line is displayed.	
	[Create Signing Request]	Create a text file that can be used for signing.

Table 27: "Device Status/Actions" – "IdentityCertificate <n>"

Parameters	Explanation	
IdentityCertificate <n> (Factory provided device identity)	For each identity certificate, a separate area is displayed.	
Certificate	Size of the certificate file	
		Download the certificate file
	If no file exists, "empty" is displayed here.	

4.2.9 Webserver

The firmware contains a Lighttpd Webserver.

The Webserver configuration includes various security features. If users make unauthorized changes to the configuration, this can decrease security.

The controller's default settings allow strong encryption, but only use simple authentication methods. Since authentication plays a key role in all secure communication channels, using secure authentication is strongly recommended. The security certificate stored on the controller is the basis for authentication.

By default, the controller uses a generic security certificate in x509 format (default certificate). To enable secure authentication, you must replace this default certificate with a specific certificate for the individual device.

To do so, you must load a corresponding certificate onto the device via the truststore or use a device certificate generated in the device.

The Webserver must then be configured to use this certificate.

If this is done, the Webserver can be operated securely in accordance with the security requirements.

The settings can be made via the WBM or WAGO Device Manager.

Table 28: "Settings" – "Webserver"

Parameters	Explanation	
Default Application	Here you can select the application that is displayed when only the product's IP address is entered	
	Web-Based Management	The Web-Based Management is displayed.
	Web Visualization	The Web visualization is displayed.

Parameters	Explanation
Server Certificate	Here you can select the server certificate for authentication from a list of certificates stored on the device

4.2.9.1 CORS Policy

The CORS policy determines which browser applications are permitted cross-origin access to the controller's REST API.

It can be set via the WBM or in WAGO Device Manager on the "System" > "Webserver" page.

Table 29: "Settings" – "Webserver Application <n>"

Parameters	Explanation
Use Separated Ports	This setting determines whether separate ports are used for the selected Webserver application. This checkbox is only visible and active for Webserver application 2 (Web Visualization). ☐ No separate ports are used for Web visualization. ☒ Separate ports are used for Web visualization. The port numbers are configurable.
HTTP Port	Here you can enter the port number for the HTTP port. This input field is only visible and active for Webserver application 2 (Web Visualization) if separate ports are used.
HTTPS Port	Here you can enter the port number for the HTTPS port. This input field is only visible and active for Webserver application 2 (Web Visualization) if separate ports are used.
CORS Policy	Here you can select the origins that are allowed to make cross-origin requests to the REST API. This drop-down menu is only visible and active for Webserver applications 2 and 3 (WAGO Auth-Service and WAGO Device Access). Allow all Cross-origin access to the REST API is permitted from all origins. Allow all origins and null In addition to all normal origins, a value of "null" is also allowed; some browsers use this to indicate that the website is hosted by a local file system. Allow origins from whitelist Only origins in the whitelist are allowed REST API access. Note: If this setting is chosen, it is essential to enter your application's origin in the whitelist; otherwise, the browser will block access to the REST API. None (empty) The Webserver instructs the browser not to perform any cross-origin access at all.

Additional settings may be available for the CORS policy.

Table 30: "Settings" – "Webserver CORS Policy <n>"

Parameters	Explanation
Name	Name of the CORS policy (fixed setting)
Max Age	Maximum lifetime of the CORS policy (fixed setting)
Allowed Origins	Here you can enter a comma-separated list of the origins of applications that are permitted cross-origin access to the REST API. This input field is only visible and active for the CORS policy "Allow origins from whitelist."

4.2.10 Open Source Licenses

Table 31: "Device Status/Actions" – "FOSS Module List"

Parameters	Explanation
FOSS module list	Number of available FOSS modules
FOSS Module <n> (<Name>)	For each list entry, a separate area is displayed.
Name	Name of the selected FOSS module
Version	Version of the selected FOSS module
Vendor	Creator of the selected FOSS module
License Info	Size of the selected FOSS module and download button
	 Download the license information as a text file

4.2.11 WAGO Device Access

WAGO Device Access (WDA) is a central service in the system used to access the device configuration and its settings.

This service provides a REST API via HTTP. The WDA REST API can be accessed at "https://<IP>/wda" or "https://<controller hostname>/wda."

Online documentation in English for your installed version is available at "https://<IP>/openapi/wda.openapi.html" or "https://<controller hostname>/openapi/wda.openapi.html." You can access the online documentation through the address line of the Web browser on the connected computer.

4.2.11.1 Device Scan

After a device scan, the controller returns the following device information:

- The item number
- The firmware version

If authentication-free device scan is enabled, this information can be retrieved without authentication.

This option reduces device security. Authentication is required in the factory settings.

This setting can be made in the WBM or in WAGO Device Manager on the "WAGODeviceAccess" page.

Table 32: "Settings" – "WAGODeviceAccess"

Parameters	Explanation
Allowed Unauthenticated Requests	Drop-down menu with possible entries indicating the enabled entries; when the drop-down menu is collapsed, the enabled entries are displayed below it. When it is expanded, a list of checkboxes for each entry is displayed.
	☐ Scanning is only possible with authentication.
	☒ Scanning is possible without authentication.
	ScanDevices Setting that determines whether devices can be scanned without authentication

4.2.12 Factory Reset

Note

All parameters and passwords are overwritten!

The reset overwrites all parameters and passwords.

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

Firmware functions that were installed later are deleted.

Software licenses are deleted.

- If you have any questions, contact WAGO Support.

The controller can be reset to factory settings via the WBM or in WAGO Device Manager on the "System" > "Factory Reset" page.

Table 33: "Device Status/Actions" – "Factory Settings"

Button	Explanation
[Reset]	The controller is reset to the factory settings.

Alternatively, you can also use the operating mode switch and the reset button to reset it as described in section [Factory Reset \[► 87\]](#).

4.3 Hardware Functions

4.3.1 Mode Selector Switch/Reset Button

Operating mode switch and reset button actuation events are saved in the event log. This allows unauthorized actions to be tracked according to security guidelines.

4.3.1.1 Operating Mode Switch

Table 34: Operating mode switch

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

Other functions can also be triggered with the reset button.

Each actuation of the operating mode switch is recorded in the log system if the switch changes to a new position (event logging).

Example of Log Entries for Operating Mode Switch:

```
Mar 10 13:29:05 wago-cc100 mcid[450]: OMS position: RUN
Mar 10 13:30:09 wago-cc100 mcid[450]: OMS position: STOP
Mar 10 13:30:11 wago-cc100 mcid[450]: OMS position: RESET
```

4.3.1.2 Reset Button

Additional functions can be triggered in combination with the operating mode switch.

Table 35: Reset Button

Operating Mode Switch Position	Duration of Reset Button Actuation	Function
RUN or STOP	1 ... 8 seconds	Software reset; the controller restarts. 🔗 Software Reset (Restart) [► 86]
RESET	> 8 seconds	Factory reset; the controller is reset to the factory settings, and all parameters are deleted. 🔗 Factory Reset [► 87]

Each reset button action (press or release) is recorded in the log system (event logging).

Example of Log Entries for the Reset Button:

```
Mar 10 13:30:39 wago-cc100 mcid[450]: Button RESET_ALL: PRESSED
Mar 10 13:30:39 wago-cc100 mcid[450]: Button RESET_ALL: RELEASED
```

4.3.2 Communication Interface

Communication via standard serial protocols is insecure, and there are no protocol mechanisms for protection.

To meet security requirements, the operator must provide physical protection (e.g., protected wiring, protection against unauthorized physical access, etc.).

4.3.3 USB-C Service Port

The service port is designed as a USB-C port and works as a network interface with the IP address 192.168.42.42.

The service port can be used for configuration and servicing purposes.

To meet security requirements, connection via the service port can be blocked by switching off the service port when not in use.

Note

If all interfaces are switched off, you may be locked out!

If all network interfaces and the USB-C service port are switched off, the device will no longer be accessible.

This configuration can only be reversed by resetting to the factory settings.

The service port is only disabled and re-enabled after the device restarts.

This setting can be made in the WBM or in WAGO Device Manager on the "Interfaces" page > "USB Service Interface."

Table 36: "Settings" – "USB Service Interface"

Parameters	Explanation	
Enabled	Enable/disable USB service interface	
	☐	The USB service interface is not active.
	☒	The USB service interface is active.

4.3.4 OnBoard I/O

4.3.4.1 Analog Inputs AI1, AI2

Table 37: Process Image - Analog Inputs AI1, AI2

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

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

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

The following measurement ranges can be configured:

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

4.3.4.1.1 AI 0 ... 10 V

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

Table 38: Process Image – Process Values AI; 0 ... 10 V; 16 Bit; WORD

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

4.3.4.1.2 AI -10 ... 10 V

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

Table 39: Process Image – Process Values AI; -10 ... +10 V; 16 Bit; WORD

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

4.3.4.1.3 AI 0 ... 20 mA

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

Table 40: Process Image – Process Values AI; 0 ... 20 mA; 16 Bit; WORD

Measured Value	Value Range		
	Hex.	Dec.	Bin.
< 0 mA	0x0000	0	0000.0000.0000.0000

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

4.3.4.1.4 AI 4 ... 20 mA

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

Table 41: Process Image – Process Values AI; 4 ... 20 mA; 16 Bit; WORD

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

4.3.4.1.5 AI 3.6 ... 21 mA

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

Table 42: Process Image – Process Values AI; 3.6 ... 21 mA; 16 Bit; WORD

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

4.3.4.2 Analog Inputs/Outputs AIO1, AIO2

Table 43: Process Image – Analog Inputs/Outputs AIO1, AIO2

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

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

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

The following measurement ranges can be configured:

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

- –12 ... +12 V
- 0 ... 20 mA
- 0 ... 22 mA
- 4 ... 20 mA

4.3.4.2.1 AI 0 ... 10 V, –10 ... +10 V, 0 ... 20 mA, 4 ... 20 mA, 3.6 ... 21 mA

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

4.3.4.2.2 AO 0 ... 10 V

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

Table 44: Process Image – Process Values AO; 0 ... 10 V; 16 Bit; WORD

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

4.3.4.2.3 AO –10 ... +10 V

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

Table 45: Process Image – Process Values AO; –10 ... +10 V; 16 Bit; WORD

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

4.3.4.2.4 AO –12 ... +12 V

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

Table 46: Process Image – Process Values AO; –12 ... +12 V; 16 Bit; WORD

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

4.3.4.2.5 AO 0 ... 20 mA

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

Table 47: Process Image – Process Values AO; 0 ... 20 mA; 16 Bit; WORD

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

4.3.4.2.6 AO 0 ... 22 mA

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

Table 48: Process Image – Process Values AO; 0 ... 22 mA; 16 Bit; WORD

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

4.3.4.2.7 AO 4 ... 20 mA

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

Table 49: Process Image – Process Values AO; 4 ... 20 mA; 16 Bit; WORD

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

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

Table 50: Process Image – Temperature Inputs PT1+/PT1–, PT2+/PT2–

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

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

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

The following measurement ranges can be configured:

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

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

4.3.4.3.1 Pt100, Pt200, Pt500, Pt1000

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

The resolution is 1 digit per 0.1 °C.

Table 51: Process Image – Process Values RTD; Pt100, Pt200, Pt500, Pt1000; –200 ... +850 °C; 16 Bit; INT

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

4.3.4.3.2 Ni100, Ni1000 (TK6180), Ni1000 (TK5000)

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

The resolution is 1 digit per 0.1 °C.

Table 52: Process Image – Process Values RTD; Ni100, Ni1000 (TK6180), Ni1000 (TK5000); –60 ... +250 °C; 16 Bit; INT

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

4.3.4.3.3 Ni120

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

The resolution is 1 digit per 0.1 °C.

Table 53: Process Image – Process Values RTD; Ni120; –80 ... +260 °C; 16 Bit; INT

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

4.3.4.3.4 Potentiometer 0 ... 1.2 kOhm

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

The resolution is 1 digit per 0.05 Ohm.

Table 54: Process Image – Process Values RTD; Potentiometer; 0 ... 1200 Ohm; 16 Bit; INT

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

4.3.4.3.5 Potentiometer 0 ... 5 kOhm

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

The resolution is 1 digit per 0.2 Ohm.

Table 55: Process Image – Process Values RTD; Potentiometer; 0 ... 5000 Ohm; 16 Bit; INT

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

4.3.4.4 Digital Inputs DI

Table 56: Process Image – Digital Inputs DI1 ... DI8

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

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

Table 57: Process Image – Process Values of Digital Inputs – BOOL

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

4.3.4.5 Digital Inputs/Outputs DIO

Table 58: Process Image – Digital Inputs/Outputs DIO1 ... DIO8

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

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

4.3.4.5.1 DI 0/24 V

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

Table 59: Process Image – Process Values of Digital Inputs – BOOL

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

4.3.4.5.2 DO 0/24V

Table 60: Process Image – Process Values, Digital Outputs – BOOL

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

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

4.4 Configuration Functions

4.4.1 Web-based Management (WBM)

The figures in the following sections are for illustration purposes and may differ from the actual design of the products.

The graphical user interface has the following structure:

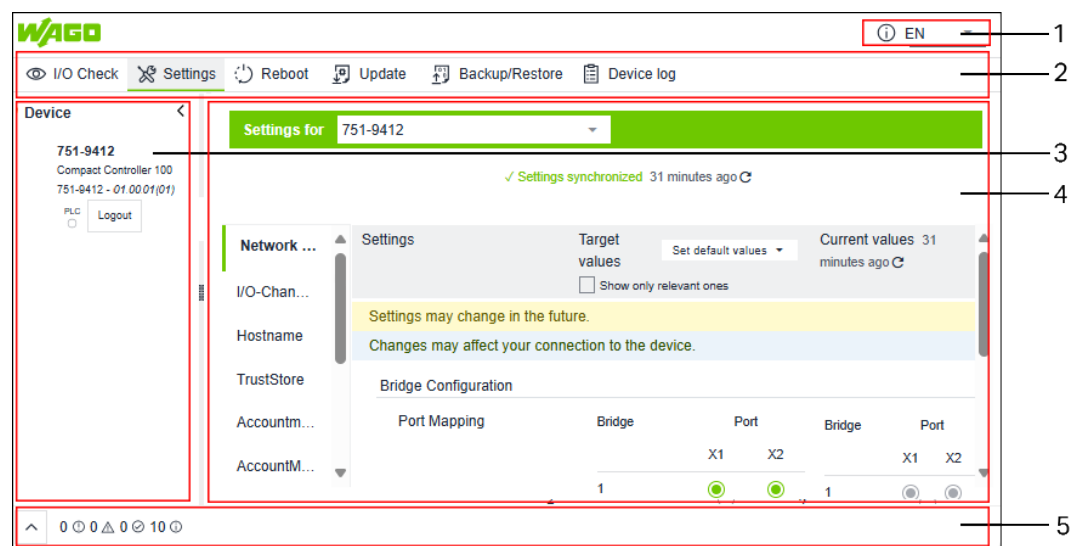


Figure 3: Graphical User Interface

4.4.1.1 General Controls

The following controls are used to make general settings and display information about the WBM:

Control	Description
	Displays general contact and program information: WAGO and Support Contact Information , WAGO software license terms, Imprint , Data Protection , GTC , Legal Information and the WBM program version
DE 	Switches the user interface language between German, English and French.

4.4.1.2 Ribbon (Device Actions)

The following device actions can be executed from the ribbon:

Icon	Function	Description
	I/O Check	Opens the "I/O Check" view in the workspace and displays the device used. The status of the device and connected channels is signaled by LED indicators. A wiring test can be performed via control mode.
	Settings	Opens the "Settings" view in the workspace. This view can be used to parameterize and configure the selected device.
	Restart	Opens the "Restart" view in the workspace. In this view, you can restart the device used.
	Firmware	Opens the "Firmware" view in the workspace. In this view, the firmware of the device used appears and can be replaced with different firmware.
	Backup/Restore	Opens the "Backup/Restore" view in the workspace. In this view, device data can be saved to a file (backup), or saved backup files can be loaded onto a device (restore).
	Device Log	Opens the "Device Log" view in the workspace. In this view, you can view device log entries.

4.4.1.3 Device

The "Device" area shows the connected device.

It displays device information, connection and status information and a button for disconnecting the connection.

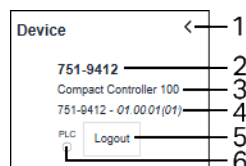


Figure 4: Connected Device

No.	Description
1	Expand/collapse the view
2	Name of the device Once the device is connected, the item number is used as the device name.
3	Item description of the device
4	Item number and device firmware version
5	[Logout] Button to log out of the device
6	The following LED indicates the status of the PLC application of a device connected online. PLC ☐ No application present ☒ Application running or application stopped in debug mode ☐ Application halted, not configured, in error state or in unknown state

No.	Description
	Notes: - For detailed LED displays, see Device View or Settings > "LEDs" tab. - For an explanation of LED displays and blink codes, see the product manual or function manual for the connected device.

4.4.1.4 Workspace

The workspace includes the right part of the window below the menu ribbon.

When a selection is made in the menu ribbon, the corresponding content opens for editing. However, what is selected in the workspace does not affect what the menu ribbon selection.

The different views of the workspace depending on the activity are described below.

4.4.1.4.1 I/O Check

Based on the device view, wiring tests can be carried out for conventional, analog and digital inputs/outputs of a device, for example by setting output signals for test purposes (see also Performing Device Diagnostics).

Note

Not all devices support testing of inputs and outputs

Please note that not all devices support testing of inputs and outputs. Only the device view with the status indicators is available for these devices.

The device hardware used is visually displayed in the upper area of the "I/O Check" view. The LED indicators on the left show the status of the device and the LED indicators on the right show the status of the channels.

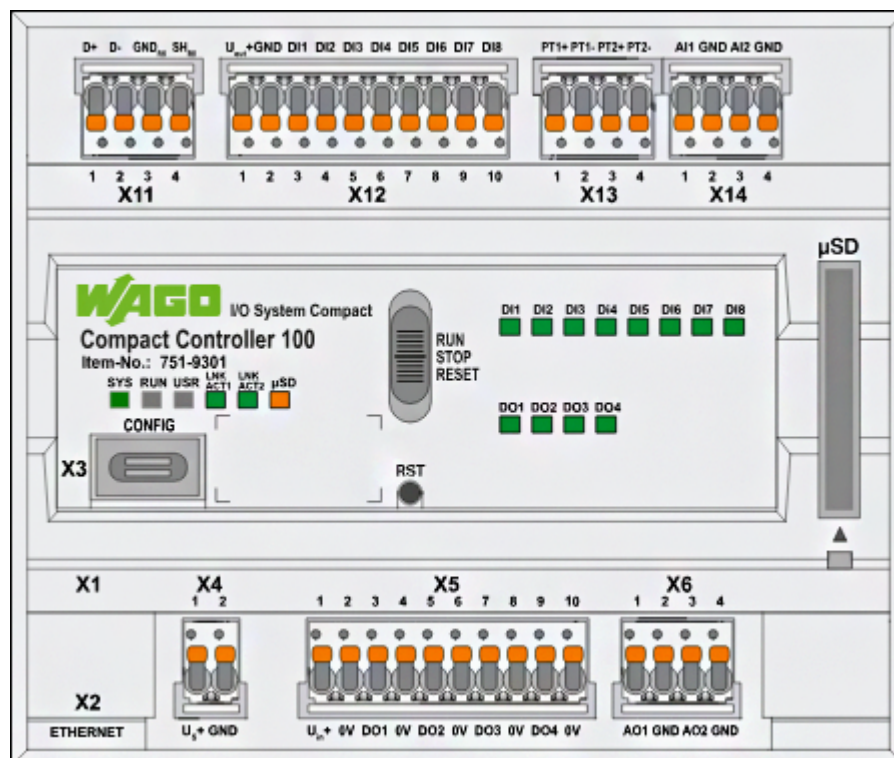


Figure 5: "I/O Check" View (Example)

Device Status Indicators

The head station status indicators are always enabled. You cannot click on the LED indicators in the graphic, but if you hover the mouse cursor over them, they show the current status message of the head station.

Note

Flash codes are not displayed in real frequency

Note that the flash codes are not displayed in real frequency. Detailed descriptions of the diagnostic messages and flash codes can be found in the manual for the respective product.



Figure 6: Device Status Indicators (Example)

Channel Status Indicators

The status indicators for the connected channels do not show the current status (read-only) of the digital inputs and outputs in permanent fashion, but only in monitor mode. Monitor mode is enabled if there is an online connection to the device.

Note

LED status refers to on/off status values related to digital I/O channels

For diagnostic channels, the physical LED indicators may consist of several status values. The LED status displayed here only refers to on/off status values directly related to digital I/O channels.

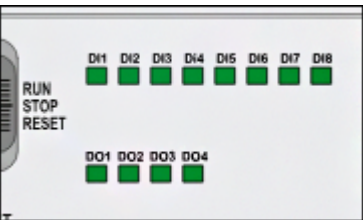


Figure 7: Channel Status Indicators (Example)

Clicking on the eye icon below the respective device displays tables with status values for the channels of the inputs and outputs used. The indicator can be switched between control and monitor mode.

Control	Description
	Zoom in Enlarges the device view by one level with each click.

Control	Description
	Zoom out Reduces the device view by one level with each click.
	Original size Shows the device view in its original size.
	Adjusts the size of the displayed areas The area between the device view and the tables with status values can be adjusted by moving the separator.
	Tables with status values hidden When you open the device view, the tables with status values for input/output channels are initially hidden. By clicking on the grayed-out eye icon, the tables below the device graphic are displayed.
	Tables with status values displayed Clicking the eye icon again hides the tables displayed for the status channels.
	Switches directly to the settings of the I/O channels Jumps to the "Settings" view > "I/O-Channels" tab and in the tab to the first configurable channel composition.
 Control mode	Control mode enabled When control mode is enabled, the channels are unlocked for changes. Values can be written.
 Control mode	Monitor mode enabled When control mode is disabled, the current status values are displayed (read access only).

The latency is also displayed, i.e., the update cycle (in s) of the displayed device values depending on the connection, device load or other factors:

Display	Description
 Monitoring active	Low latency, high synchronization rate
 Monitoring active	Higher latency, delayed synchronization rate
 Connection unstable	High latency, unstable connection

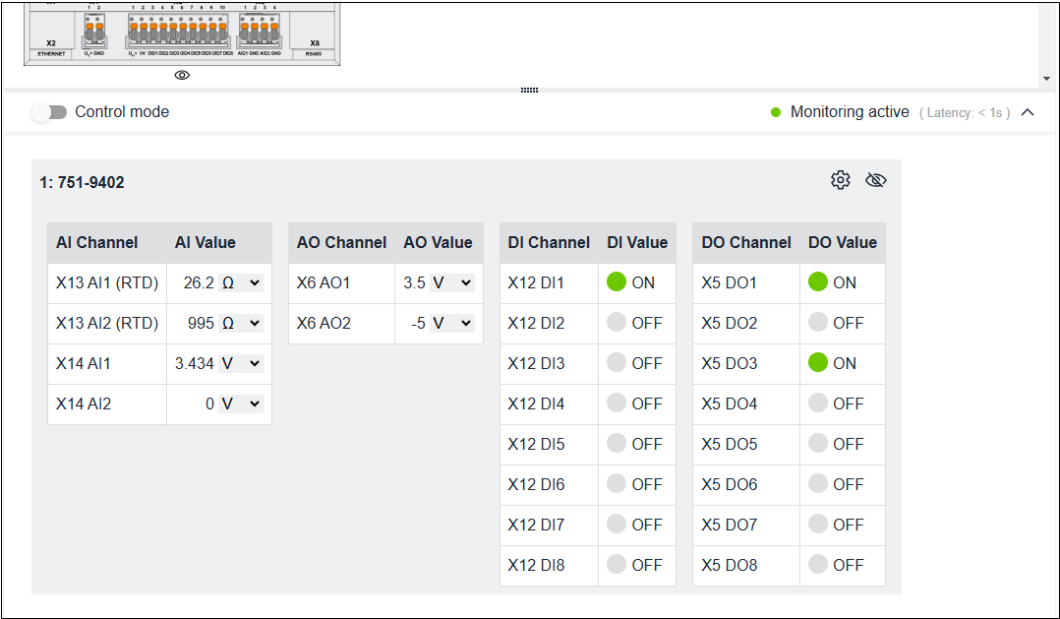


Figure 8: Monitoring active (Example)

Display/setting of status values

Status values can be shown as follows using selection fields:

- as raw values or
- as scaled values with units.

Scaled representations can only be set on the user interface; raw values are still used for communication.

Sliders can be used to set digital values:

- Switch setting  corresponds to 1 or true
- Switch setting  corresponds to 0 or false

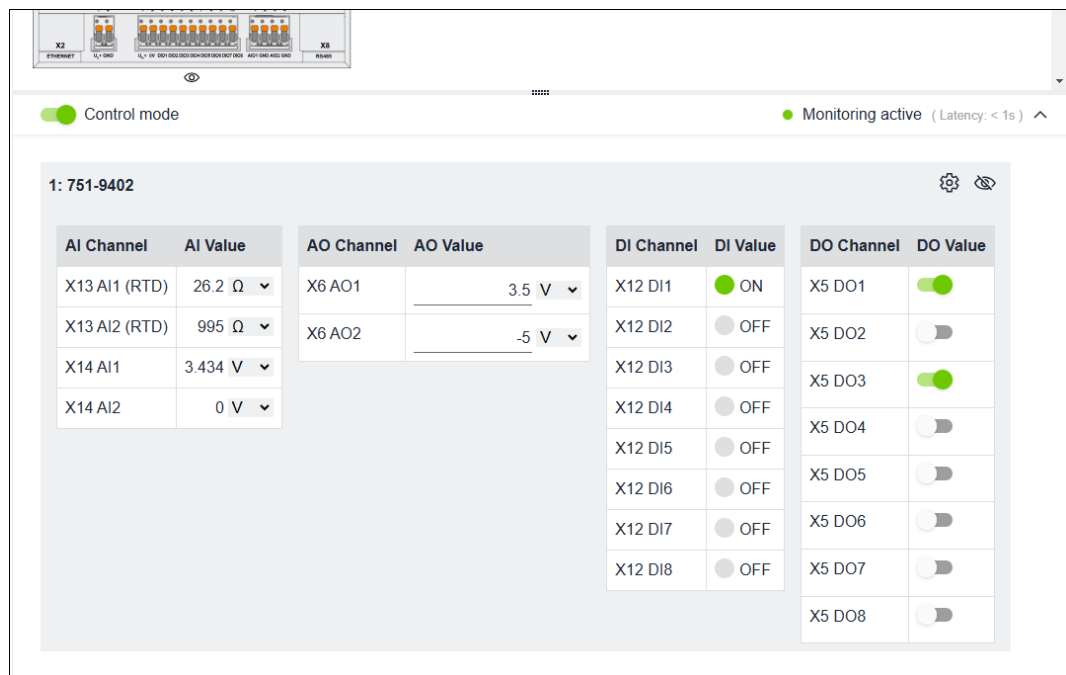


Figure 9: Control Mode Active (Example)

Note

"I/O Check" view may not show original channel configuration

For devices that support variable channel configuration (e.g., WAGO Compact Controller 100, Item no. 751-9402/xxx-xxx), the assignment of the channels can be changed in the "Settings" > "I/O-Channels" view. The "I/O Check" view then shows the modified channels instead of the original ones.

Tip:

You can also access an overview of the LED indicators/status messages via the "Settings" > "LEDs" view.

In addition, each page has a "Device Status/Actions" section via Settings.

4.4.1.4.2 Settings

In the "Settings" view, the device parameters and settings are compared as target values vs. current values. In this view, parameters can be adjusted, written to the device or read from the device.

The parameters and settings relate to the connected device (1).

The upper area (2) indicates whether the current device values and project values match. The **[Refresh]** button can be used to read the device values out again.

The tabs on the left side (8) bundle device parameters according to specific content, e.g., network settings, routing or cloud specifications. Which and how many tabs are displayed differs depending on the device and results from the respective device description file.

Settings and parameter names are displayed in groups on the individual tabs (6). The target values (5) and the current device values (3) are displayed. These values are compared with each other and marked if they differ (4).

Various control elements (e.g., text boxes, drop-down menus and sliders) can be used to edit configured values. On each tab, buttons appear for writing to the device or applying values as target values. These write/read operations only apply to the tab page that is currently open.

Various online actions appear in the lower "Device Status/Actions" area of a tab, if available (7). Some tabs contain only online actions (e.g., "PasswordManagement"). Online actions are always executed immediately and are independent of the read/write function. They are executed directly on the device (example: changing the system time). No changes are made to the project.

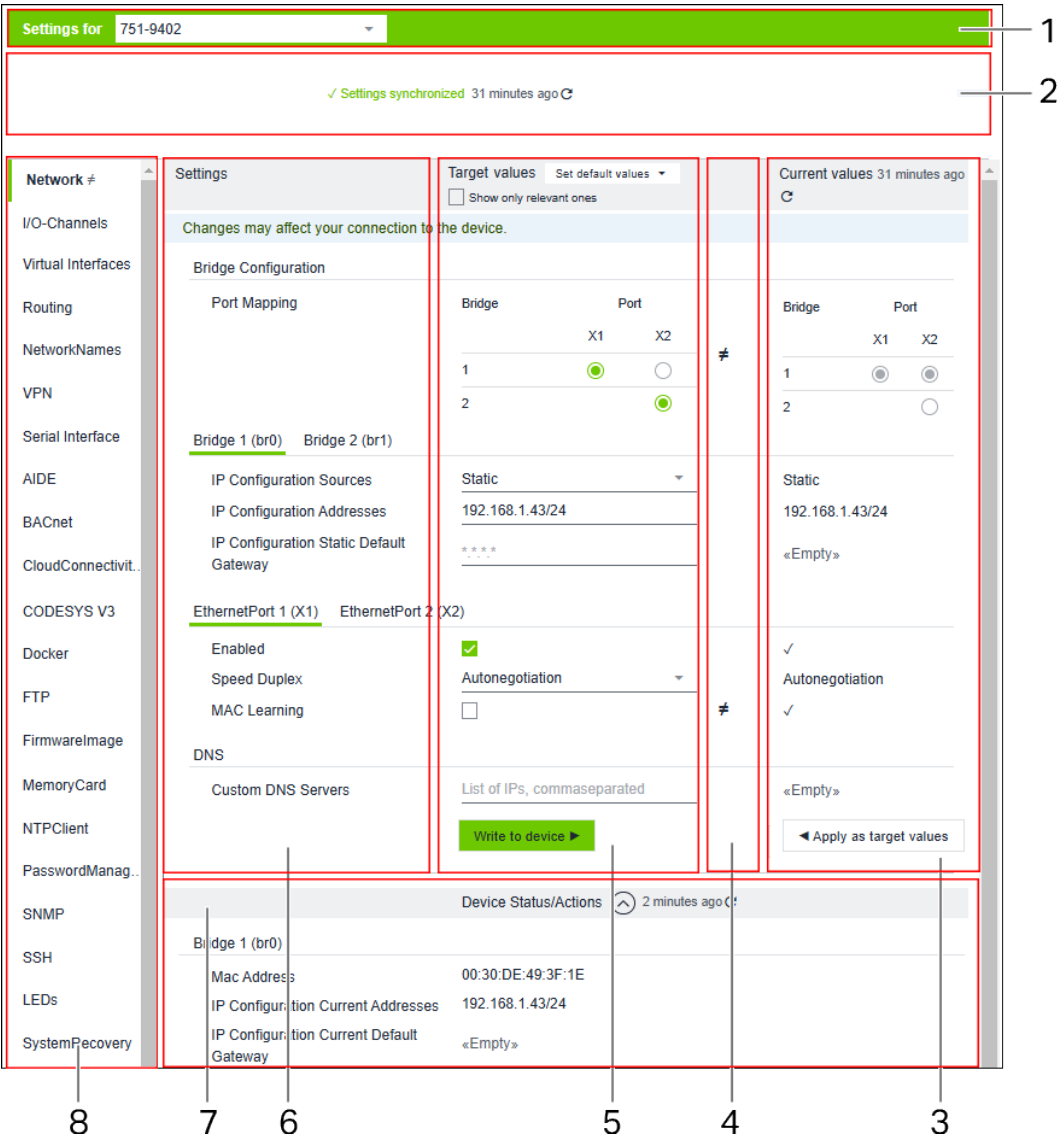
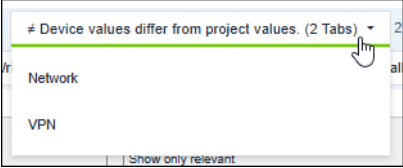


Figure 10: "Settings" View (Example)

Pos.	Parameter/Element	Description
1	Settings for 751-9402	Item number of the device If a name has been assigned for the device in the project: Name (item number) The settings shown below refer to this device.
2	✓ Settings synchronized 31 minutes ago	Status of the target values/device values and information on how long ago the last synchronization was: The current device values and target values match.
	≠ Device values differ from target values. (x tab)	The current device values differ from the target values. The software indicates the number of tabs containing differences. By clicking with the mouse, you can view the list of tabs and switch directly to a tab. 
	__ minutes/hours ago	This indicates how long ago the last synchronization was. Clicking the Refresh icon reads in the values of all tabs of the device and compares them with the target values.

Pos.	Parameter/Element	Description
3	"Current Values" column __ minutes/hours ago 	Displays the values of a device. The displayed device values are updated when target values are written to the device or when a Refresh icon is clicked. In this context, the Refresh icon next to "Current Values" applies to the tab that is currently open. The column header also indicates how long ago the last device value synchronization occurred.
4	Comparison between "Target Value" and "Current Value" ≠	A "not equal to" sign appears between the "Target Values" and "Current Values" columns if the target values and device values differ. The "not equal to" sign is added as a marker next to the corresponding tab name so even differences on unopened tabs can be located quickly.
5	"Target Values" Column	Shows the target values for settings and parameters. "Reset default values" resets the target values to default values. The values can be reset either for "This tab" only or for "All tabs" by selecting the corresponding option from the drop-down menu.
	- Set default values	
	Show only relevant	☐ Shows all project and device values (default setting). The settings and parameter groups that are irrelevant in the configuration that is currently selected are grayed out/italicized. They cannot be changed and are not transferred. Examples of irrelevant parameters include setting a fixed IP address when DHCP is configured. To evaluate whether target values and device values match, only the relevant target values are compared. ☒ Shows only the target and device values that are relevant in the selected configuration. Relevance is evaluated on the basis of the target values.
6	Group/Parameter	Shows device settings and parameters that result from the device description, grouped by topic.
7	"Device Status/Actions" Area __ minutes/hours ago 	This area indicates the current device status. Device actions can be executed directly on the device. No changes are made to the target values.
8	Register	The individual tabs summarize settings for related topics. The number and contents of tabs are device-specific.

Explanation of Icons and Controls in the "Settings" View

Table 61: Icons and Controls in the "Settings" View

Icon	Description
	Exclamation point icon The exclamation point icon provides information on validation: - An exclamation point next to a tab indicates that the tab contains at least one parameter with a warning. - An exclamation point next to a parameter generally means that the parameter does not have a suitable value or format (e.g., the format of an IP address). The check is carried out as an offline validation on the basis of the device description. A warning with an exclamation point does not prevent writing. - An exclamation point next to a parameter that has been written to a device means that the device has not accepted the parameter (online validation). In this case, the exclamation point appears in red . Thus, values are validated on the device itself (online). Offline validation is a simple way of checking values based on certain criteria. The exclamation point remains until the next time the parameter is changed.
beta	"Beta" Label The "Beta" label on a tab indicates a set of available settings and parameters that can change for future developments (e.g., for newer firmware versions of the device, changes to the interface, etc.).
	Refresh Icon Device values are not automatically queried and displayed by the device. This is done once when a connection is established and then again by clicking the refresh icon. Next to the icon, the time since the last device value query is displayed.
	Speech Bubble Icon Clicking on a speech bubble icon displays information/notes on certain parameters. If you click in a different area, the information is hidden again.
	Table view icon Lists with this icon can also be displayed in tabular form to provide a clearer overview. Clicking the icon opens the table in a dialog. The table shows either "Target Values" or "Current Values"; to toggle between these, use the Project values  Device values button. The following buttons can be used to edit the table:  Edit list item  Move list item up one position  Move list item down one position  Delete list item  Add new list item
≠	"Not equal to" sign A "not equal to" sign appears between the "Target Values" and "Current Values" columns if the target values and device values differ. The "not equal to" sign is added as a marker next to the corresponding tab name so even differences on unopened tabs can be located quickly.

File Handling

It is possible to upload/download files at various places in the tab. It is also possible to store certain actions for files that are to be executed when a transfer/write to the device occurs.

Table 62: File Handling

Icon	Description
	Downloading the file to the selected location.

Icon	Description
▼	Opens a drop-down menu with the following options: Not set No action is taken when writing the project data to the device. The file on the device (if any) remains unchanged. Select Opens the file explorer to select a file. The content of the selected file is transferred to the corresponding, already existing file on the device when writing to the device. Clear file on device The contents of the file on the device (not the file itself) are deleted when written to the device.

4.4.1.4.3 Restart

This view shows the connection status of the device used. Clicking the **[Reboot Device]** button initiates the restart of the device.

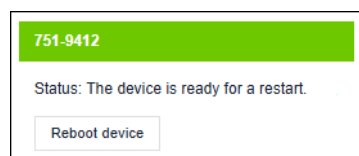


Figure 11: "Reboot" View

4.4.1.4.4 Firmware

In this view, the firmware can be updated for the online connected device.

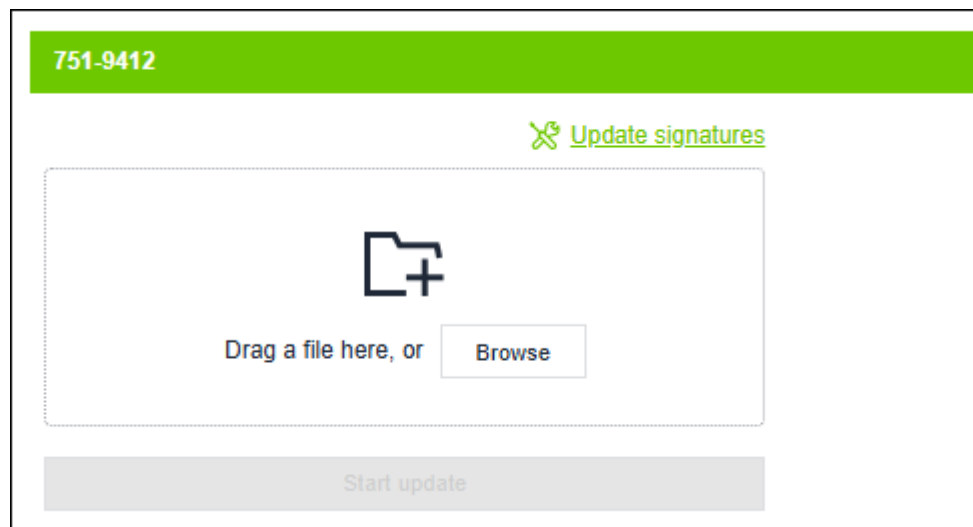


Figure 12: "Firmware" View

Option/Button	Description
[Update signatures]	Open the "Settings" tab and then the "UpdateSignatures" page. If firmware is loaded with components that are not from WAGO and/or multiple components, the corresponding certificates must be uploaded to the "UpdateSignatures" page so that the signature of the entire firmware update can be verified.
📁 or [Browse]	You can drag and drop an update file onto the storage area. Alternatively, select the update via [Browse] in a file browser.
[Choose another file]	Displayed if an update file has already been selected. Click this button to change the update file again.
[Start update]	Updates the firmware with the selected update file.

4.4.1.4.5 Backup/Restore

The **Backup function** can be used to back up device data. The backup file is stored in a network/PC folder or on a removable medium (SD card or USB memory stick) connected to the device. The backup is stored encrypted by entering a password and contains settings, user data and the CODESYS application.

The **Restore function** can be used to restore device data from a backup file. To do this, the password that was used when creating the backup must be entered again.

Note

Note the firmware version!

The Restore function is only possible if the firmware versions are the same at the time of backup and restoration.

Note

Backup/restore can take several minutes!

Creating backup files and restoring data may take several minutes.

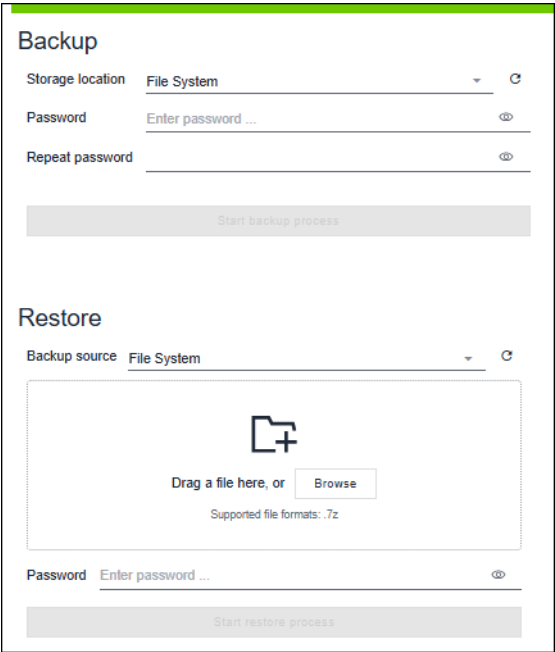


Figure 13: "Backup/Restore" View

Option/Button	Description
Storage location	Selecting the storage location for the backup file 🔄 Updates the list of possible storage locations.
Password / Repeat password	Input field for the password with which the backup file is to be saved. You must enter a password to start the backup. ❗ Password input missing. 👁 Display password in plain text.
[Start backup process]	This button is enabled as soon as a password for the backup has been entered and other processes (e.g., restore or firmware update) have been completed. After the backup file is created, it is initially downloaded into the "Downloads" folder in the form of an archive file (*.zip).

Option/Button	Description
Backup source	Selecting the storage location for the backup source 🔄 Updates the list of storage locations for backup sources.
Password	Input field for the password used to save the backup file. The password is verified by the device itself during the subsequent restore process. ❗ Password input missing. 🔍 Display password in plain text.
📁 or [Browse]	The storage area 📁 is displayed if the file system has been selected as the backup source. To restore a backup file, drag and drop it onto the storage area. Alternatively, click [Browse] to select the backup file in a file browser.
[Start restore process]	The button is enabled once the password has been entered and a valid backup file has been selected. [Start restore process] starts the restore process.

4.4.1.4.6 Device Log

In this view, logged entries for the device can be displayed.

Before retrieving the log entries, display filters can be used to select different log levels (severity of the message) for viewing.

The entries are sorted by timestamp. The latest entry is at the bottom of the list.

i Note

Configure device log in the “Settings” tab!

You can configure which device messages are logged in general on the “Settings” tab under “Logging.” The “Device Log” tab only displays the configured device logs and offers additional filter options.

751-9412

Max. number of entries

100

Min. log Level

Informational

Log sources

For example: kernel or sspd.service

Log entries (from time)

☐ 6/27/25, 6:57 AM

File output format

TXT

Retrieve log entries

Retrieve log entries as a file

Number of log entries: 100

Fri Jun 06 2025 14:37:00 GMT+0200 (Mitteleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational(6)

Reconfig Trigger: Firewall - Apply ruleset

Fri Jun 06 2025 14:37:00 GMT+0200 (Mitteleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational(6)

Reconfig Trigger: Firewall - IP filter

Fri Jun 06 2025 14:37:00 GMT+0200 (Mitteleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational(6)

Reconfig Trigger: HostnameDisableDHCP

Fri Jun 06 2025 14:37:00 GMT+0200 (Mitteleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational(6)

Reconfig Trigger: PasswordQuality

Fri Jun 06 2025 14:37:00 GMT+0200 (Mitteleuropäische Sommerzeit) # wcs-rollout.service [354] # Informational(6)

Reconfig Trigger: Device Certificate AutoRenewal

Figure 14: “Device log” View

Option/Button	Description
Max. number of entries	Specifies the maximum number of entries that are read by the device (default: 100). A maximum of 1,000 log entries can be retrieved and displayed in this tab. When saving to a file, the number can be increased to 100,000,000 entries.

4079033611 | 3 | en-US | 2026-04-27 09:13 | Valid for FW version 01.02.03(03)
Control manual | Controller with YECTO Firmware

61

Option/Button	Description
Min. log level	Filters the displayed log entries by the log level.
Log sources	Filters the log sources of the log entries by the character string entered and only displays corresponding entries.
Log entries (from time)	If you select this option, you can select the date and time from which the log entries are displayed via a calendar. In this way, the results can be limited to the last 20 minutes, for example.
File output format	If "Retrieve log entries as a file" is selected: Selects the output format for the file in which log entries are stored. The text format "TXT" or the table format "CSV" are available.
[Retrieve log entries]	Displays the log entries based on the configuration and the selected filters.
[Retrieve log entries as a file]	Opens a file explorer to save the log entries based on the configuration and according to the selected filters.
Table content	Displays the following information for each log entry: Timestamp (creation time of the entry), source (service/service that created the log entry), log level (severity of the entry) and, if necessary, other information, depending on source/service Entries are sorted by timestamp from oldest (top) to newest (bottom).

4.4.1.5 Message Window

The message bar or message window of the WAGO Device Manager is located at the bottom of the interface. Errors, warnings, success messages and additional information are continuously displayed here during configuration.

First, the message bar is displayed:

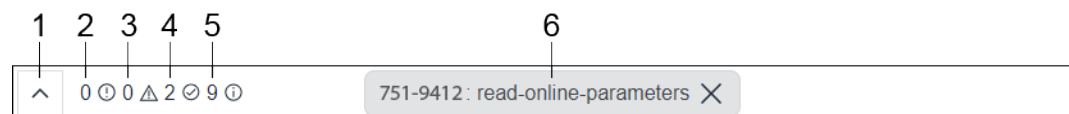


Figure 15: Message bar

Pos.	Description
1	Opens the message window for detailed information.
2	Minimizes the message window and displays the message bar.
2	Displays the number of errors. The indicator flashes until the message window is opened.
3	Displays the number of warnings.
4	Displays the number of success messages.
5	Indicates the amount of additional information.
6	Displays the last message for a few seconds. If there is an error message, it is highlighted in red.

The complete list of messages with detailed information is displayed in the message window.

The  button opens the message list:

▼

❗ 1 Errors

⚠ 0 Warnings

✅ 1 Successes

ℹ 6 Info

🗑 Clear

🔄 Restore

💾 Save

📌 Pin

🔍

Description		Source	Message Time
ℹ	Read device values: completed	Settings	2026-03-03 10:44:04
ℹ >	Read device values: in progress	Settings	2026-03-03 10:44:04
ℹ >	Read device values: in progress	Settings	2026-03-03 10:44:03
❗	Failed to update license repository (in license client)	Licenses	2026-03-03 10:44:03
ℹ	Read device values: started	Settings	2026-03-03 10:44:00
✅	Connected to 192.168.1.43	WDA connection	2026-03-03 10:44:00
ℹ	Trying to connect to 192.168.1.43	WDA connection	2026-03-03 10:43:57
ℹ >	New device added to the project.	Project	2026-03-03 10:43:57

Figure 16: Message window

By default, all messages are displayed when the Messages window opens.

You can filter the messages using the "Errors," "Warnings," "Successes" and "Info" buttons. When enabled (button shown in color), only the filtered messages are displayed in the list. Clicking again (button shown in white) hides those messages again.

The buttons can be used to carry out the following functions:

Button / Table Entry	Description
❗ 1 Errors	Displays errors during the configuration.
⚠ 0 Warnings	Displays warnings during the configuration.
✅ 1 Successes	Displays success messages such as successfully connected devices or successfully transferred data.
ℹ 6 Info	Displays status messages/configuration information.
🗑 Clear	Removes the displayed messages from the list.
🔄 Restore	Restore removed messages.
💾 Save	Opens a dialog window for saving all displayed messages as a text file. Depending on the PC configuration, the download may be made directly to the Downloads folder.
📌 Pin	Keeps the window visible and expanded in the foreground.
📌 Unpin	Unpins the pinned message window. If you click in a different area of the page after releasing the mouse button, the window is minimized to a message bar.
🔍	Searches for and filters any text in the message window. Entering a character enables the search function for the "Device," "Description" and "Source" columns and displays the results in green. Lines without hits are hidden.
Description	Displays the description of the message. For more extensive messages, further information can be opened using the button. Description > read-online-parameters
Source	Shows the source of the messages, e.g., "Settings."
Message Time	Displays the date and time when the message was created. The latest message is at the top.

4.5 Network Functions

4.5.1 Network Configuration

4.5.1.1 Configuration for Security Requirements

To operate the controller securely in the network, the following configuration parameters must be set according to the network infrastructure:

- All unused ETHERNET ports must be switched off (Enable = FALSE).
This prevents external access.
- Network segmentation via bridge configuration
 - Common bridge with multiple Ethernet ports → switching of network packets
 - Only one ETHERNET port per bridge → no switching of network packets
- IP addressing
 - Static
 - Automatic via DHCP reference
- Default gateway
 - Via configuration
 - Automatic via DHCP reference
- Hostname and domain name
 - Via configuration
 - Automatic via DHCP reference
- DNS Server
 - Via configuration
 - Automatic via DHCP reference

The factory setting specifies automatic receipt via DHCP. This automatically sets the following values in the system:

- The default gateway
- The hostname

Since the DHCP protocol is based on broadcast, the network must be protected accordingly.

4.5.1.2 Interface Configuration

4.5.1.2.1 Bridge and Port Configuration

When shared ports are used (switched mode), both physical network ports are part of the same network.

Forwarded packets are not filtered at the Layer 2 level.

Table 63: "Settings" – "Bridge Configuration"

Parameters	Explanation
Port mapping	Assigns physical ports X1 ... X<n> to logical bridges 1 ... <n>; to do so, click the corresponding option button. The assignment is marked in color. A port can only be assigned to one bridge at a time.

Table 64: "Settings" – "Bridge 1 ... Bridge <n>"

Parameters	Explanation
Bridge <n>	For each bridge in the controller, a separate tab is displayed.
Address	Enter the IP addresses for the selected bridge as a comma-separated list in CIDR format

Parameters	Explanation
Gateway	Enter the gateway address
Gateway Metric	Enter the gateway metric; default: "200"
Sources	Selection that determines whether IP addresses transmitted via DHCP are used
	DHCP IP addresses transmitted via DHCP and the IP addresses entered under "Addresses" are used.
	"Empty" Only the IP addresses entered under "Addresses" are used.
DHCP – RouteMetric	Enter the metric for routes transmitted via DHCP; default setting: "100" This input field is only enabled if "DHCP" is selected in the "Sources" drop-down menu.
DHCP – UseDNS	Setting that determines whether DNS addresses transmitted via DHCP are used. This checkbox is only enabled if "DHCP" is selected in the "Sources" drop-down menu.
DHCP – UseDomains	Selection that determines whether and how domains transmitted via DHCP are used; this drop-down menu is only enabled if "DHCP" is selected in the "Sources" drop-down menu.
	False Domains transferred via DHCP are not used.
	True Domains transferred via DHCP are used as search domains.
	Route Domains transferred via DHCP are used as routing-only domains.
DNS	Enter the IP addresses of the DNS servers as a comma-separated list
Domains	Enter the domain addresses as a comma-separated list; if a tilde (~) is prefixed to an address, the domain is used as a routing-only domain. If no tilde (~) is prefixed to an address, the domain is used as a search domain.
MTU	Enter the MTU value; factory setting: "1500"

To protect the controller against processor overload, the storm protection function can be configured for the expected network traffic (in terms of broadcast and multicast rates):

- The storm protection rate is set globally for all ETHERNET ports
- For all ETHERNET ports, you can specify whether the broadcast rate setting should also apply to multicast
- The storm protection function can be enabled separately for each ETHERNET port

Table 65: "Settings" – "Networking/StormProtection"

Parameters	Explanation
Broadcast Rate Limit	Set broadcast rate limit. Factory setting: "10 %"
Multicast Rate Limit	This input field is disabled. It is not visible if the "Show relevant only" box at the top of the page is checked.
Enable Multicast Rate Limiting	Enable/disable multicast rate limiting.
	☐ Multicast rate limiting is disabled. The broadcast rate limiting value setting is only applied to broadcast messages (factory setting).
	☒ Multicast rate limiting is enabled. The broadcast rate limiting value setting is applied to both broadcast and multicast messages together.

Table 66: "Settings" – "EthernetPort 1 ... EthernetPort <n>"

Parameters	Explanation	
EthernetPort <n> (X<n>)	For each port in the controller, a separate tab is displayed.	
Enabled	Enable/disable selected port.	
	☐	The port is disabled.
	☒	The port is enabled.
Speed Duplex	Select transmission speed and transmission method The drop-down menu is only enabled if the port is enabled. If "Autonegotiation" is selected, the connection modalities are automatically negotiated with the remote peer. Factory setting: "Autonegotiation"	
MAC Learning	Enable/disable the "MAC Learning" functionality for the selected port The checkbox is only enabled if the port is enabled.	
	☐	The "MAC Learning" functionality is disabled
	☒	The "MAC Learning" functionality is enabled
Enable Broadcast Rate Limiting	Enable/disable broadcast protection for the selected port	
	☐	Broadcast protection is disabled.
	☒	Broadcast protection is enabled.
Enable Multicast Rate Limiting	This checkbox is not enabled. It is not visible if the "Show relevant only" box at the top of the page is checked.	

A separate group is displayed for each bridge in the "Device Status/Actions" area.

Table 67: "Device Status/Actions" – "Bridge <n> (br<n-1>)"

Parameters	Explanation
MAC Address	MAC address of the selected bridge
Addresses	Shows the IP addresses as a comma-separated list in CIDR format
Gateway	Shows the gateway address
DNS	Shows the IP addresses of the DNS servers as a comma-separated list
Domains	Shows the domain addresses as a comma-separated list; if a tilde (~) is prefixed to an address, the domain is used as a routing-only domain. If no tilde (~) is prefixed to an address, the domain is used as a search domain.

For each ETHERNET port, a separate group is displayed in the "Device Status/Actions" area.

Table 68: "Device Status/Actions" – "EthernetPort <n> (X<n>)"

Parameters	Explanation	
MAC Address	MAC address of the selected ETHERNET interface	
Has Link	Indicates the connection status	
	false	The interface is not connected.
	true	The interface is connected.
Speed Duplex	Shows the transmission rate and the transmission method	

4.5.1.3 Hostname/Domain Addresses

The hostname is set globally for the controller.

The domain addresses are set separately for each bridge configured in the controller.

4.5.1.3.1 Hostname

If no hostname is set in the configuration, the controller is assigned a default name. This name contains part of the product name and the last three values of the controller's MAC address. The default name remains valid until a hostname is set in the configuration or assigned to the controller via DHCP.

If there are multiple network interfaces with DHCP, the last hostname transmitted via DHCP is used.

The default hostname is reactivated if the network interfaces are changed to static IP addresses or the DHCP lease has expired.

If the hostname is set manually, the name set in the configuration has the highest priority and is not overwritten by hostnames received via DHCP.

The hostname settings can be made on the WBM "Hostname" page in the "Hostname" group, for example.

4.5.1.3.2 Domain Addresses

Domain addresses can be entered manually in a list. Furthermore, automatic transmission via DHCP is possible if the controller is configured accordingly.

You can specify whether the domains are search domains or routing-only domains for the addresses that are entered manually, as well as for the addresses transmitted via DHCP.

For search domains, the address serves as a search suffix to extend single-label hostnames to fully qualified domain names (FQDNs).

For routing-only domains, all DNS traffic that does not match another domain is forwarded to this interface with the specified DNS server. This setting allows you to give preference to specific DNS servers.

For more information on the meaning and configuration of the domain addresses, search the Internet for documentation on "systemd-networkd."

The settings for the domain addresses can be made in the WBM or in WAGO Device Manager under "Settings" on the WBM "Network" page in the "Bridge 1 ... Bridge <n>" groups, for example.

4.5.2 Network Security

4.5.2.1 Providing a Secure Network Environment

Communication via standard fieldbus protocols is insecure, and there are no protocol mechanisms for protection.

To meet security requirements, the operator must provide physical protection (e.g., protected cable installation, protection against unauthorized physical access, etc.) or access via VPN.

4.5.2.2 Firewall

The firewall protects the controller against unauthorized network access and starts up before the network is active.

The firewall must be configured according to the operational security requirements.

The following can be set:

- Approved/blocked MAC or IP addresses
- Flood and broadcast protection
- Enabling ports/bridges for the various services

The settings can be made via the WBM or WAGO Device Manager.

The firewall is active even while firewall parameters are being reconfigured.

To check the firewall, you can attempt to access ports or addresses that are not permitted in the settings and verify that these access attempts are rejected.

4.5.2.2.1 MAC Address Filter

Different filter rules can be created for sender MAC addresses.

The following settings can be made for each filter rule:

- Rule name
- Enable/disable the rule (Enabled/Disabled)
- Rule effect (drop/accept)
- Sender MAC address
- Mask

These settings can be made with the WBM or WAGO Device Manager.

Table 69: "Settings" – "FirewallMACFilterRule List"

Parameters	Explanation	
FirewallMACFilterRule <n>	For each filter rule, a separate group is displayed.	
Name	Enter the name for the filter rule	
Enabled	Enable/disable the filter rule	
	☐	The filter rule is not applied.
	☒	The filter rule is applied.
Verdict	Setting for the effect of the filter rule	
	Drop	Packets with MAC addresses that match the filter are rejected.
	Accept	Packets with sender MAC addresses that match the filter are accepted.
Address	Enter the sender MAC address affected by the filter rule	
Mask	Enter the mask in the format "ff:ff:ff:ff:ff:ff"	

4.5.2.2.2 ServiceRules

For each service, a separate FirewallServiceRule can be configured.

The assigned interfaces (bridge) can be selected for each FirewallServiceRule.

The list of possible interfaces is generated from the settings in the "Bridge and Port Configuration" section.

- FirewallServiceRule <m>
 - Interfaces

These settings can be made with the WBM or WAGO Device Manager.

4.5.2.2.3 IP Address Filter

Different filter rules can be created for source IP addresses.

For each filter rule, the following settings can be made:

- Rule name
- Enable/disable the rule (Enabled/Disabled)
- Rule effect (drop/accept)
- Protocol (TCP, UDP or both)
- Interfaces
- Source IP address (CIDR format)
- Source port
- Destination port

These settings can be made with the WBM or WAGO Device Manager.

Table 70: "Settings" – "FirewallIPFilterIncomingRule List"

Parameters	Explanation	
FirewallIPFilterIncomingRule <n>	For each filter rule, a separate group is displayed.	
Name	Enter the name for the filter rule	
Enabled	Enable/disable the filter rule	
	☐	The filter rule is not applied.
	☒	The filter rule is applied.
Verdict	Setting for the effect of the filter rule	
	Drop	Packets with IP addresses that match the filter are rejected.
	Accept	Packets with source IP addresses that match the filter are accepted.
Protocol	Select IP protocols	
	Any	"Any" also includes "TCP" and "UDP."
	TCP	
	UDP	
Interfaces	Select the interfaces to which the rule is applied: If no interface is selected, the rule is applied to all interfaces.	
Source IP	Enter the source IP address and mask in CIDR format	
Source Port	Enter the source port ("0" = all)	
Destination Port	Enter the destination port ("0" = all)	

4.5.2.2.4 IP Forwarding Filter

Different filter rules can be created for source and destination IP addresses.

For each filter rule, the following settings can be made:

- Rule name
- Enable/disable the rule (Enabled/Disabled)
- Rule effect (drop/accept)
- Protocol (TCP, UDP or both)
- Input and output interfaces
- Source IP address (CIDR format)
- Source port
- Destination IP address (CIDR format)

- Destination port

These settings can be made with the WBM or WAGO Device Manager.

Table 71: "Settings" – "FirewallIPFilterForwardingRule List"

Parameters	Explanation	
FirewallIPFilterForwardingRule <n>	For each filter rule, a separate group is displayed.	
Name	Enter the name for the filter rule	
Enabled	Enable/disable the filter rule	
	☐	The filter rule is not applied.
	☒	The filter rule is applied.
Verdict	Setting for the effect of the filter rule	
	Drop	Packets are dropped according to filter criteria.
	Accept	Packets are accepted according to filter criteria.
Protocol	Select IP protocols	
	Any	"Any" also includes "TCP" and "UDP."
	TCP	
	UDP	
Incoming Interfaces	Select the input interfaces to which the rule is applied: If no interface is selected, the rule is applied to all interfaces.	
Outgoing Interfaces	Select the output interfaces to which the rule is applied: If no interface is selected, the rule is applied to all interfaces.	
Source IP	Enter the source IP address and mask in CIDR format	
Source Port	Enter the source port ("0" = all)	
Destination IP	Enter the destination IP address and mask in CIDR format	
Destination Port	Enter the destination port ("0" = all)	

4.5.2.2.5 Flood/Broadcast Protection

4.5.2.2.5.1 ICMP Echo Flood Protection

The firewall reduces the number of ICMP echo packets; this prevents attacks without negatively affecting normal operation.

The number of ICMP echo packets is set to a maximum of 10 packets per second so as not to interfere with multiple parallel pings.

This setting cannot be changed.

4.5.2.2.5.2 ICMP Echo Broadcast Protection

The firewall discards broadcast ping packets.

This setting cannot be changed.

4.5.2.3 IPsec

Various IKE connections can be configured for protection via IPsec.

For each IKE connection, the following settings can be made:

- Name
- Authentication method ("X.509"/"PSK")
- Remote address

- Secret
- Local certificate
- Local identity
- Remote CA certificate
- Remote certificate
- Remote identity

The "X.509" setting is recommended for the authentication method.

PreSharedKeys ("PSK") authentication is less secure than certificate-based authentication with a truststore ("X.509").

For configuration of the remote CA, we strongly recommend that you enter an IKE identity. If no identity is configured, any certificate issued by the CA is accepted.

All IKE and ESP algorithms that the German Federal Office for Information Security classifies as secure are permitted. This default setting is not adjustable.

The IKE connections can be configured in the WBM or in WAGO Device Manager on the "IPsecClient" page under "Settings."

Table 72: "Settings" – "IKEConnection"

Parameters	Explanation
IKEConnection List	Number of created IKE connections
IKEConnection <n>	For each created IKE connection, a separate area is displayed.
Name	Enter the name for the IKE connection.
Authentication Method	Select the authentication method for the IKE connection
	X.509 (recommended)
	PSK
Remote Address	Enter the hostname or IP address of the IPsec responder
Secret	Enter the "Pre-shared Key" that is used for authentication when the "PSK" authentication method is selected
Local Certificate	Enter the certificate of the local peer
Local Identity	Enter IKE identity of the local peer If no identity is configured, the IPsec client automatically determines the identity.
Remote CA Certificate	Select the CA certificate with which the remote peer certificate must be signed
Remote Certificate	Select the certificate of the remote peer
Remote Identity	Enter IKE identity of the remote peer If no identity is configured, every identity is accepted.

Different IPsec tunnels can be configured for each IKE connection.

The following settings can be made for each IPsec tunnel:

- Status (Enabled/Disabled)
- Source address in CIDR format
- Destination address in CIDR format

The IPsec tunnel can be configured in the WBM or in WAGO Device Manager on the "IPsec-Client" page under "Settings."

Table 73: "Settings" – "IPsecTunnel"

Parameters	Explanation
IPsecTunnel List	Number of IPsec tunnels created
IPsecTunnel <n>	For each IPsec tunnel created, a separate area is displayed.

Parameters	Explanation	
Connection	Select the IKE connection for which the IPsec tunnel has been / is being configured	
Enabled	Enable/disable IPsec tunnel	
	☐	The IPsec tunnel is not active.
	☒	The IPsec tunnel is active.
Source Address	Enter the source IP address and mask in CIDR format	
Destination Address	Enter the destination IP address and mask in CIDR format	

The following information is displayed in the WBM or in WAGO Device Manager on the "IPsecClient" page under "Device Status/Actions."

Table 74: "Device Status/Actions" – "IPsecTunnel"

Parameters	Explanation	
IPsecTunnel List	Number of enabled IPsec tunnels	
IPsecTunnel <n>	For each enabled IPsec tunnel, a separate area is displayed.	
Established	Connection status of the IPsec tunnel	
	☐ false	The connection has not been established.
	☒ true	The connection has been established.

4.5.3 Network Services

4.5.3.1 DHCP Client

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

The following parameters can be obtained:

- IP address
- Subnet mask
- Router/Gateway
- Hostname
- Domain
- DNS Server
- NTP server

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

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

4.5.3.2 SSH Service

The SSH service is always enabled.

Communication takes place via port 22.

These settings cannot be changed.

When the factory settings are used, the service cannot be reached from the outside. Access is blocked via all network interfaces.

External access is possible if the firewall rules are set accordingly.

The SSH service only allows password-based authentication.

All authentication attempts are logged regardless of success.

Login as root is not possible.

However, other users can be converted to root users if this option is enabled.

Please refer to section "'root' User Account" for information on the significance and use of the "root" account.

4.6 Memory Functions

4.6.1 Automount

Table 75: "Settings" – "Automount"

Parameters	Explanation	
Enabled Storage Devices	Drop-down menu with possible storage media indicating the storage media that are automatically enabled; when the drop-down menu is collapsed, the storage media that are automatically enabled are displayed below it. When it is expanded, a list of checkboxes is displayed for each available storage medium.	
	☐	The storage media are not automatically enabled.
	☒	The storage media are automatically enabled.
	SDCards	Determines whether SD cards are automatically enabled.

4.6.2 Data Backup

The device has a backup and restore function.

Note

Note the firmware version!

The Restore function is only possible if the firmware versions are the same at the time of backup and restoration.

Execution of the backup or restore function is recorded in the event log.

4.6.2.1 Backup Function

The backup function can be used to copy the device's settings and user data and save them in an encrypted backup file.

The backup function can be executed with WBM or WAGO Device Manager.

The process of backing up the data with the backup function in the WBM is described in section " **Performing a Backup** [[p. 88](#)]."

4.6.2.2 Restore Function

The Restore function can be used to copy and restore the settings and user data from an encrypted backup file to the device.

The backup file is checked for integrity before the restore. If this check fails, the backup file cannot be imported.

After a successful integrity check, restarting the device completes the restore process.

The restore function can be executed with the WBM or WAGO Device Manager.

The process of restoring the data via the restore function in the WBM is described in the section " **Performing a Restore [► 89].**"

4.7 Diagnostic Functions

4.7.1 Diagnostics via Indicators

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

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

4.7.2 Diagnostics via WBM or WAGO Device Manager

4.7.2.1 Illustration of LEDs

The states of the device LEDs are indicated in WBM or WAGO Device Manager in the "Settings" view on the "LEDs" page.

The following information is displayed for each LED in the "Device Status/Actions" area:

- The name of the LED according to the marking on the device
- The diagnostic information
- The color(s) corresponding to the actual LED state on the device

Solid-colored regions indicate that the LED is continuously illuminated in the corresponding color.

Multicolor overlapping regions indicate that it is flashing in the corresponding colors.

A gray region corresponds to the "Off" state.

The number and type of LEDs depend on the product. For the diagnostics indicated by these LEDs and suggested fixes, see the corresponding product manuals.

4.7.2.2 Wiring Test (I/O Check)

A simple wiring test can be performed via the "I/O Check" view.

For this purpose, the states of the inputs (if present or configured) can be indicated via the LED symbols or in plain text (monitoring mode).

In addition, the states of the outputs (if present or configured) can be set via the LED symbols or in plain text (control mode).

This process is described in section " **Testing the Wiring [► 93].**"

4.7.2.3 Event Log (Device Log)

In the "Device Log" view, you can view device log entries.

Before retrieving the log entries, display filters can be used to select different log levels (severity of the message) for viewing.

The entries are sorted by timestamp. The latest entry is at the bottom of the list.

Note

Configure device log in the "Settings" tab!

You can configure which device messages are logged in general on the "Settings" tab under "Logging." The "Device Log" tab only displays the configured device logs and offers additional filter options.

The screenshot displays the 'Device Log' configuration and view interface. At the top, a green header bar shows the device ID '751-9412'. Below this, configuration fields include: 'Max. number of entries' set to 100, 'Min. log Level' set to 'Informational', 'Log sources' with the example 'kernel or sspd.service', and 'File output format' set to 'TXT'. There are two buttons: 'Retrieve log entries' and 'Retrieve log entries as a file'. Below the configuration, a section titled 'Number of log entries: 100' shows a list of log entries. Each entry includes a timestamp, timezone, service name, log level, and a reconfig trigger.

Option/Button	Description
Max. number of entries	Specifies the maximum number of entries that are read by the device (default: 100). A maximum of 1,000 log entries can be retrieved and displayed in this tab. When saving to a file, the number can be increased to 100,000,000 entries.
Min. log level	Filters the displayed log entries by the log level.
Log sources	Filters the log sources of the log entries by the character string entered and only displays corresponding entries.
Log entries (from time)	If you select this option, you can select the date and time from which the log entries are displayed via a calendar. In this way, the results can be limited to the last 20 minutes, for example.
File output format	If "Retrieve log entries as a file" is selected: Selects the output format for the file in which log entries are stored. The text format "TXT" or the table format "CSV" are available.
[Retrieve log entries]	Displays the log entries based on the configuration and the selected filters.
[Retrieve log entries as a file]	Opens a file explorer to save the log entries based on the configuration and according to the selected filters.

Figure 17: "Device log" View

Option/Button	Description
Max. number of entries	Specifies the maximum number of entries that are read by the device (default: 100). A maximum of 1,000 log entries can be retrieved and displayed in this tab. When saving to a file, the number can be increased to 100,000,000 entries.
Min. log level	Filters the displayed log entries by the log level.
Log sources	Filters the log sources of the log entries by the character string entered and only displays corresponding entries.
Log entries (from time)	If you select this option, you can select the date and time from which the log entries are displayed via a calendar. In this way, the results can be limited to the last 20 minutes, for example.
File output format	If "Retrieve log entries as a file" is selected: Selects the output format for the file in which log entries are stored. The text format "TXT" or the table format "CSV" are available.
[Retrieve log entries]	Displays the log entries based on the configuration and the selected filters.
[Retrieve log entries as a file]	Opens a file explorer to save the log entries based on the configuration and according to the selected filters.

Option/Button	Description
Table content	Displays the following information for each log entry: Timestamp (creation time of the entry), source (service/service that created the log entry), log level (severity of the entry) and, if necessary, other information, depending on source/service Entries are sorted by timestamp from oldest (top) to newest (bottom).

For more information, see section "[🔗 Viewing the Device Log \[► 94\].](#)"

5 Commissioning

5.1 Switching On the Controller

Before switching the controller on, verify that you:

- Have mounted the controller correctly (see product manual, "Mounting" section)
- Have connected all required data lines (see product manual, section "Connections") to the corresponding interfaces/ports
- Have connected the power supply (see product manual, section "Connections")
- Have performed appropriate potential equalization on your machine/system
- Have implemented the shielding properly

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

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

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

The CODESYS V3 runtime system starts simultaneously.

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

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

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

5.2 Setting an IP Address

The following default settings apply to ETHERNET communication when the controller is first delivered:

Table 76: ETHERNET Communication Default

Interface	Default Setting
ETHERNET ports X1/X2	▪ Switched Mode (Bridge 1) ▪ Dynamic IP address assignment via DHCP ▪ Default static IP address: 172.29.233.42/24
USB service port	Fixed static IP address: 192.168.42.42

- Use a configuration tool (e.g., WBM or WAGO Device Manager) to adapt the IP addressing of ETHERNET ports X1/X2 to your system structure; see [🔗 Configuration \[► 82\]](#).
- ➔ All required network subscribers are located in the same subnet and can communicate with one another

5.2.1 Setting an IP Address via the WBM

The required settings can be found on the "Settings" tab on the "Network" page.

1. Select the port assignment in the "Bridge Configuration" group.
2. Enter the corresponding IP address(es) in the "Bridge <n>" group

5.2.2 Assigning an IP Address with DHCP

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

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

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

5.3 Changing Passwords

When you log in for the first time, or if your administrator requires, the login window prompts you to set a new password or change your existing password.

1. If applicable, enter the old password.
2. Enter the new password.
3. Repeat the new password.

To increase security, passwords must contain a mixture of lower case letters, upper case letters, numbers and special characters.

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

Note

Valid characters for passwords

Passwords may contain only the following characters:

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

The minimum number of characters can be set via the WBM or WAGO Device Manager.

Table 77: "Settings" – "Account Management/PasswordQuality"

Parameters	Explanation
Min Length	Enter the minimum length of the password (6 ... 100; factory setting = 8)
Min Capital	Minimum number of uppercase letters (A ... Z) (0 ... 100, factory setting = 1)
Min Lowercase	Minimum number of lowercase letters (a ... z) (0 ... 100, factory setting = 1)
Min Digit	Minimum number of digits (0 ... 9) (0 ... 100, factory setting = 1)
Min Special	Minimum number of special characters () (0 ... 100, factory setting = 1)

5.4 Managing Users

5.4.1 Managing Local User Roles and Accounts

Local user roles and accounts are managed in the WBM or in WAGO Device Manager on the "AccountmanagementLocal" page.

Displaying the local user management requires the "StaticPermission 3041 (wdx-account-management local-ro)" user right.

Modifying the local user management requires the "StaticPermission 3040 (wdx-account-managementlocal-rw)" user right.

The "admin" system user has both permissions.

The predefined user role "RBAC Admin" also has both permissions according to the factory settings.

- ✓ You must be logged on to the controller as a user with the required authorization.
- Check the "Enabled" box in the "Account Management/Local" area to enable local user management.

5.4.1.1 Managing Local User Accounts

The user accounts that have been created are displayed in the "User List" area along with their roles.

Creating a New User Account

1. Click the **[+User]** button at the end of the list.
 - ⇒ A new "User <n>" area appears.
2. Enter the name you want for the user account in the "Name" field.
3. Enable or disable the user account with the "Enabled" checkbox.
4. Click on the user roles you want in the "Roles" drop-down menu.
 - ⇒ The selected user roles are highlighted in gray in the drop-down menu and entered in the list.
5. To remove a user role from the list, click the **[×]** button next to the user role. Alternatively, find the corresponding user role, which is now highlighted in gray, in the drop-down menu and click on it again.
 - ⇒ The corresponding user roles are deleted from the list.
6. Check the "Force Password Change" box if you want to require the new user to change the password the first time they log in.
7. After assigning all required user roles, click the **[Write to Device]** button.
 - ➔ The new user account has been created and can be used if enabled.

Changing a User Account

1. Navigate to the user account you want to change.
2. If applicable, change the name for the user account in the "Name" input field.
3. If applicable, enable or disable the user account using the "Enabled" checkbox.
4. Add user roles or remove existing user roles as described above.

5. If applicable, change the setting in the "Force Password Change" checkbox according to whether or not you want a password change to be required the next time this user logs in.
6. After changing the settings, click the **[Write to Device]** button.
➔ The user account has been changed.

Removing a User Account

1. Navigate to the user account you want to delete.
2. Click the **[Trash Can]** button in the account entry header.
⇒ The user account is removed from the "User List" area.
3. After removing the user account, click the **[Write to Device]** button.
➔ The user account has been permanently removed and can no longer be used.

5.4.1.2 Managing Local User Roles

The "UserRole List" area shows the user roles that have been created and their permissions.

Creating a New User Role

1. Click the **[+UserRole]** button at the end of the list.
⇒ A new "UserRole <n>" area appears.
2. Enter the name you want for the user role in the "Name" input field.
3. In the "Permissions" drop-down menu, select the permissions you want.
⇒ The selected permissions are highlighted in gray in the drop-down menu and entered in the list.
4. To remove a permission from the list, click the **[x]** button next to the permission. Alternatively, locate the corresponding permission, which is now highlighted in gray, in the drop-down menu and click on it again.
⇒ The corresponding permissions are deleted from the list.
5. After assigning all required permissions, click the **[Write to Device]** button.
➔ The new user role has been created and can be used in the user accounts.

Changing a User Role

1. Navigate to the user role you want to change.
2. If necessary, change the name for the user role in the "Name" input field.
3. Add or remove existing permissions as described above.
4. After changing the settings, click the **[Write to Device]** button.
➔ The user role has been changed.

Removing a User Role

1. Navigate to the user role you want to delete.
2. Click the **[Trash Can]** button in the role entry header.
⇒ The user role is removed from the "UserRole List" area.
3. After removing the user role, click the **[Write to Device]** button.

- ➔ The user role is permanently removed and can no longer be used.

5.5 Switch Off/Restart

Switch off the power supply to shut down the controller.

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

Note

Do not power cycle the controller after changing any parameters!

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

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

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

6 Configuration

6.1 Configuring in WBM

- ✓ The device can be accessed via the network or USB.
- 1. Open the browser and enter the IP address of the controller.
 - ⇒ The WBM opens and a login message appears.
- 2. Click the **[Open Login Window]** button.
 - ⇒ The login window opens.
- 3. Enter your login credentials (username and password) and click the **[Login]** button.
 - ⇒ After successful login, you can navigate through the WBM.
- 4. Open the "Settings" view.
See tips for using the "Settings" view below.
 - ⇒ The device data is automatically read out after the connection is established and is initially applied as target values (left), so the current device values initially match the target values.
- 5. Select a tab in which you want to make settings, e.g., "VPN."
- 6. Make your changes in the "Target Values" column. For example, you can set "OpenVPN" to "Enabled."
 - ⇒ A "not equal to" sign indicates that the target value now differs from the device's current value.
- 7. Make any further changes in different tabs as needed.
 - ⇒ You can find an overview of which tab you have made changes in the drop-down menu at the top. From this menu, you can switch directly to the tab in which you have made changes if required. The corresponding tabs themselves are also marked with an unequal sign after changes.
- 8. To transfer the changes to the device, click **[Write to Device ►]** under the changed values.
 - ➔ Configurations and parameters have been transferred to the device. The node is ready for use.

Tips

- A description of the "Settings" view with explanations of icons, operating elements and file handling can be found under Settings.
- Check the "Show only relevant ones" checkbox to display only those settings that are relevant to the configuration used. In this case, grayed out and thus unchangeable, irrelevant settings are hidden.
- Use the update icon  to read and display current values from the device. Otherwise, the values are updated each time a connection is established and write operations are executed.

Execute actions directly

Certain changes are sent directly to the device, so you do not have to save them as target values and then transfer them; examples include changes to the system time.

You can find such actions in the lower area of the respective tabs under "Device Status/Actions." You can also find device status information in the same area.

7 Service

7.1 Firmware Updates

! NOTICE

Do not switch the controller off!

Interrupting the update process can damage the controller.

- Do not switch the controller off during the update process and do not interrupt the power supply!

i Note

Have the matching documentation ready for the target firmware version!

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

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

You can update the firmware via the WBM.

7.1.1 Performing a Firmware Update with the WBM

If you want to use the device with a different firmware version than the one set in the configuration, you can change the firmware version via the interface.

! NOTICE

To prevent damage to the device, follow the instructions!

Interrupting the update process can damage the device. For this reason, please note the following instructions regarding hardware and software.

Hardware Notes

- Do not switch devices off.
- Do not interrupt the power supply of the device.
- Do not remove devices from the node group.
- Ensure that communication with the device is not interrupted during the update.
- For updates via the service interface, disconnect the fieldbus cable from the device beforehand.
- Do not exit the software during the operation.

Software Notes

- Stop application on device before performing the update.

- Programs and data on the device can be lost during the update. Make sure you have a recent backup of the data.
- The application and other files in the memory or file system must be transferred to the new controller after updating.
- After replacing the firmware, note the new firmware version (xx) in the box provided on the controller.

Note

Disclaimer for Updates!

Liability claims against WAGO GmbH & Co. KG relating to material or immaterial damage caused by updates (e.g., firmware changes) are excluded. Use is at the risk of the user exclusively.

Note

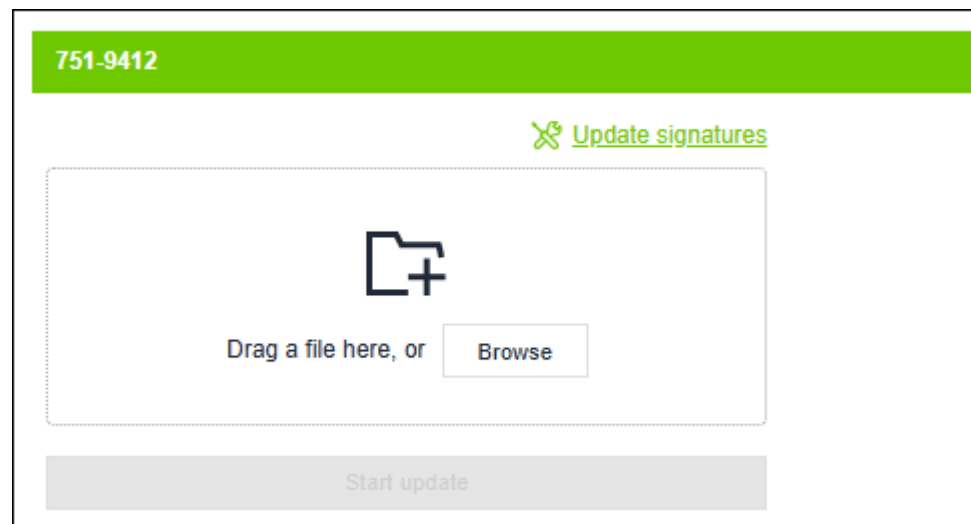
Additional information from WAGO Support!

Please contact WAGO GmbH & Co. KG Support for more information on updates/firmware changes.

Note

Updates can take a few minutes!

Note that updates, e.g. replacing the firmware, may take several minutes depending on the hardware configuration of the device.



- ✓ You have downloaded a new update file for your device in the [WAGO Download Center](#) or you will download it directly via the WAGO Download Center below.
- ✓ **Note: Custom firmware requires corresponding certificates!**
Firmware files must be signed. This is already the case for WAGO firmware downloaded via WAGO Navigator/WAGO Download Center. However, if you are loading firmware with your own or multiple components, click on "Update signatures" and add the appropriate

certificates on the page, which is used to verify the signature of the entire firmware update. The firmware cannot be updated without a certificate.

1. Click the **[Update]** button in the ribbon.
 2. Drag the update file to the storage area.
Alternatively, click **[Browse]** and select the downloaded update file.
 - ⇒ The file name of the selected update file is displayed. Use **[Choose another file]** to change the update file as needed.
 3. Click **[Start update]**.
 - ⇒ The update file is first loaded onto the device. The update is then executed.
 - ⇒ The update process may take some time (about 20 min). During the process, other processes and WBM operation are not available. The connection to the device may be temporarily interrupted.
 - ⇒ The device restarts after the update.
 4. Click **[Reload WBM]**.
 5. Log in to your device with the access data.
 - ⇒ If errors occurred, they are displayed in the message window and in the "Update" tab.
- ➔ The device is running with the new firmware.

7.2 Clearing Reset Functions

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

7.2.1 Warmstart Reset

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

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

7.2.2 Coldstart Reset

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

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

7.2.3 Software Reset (Restart)

The product is restarted during a software reset.

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

7.2.4 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!

i Note

All parameters and passwords are overwritten!

The reset overwrites all parameters and passwords.

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

Firmware functions that were installed later are deleted.

Software licenses are deleted.

- If you have any questions, contact WAGO Support.

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

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

Alternatively, you can perform a factory reset via the WBM or WAGO Device Manager. To do so, proceed as follows:

1. Connect the controller to your computer via an ETHERNET interface or the USB service interface.
 2. Open the WBM on the controller or in WAGO Device Manager on the computer.
 3. Sign in to the controller with your username and password.
 4. Open the "System" tab.
 5. Navigate to the "Factory Reset" entry.
 6. Click the **[Reset]** button in the "Device Status/Actions" area.
 - ⇒ A dialog with a security prompt opens.
 7. Click the **[Restore Factory Settings]** button.
- ➔ The controller is reset and restarts automatically.

7.3 Starting/Stopping CODESYS Applications

CODESYS applications can be started or stopped with the operating mode switch or the CODESYS programming interface.

To launch CODESYS applications via the CODESYS programming interface, the operating mode switch must be in the "RUN" position.

CODESYS application launch and halt events are recorded in the log system (event logging).

7.3.1 Launching CODESYS Applications

- Set the operating mode switch to "RUN."
- ➔ The CODESYS applications start.
- ➔ The "RUN" LED lights up green.

7.3.2 Halting CODESYS Applications

- Set the operating mode switch to "STOP."
- ➔ All CODESYS applications are halted.
- ➔ The "RUN" LED goes out.

The CODESYS applications cannot be launched via the CODESYS programming interface when the operating mode switch is in the "STOP" position.

7.4 Backing Up and Restoring Data

Note

Note the firmware version!

The Restore function is only possible if the firmware versions are the same at the time of backup and restoration.

7.4.1 Performing a Backup

1. In the ribbon, click **[Backup/Restore]**.
2. In the "Storage location" selection box, choose the network/PC folder or removable media where you want to store the backup.
3. Under "Backup," enter the password with which you want to save the backup file in encrypted form and repeat the password entry.
 - ⇒ **Note: Keep your password safe!**
The password is required to restore the backup. Without the correct password, access to the secured data is no longer possible.
 - ⇒ **Note: Protect backup file and password from unauthorized access!**
With knowledge of the password and access to the backup file, it is possible to indirectly change the device configuration.

4. Click **[Start backup process]**.

- ⇒ Settings and user data as well as the CODESYS application are compiled as a backup on the device and then downloaded from the device to the engineering PC as a backup file (*.7zip). A percentage indicator shows you when the download is complete.
- ⇒ Unless your browser is configured differently, you will find the downloaded file in your "Downloads" folder (browser-dependent).

➔ The backup process is complete.

7.4.2 Performing a Restore

Please note the following information when restoring your data:

- The restore process may take a few minutes. After the restore process, the device is restarted and is then ready for use again.
- Please note that device data is overwritten according to the contents of the selected backup. If you change connection-related data (e.g., the IP address) after creating the backup, it may not be possible to establish a connection to the device during an automatic restart during the restore process.
- Make sure you have the correct login details (username/password) for the device, as they may have changed.
- Make sure that the device is physically accessible during and after the restore process: A network connection must be established via a suitable medium (e.g., cable, WLAN) for the entire duration of the restore process.
- Make sure you have any changed IP addresses/device addresses/DHCP server addresses at hand.
- Data recovery may fail if there is insufficient free memory on the device.

1. In the ribbon, click **[Backup/Restore]**.

2. In the "Restore" area, select the source of your backup file.

- ⇒ If you select the file system as the source, a storage area  is displayed.

3. Under "Restore," enter the password with which you have saved the backup file.

4. Drag the backup file (*.7zip) to the storage area.

Alternatively, click **[Browse]** and select a backup file.

- ⇒ The file name of the selected backup file is displayed. Click **[Choose another file]** to change the backup file as needed.

5. To restore the data from the selected backup file, click **[Start restore process]**.

- ⇒ The backup file is first loaded onto the device. The restore process on the device then starts automatically.
You are notified on the display if the data has been restored successfully.
- ⇒ If the device can no longer be accessed, for example due to changed IP address, you are prompted to manually open the WBM of the device with the new IP address in the browser.

➔ The restore process is complete.

7.5 WDX Methods for Production

The following WDX methods are only applicable for production:

- Manufacturing/ExecuteCommand "CODESYSLicense" <license file>
- Manufacturing/ExecuteCommand "DeviceIdentityCert" <PEM certificate>

They can only be called once.

Repeated calls by default user accounts are not possible and triggers an error message!

7.6 Creating and Managing Certificates

7.6.1 Creating Device Certificates

Device certificates (certificate files and associated private key files) can be created in two ways:

1. Directly on the controller with subsequent signing via an external PKI
2. Via a connected enrollment server with automatic signing

7.6.1.1 Self-Signed Certificates

Self-signed device certificates (the certificate file and the associated private key file) can be generated directly on the controller.

Self-signed device certificates can then be signed manually via an external PKI.

To generate a self-signed certificate file and the associated private key file and then sign it manually via an external PKI, proceed as follows:

1. Open the "Device Certificates" page in the WBM or WAGO Device Manager.
2. Click the **[Create Certificate]** button in the "Device Status/Actions" area.
 - ⇒ The "CertStore/Device/CreateCertificate" pop-up window appears.
3. Select the key type (RSA:2048/RSA:4096/EC:prime256v1) in the "KeyType" drop-down box.
4. Enter a name for the certificate in the DistinguishedName field. This name is displayed as a comment in the list of certificates. The name syntax is specified according to "RFC 4514." Help is displayed as you type.
5. Click the **[Create Certificate]** button.
6. Close the pop-up window.
 - ⇒ The certificate that has been generated appears in the "Settings" area in the "Current Values" column as a new entry "DeviceCertificate <n> (<Name>)" ; for its name, the name from the "DistinguishedName" field is used.
7. Click the **[Apply as Target Values]** button.
 - ⇒ The certificate appears in the "Target Values" column.
8. In the "Device Status/Actions" area, click the **[Create Signing Request]** button for the certificate that has just been generated.
 - ⇒ The "CertStore/Device/Certificates/2/CreateSigningRequest" pop-up window opens.
9. In the "DistinguishedName" field, reenter the name for the certificate you want to sign.
10. Click the **[Create Signing Request]** button.
 - ⇒ The software indicates the status and outputs a certificate file in text form.

11. Copy this text file for signing via the external PKI.
12. Once the certificate file has been successfully signed, load this file back onto the controller.
13. To do this, open the drop-down menu for selecting the size.
14. Click on the **[Select]** menu item.
 - ⇒ A file manager window opens.
15. Navigate to the signed file and import it.
16. Click the **[Write to Device]** button to apply the change.
 - ⇒ The certificate is displayed in the Device Status/Actions area; for the name, the name in the "DistinguishedName" field is used.
- ➔ The certificate can now be used.

7.6.1.2 Certificates Signed via an External PKI

Device certificates (the certificate file and the associated private key file) can be generated and automatically signed via an external PKI when the controller is connected to an enrollment server.

To establish a connection to an enrollment server, proceed as follows:

1. Open the "Device Certificates" page in the WBM or WAGO Device Manager.
2. Enter the hostname of the server and the authentication data in the "CertStore/EnrollmentServer" group in the "Settings" area.
3. Use the "Verbose" checkbox to determine whether detailed information on the connection should be logged.
4. Select a root certificate in the "CA Certificate" drop-down menu to verify the connection.
5. Click the **[Write to Device]** button to apply the settings in the controller.
- ➔ The settings appear in the "Current Values" column.

To generate a certificate file and the associated private key file and sign it automatically via an external PKI, proceed as follows:

1. In the "Device Status/Actions" area, click the **[Create Certificate with Enrollment]** button.
 - ⇒ The "CertStore/Device/CreateCertificateWithEnrollment" pop-up window opens.
2. Select the key type ("RSA:2048"/"RSA:4096"/"EC:prime256v1") in the "KeyType" drop-down box.
3. Enter a name for the certificate in the DistinguishedName field. This name is displayed as a comment in the list of certificates. The name syntax is specified according to "RFC 4514." Help is displayed as you type.
4. Enter the authentication data ("AuthUser" and "AuthPassword") for the enrollment server.
5. Click the **[Create Certificate with Enrollment]** button.
6. Close the pop-up window.
 - ⇒ The certificate that has been generated appears in the "Settings" area in the "Current Values" column as a new entry "DeviceCertificate <n> (<Name>); for its name, the name from the "DistinguishedName" field is used.

7. Click the **[Apply as Target Values]** button.
 - ⇒ The certificate appears in the "Target Values" column.
8. Check the "Automatic Renewal" box if you want the certificate to be automatically renewed. Automatic renewal is only possible if the controller is connected to an enrollment server.
9. Click the **[Write to Device]** button to apply the change.
 - ⇒ The certificate is displayed in the Device Status/Actions area; for the name, the name in the "DistinguishedName" field is used.
- ➔ The certificate can now be used.

7.6.2 Loading Externally Created and Signed Device Certificates

Externally created and signed device certificates (the certificate file and the associated private key file) can be loaded directly onto the controller.

To load an externally created and signed certificate file and the associated private key file onto the controller, proceed as follows:

1. Open the "Device Certificates" page in the WBM or WAGO Device Manager.
2. In the "DeviceCertificate List" group in the "Settings" area, click the **[+ DeviceCertificate]** button.
 - ⇒ A new "DeviceCertificate <n>" entry is created.
3. In the "Certificate" field, open the drop-down menu when "Not set" appears.
4. Click on the **[Select]** menu item.
 - ⇒ A file manager window opens.
5. Navigate to the certificate file and import it.
6. Enter a name for the certificate in the "Comment" field. This name is displayed as a comment in the list of certificates.
7. In the "Private Key" field, open the drop-down menu when "Not set" appears.
8. Click on the **[Select]** menu item.
 - ⇒ A file manager window opens.
9. Navigate to the key file and import it.
10. Check the "Automatic Renewal" box if you want the certificate to be automatically renewed. Automatic renewal is only possible if the controller is connected to an enrollment server.
11. Click the **[Write to Device]** button to apply the change.
 - ⇒ The certificate appears in the Device Status/Actions area; for the name, the contents of the "Comment" field are used.
- ➔ The certificate can now be used.

8 Diagnostics

8.1 Diagnostics via Indicators

Various indicators on the device signal the device's status and system status.

The number, design and arrangement of the indicators is product-specific.

For a detailed description of the diagnostics via indicators, see the section "Diagnostics via Indicators" in the respective product manual.

8.2 Diagnostics via WBM

You can use various diagnostic functions to determine the status of the device via the WAGO Device Manager.

- Test the device wiring (see [I/O Check \[p. 51\]](#), [Testing the Wiring \[p. 93\]](#)).
- View the status of the device in relation to certain settings. You can find the device status in the lower area "Device Status/Actions" of the various tabs in the "Settings" view.
- View the LED status of the device in the "Settings" view on the "LEDs" tab.
- The status of the application is indicated by the "PLC" LED indicator in the "Device" area on the left (see [Device \[p. 50\]](#)).
- The "Device Log" view displays device log entries (see [Device Log \[p. 61\]](#), [Viewing the Device Log \[p. 94\]](#)).
- For current (error) messages and information generated during configuration, see the message window (see [Message Window \[p. 62\]](#)).

8.2.1 Testing the Wiring

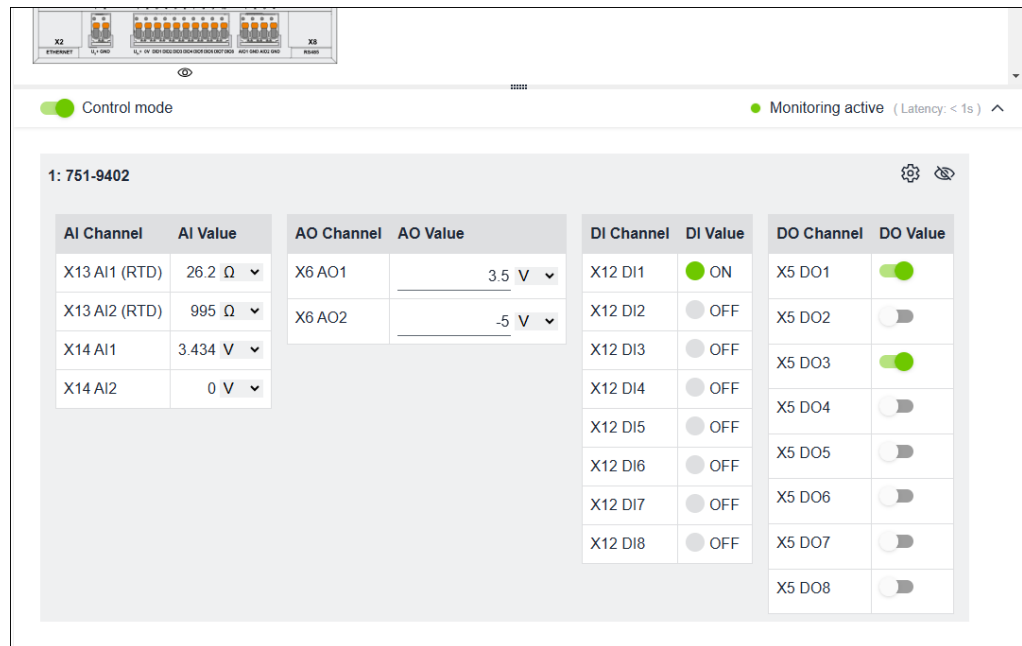
In the I/O Check view, you can perform a wiring test for conventional analog and digital inputs/outputs of a device. Output signals can be set for test purposes ("control mode") or input states can be read into the corresponding physical unit. If the states are visualized on the device itself, e.g., via an LED, the state is displayed in the form of an LED highlighted in a corresponding color.

1. Open the "I/O Check" view.
2. Click the eye icon  below the device graphic.
 - ⇒ Monitoring is enabled , i.e., current status values are displayed in tabular form.
 - ⇒ The latency indicates the update cycle of the displayed device values depending on the connection, device load or other factors.
3. Compare the displayed values with your hardware, e.g., whether the green LED actually lights up on your device.
4. Besides value monitoring, you can also write or read them. Use the slider to switch to control mode.



5. Change the individual values. For this purpose, use input fields for analog output modules and slide switches for digital output modules.

Note: Changes are not collected, writing is performed continuously during input.



8.2.2 Viewing the Device Log

- Open the "Device Log" tab.

You have two options to view log entries:

1. To display device log entries directly in the "Device Log" tab, click **[Retrieve log entries]**.
2. To retrieve device log entries and save them to a file, first select the desired **File output format** ("TXT" or "CSV"). Then click **[Retrieve log entries as a file]**.

⇒ By default, the last 100 log entries that have at least the "Informational" log level are displayed or saved.

Filter Log Entries

You have various options for filtering log entries and thus reducing long lists.

- Specify a **Maximum number of entries**:
Up to 1,000 log entries when displayed directly, or up to 100,000,000 log entries when stored in a file.
- Select the **Log Level** that should be displayed at a minimum.
Log levels indicate the severity or urgency of a log entry.
Tip: You can configure which log levels are generally logged via the "Settings" > "Logging" tab.
- Enter a string by which the **Log sources** of the entries should be filtered.
- Under **Log entries** select the point in time from which log entries are displayed. To do this, check the box and select the time and date from the calendar widget.

Configure Logging

The "Device Log" tab is used to display and filter log entries. You can configure which events are logged by the device in a different area of the interface:

1. Open the "Settings" tab.
2. Open the "Logging" page.
3. Here, for example, you can change the setting so that log entries are created starting at "Debug" log level.
4. You can also adjust the memory size reserved for the log entries.
5. You can connect an external logging server if required on the "RemoteLogging" page.

8.3 Checking System Integrity

The system can calculate a checksum for the configuration upon request.

To calculate this, use the [**Calculate Config Checksum**] button on the "Information" page in the WBM or WAGO Device Manager or call the WdX method "Security/CalculateConfigChecksum."

The checksum remains the same if the configuration is not modified.

If parameters are modified and the modifications are then undone, the checksum may not be the same as before the modification.

Testing procedure:

1. Generate the checksum for the configuration.
2. View the checksum.
3. Write down the checksum and keep it for later comparison.
4. Repeat this procedure regularly to detect unauthorized changes in the configuration by comparing checksums.
5. After each authorized change, generate the checksum and store it (see above).

List of Tables

Table 1	"Device Status/Actions" – "Security"	23
Table 2	"Settings" – "Account Management/PasswordQuality"	24
Table 3	"Device Status/Actions" – "Account Management"	25
Table 4	"Settings" – "SystemUser 2 (admin)"	25
Table 5	"Device Status/Actions" – "Account Management"	26
Table 6	"Settings" – "SystemUser 1 (root)"	26
Table 7	"Settings" – "User List"	26
Table 8	"Settings" – "UserRole List"	27
Table 9	"Settings" – "OAuth2Server"	29
Table 10	"Device Status/Actions" – "OAuth2Server"	29
Table 11	"Settings" – "Logging"	30
Table 12	"Settings" – "RsyslogClientConfig 1"	31
Table 13	"Device Status/Actions" – "Identity"	32
Table 14	"Device Status/Actions" – "Version"	32
Table 15	"Settings" – "Time Zone"	32
Table 16	"Device Status/Actions" – "UTC"	33
Table 17	"Device Status/Actions" – "Local Device Time"	33
Table 18	"Settings" – "NTPClient"	33
Table 19	"Settings" – "CertStore/CA"	36
Table 20	"Settings" – "CACertificate List"	36
Table 21	"Settings" – "CertificateRevocationList List"	36
Table 22	"Device Status/Actions" – "CertificateRevocationList List"	37
Table 23	"Settings" – "DeviceCertificate List"	37
Table 24	"Settings" – "CertStore/EnrollmentServer"	37
Table 25	"Device Status/Actions" – "CertStore/Device"	38
Table 26	"Device Status/Actions" – "DeviceCertificate List"	38
Table 27	"Device Status/Actions" – "IdentityCertificate <n>"	38
Table 28	"Settings" – "Webserver"	38
Table 29	"Settings" – "Webserver Application <n>"	39
Table 30	"Settings" – "Webserver CORS Policy <n>"	39
Table 31	"Device Status/Actions" – "FOSS Module List"	40
Table 32	"Settings" – "WAGOdeviceAccess"	40
Table 33	"Device Status/Actions" – "Factory Settings"	41
Table 34	Operating mode switch	41
Table 35	Reset Button	42
Table 36	"Settings" – "USB Service Interface"	42

Table 37	Process Image - Analog Inputs AI1, AI2	43
Table 38	Process Image – Process Values AI; 0 ... 10 V; 16 Bit; WORD	43
Table 39	Process Image – Process Values AI; –10 ... +10 V; 16 Bit; WORD	43
Table 40	Process Image – Process Values AI; 0 ... 20 mA; 16 Bit; WORD	43
Table 41	Process Image – Process Values AI; 4 ... 20 mA; 16 Bit; WORD	44
Table 42	Process Image – Process Values AI; 3.6 ... 21 mA; 16 Bit; WORD	44
Table 43	Process Image – Analog Inputs/Outputs AIO1, AIO2.....	44
Table 44	Process Image – Process Values AO; 0 ... 10 V; 16 Bit; WORD	45
Table 45	Process Image – Process Values AO; –10 ... +10 V; 16 Bit; WORD.....	45
Table 46	Process Image – Process Values AO; –12 ... +12 V; 16 Bit; WORD.....	45
Table 47	Process Image – Process Values AO; 0 ... 20 mA; 16 Bit; WORD	45
Table 48	Process Image – Process Values AO; 0 ... 22 mA; 16 Bit; WORD	46
Table 49	Process Image – Process Values AO; 4 ... 20 mA; 16 Bit; WORD	46
Table 50	Process Image – Temperature Inputs PT1+/PT1–, PT2+/PT2–	46
Table 51	Process Image – Process Values RTD; Pt100, Pt200, Pt500, Pt1000; –200 ... +850 °C; 16 Bit; INT	47
Table 52	Process Image – Process Values RTD; Ni100, Ni1000 (Tk6180), Ni1000 (TK5000); – 60 ... +250 °C; 16 Bit; INT	47
Table 53	Process Image – Process Values RTD; Ni120; –80 ... +260 °C; 16 Bit; INT	47
Table 54	Process Image – Process Values RTD; Potentiometer; 0 ... 1200 Ohm; 16 Bit; INT.....	47
Table 55	Process Image – Process Values RTD; Potentiometer; 0 ... 5000 Ohm; 16 Bit; INT.....	48
Table 56	Process Image – Digital Inputs DI1 ... DI8	48
Table 57	Process Image – Process Values of Digital Inputs – BOOL.....	48
Table 58	Process Image – Digital Inputs/Outputs DIO1 ... DIO8.....	48
Table 59	Process Image – Process Values of Digital Inputs – BOOL.....	49
Table 60	Process Image – Process Values, Digital Outputs – BOOL	49
Table 61	Icons and Controls in the “Settings” View.....	58
Table 62	File Handling	58
Table 63	“Settings” – “Bridge Configuration”	64
Table 64	“Settings” – “Bridge 1 ... Bridge <n>”	64
Table 65	“Settings” – “Networking/StormProtection”	65
Table 66	“Settings” – “EthernetPort 1 ... EthernetPort <n>”	66
Table 67	“Device Status/Actions” – “Bridge <n> (br<n-1>)”	66
Table 68	“Device Status/Actions” – “EthernetPort <n> (X<n>)”	66
Table 69	“Settings” – “FirewallMACFilterRule List”	68
Table 70	“Settings” – “FirewallIPFilterIncomingRule List”	69
Table 71	“Settings” – “FirewallIPFilterForwardingRule List”	70
Table 72	“Settings” – “IKEConnection”	71

Table 73	"Settings" – "IPsecTunnel"	71
Table 74	"Device Status/Actions" – "IPsecTunnel"	72
Table 75	"Settings" – "Automount"	73
Table 76	ETHERNET Communication Default.....	77
Table 77	"Settings" – "Account Management/PasswordQuality"	78

List of Figures

Figure 1	Onion Pattern (Example)	14
Figure 2	Reference Architecture.....	15
Figure 3	Graphical User Interface.....	49
Figure 4	Connected Device	50
Figure 5	"I/O Check" View (Example).....	51
Figure 6	Device Status Indicators (Example)	52
Figure 7	Channel Status Indicators (Example)	52
Figure 8	Monitoring active (Example).....	53
Figure 9	Control Mode Active (Example)	54
Figure 10	"Settings" View (Example).....	56
Figure 11	"Reboot" View	59
Figure 12	"Firmware" View.....	59
Figure 13	"Backup/Restore" View	60
Figure 14	"Device log" View.....	61
Figure 15	Message bar	62
Figure 16	Message window	63
Figure 17	"Device log" View.....	75

WAGO GmbH & Co. KG

Postfach 2880 · D - 32385 Minden
Hansastraße 27 · D - 32423 Minden

✉ info@wago.com
🌐 www.wago.com

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

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Copyright – WAGO GmbH & Co. KG – All rights reserved. The content and structure of the WAGO websites, catalogs, videos and other WAGO media are subject to copyright. Distribution or modification of the contents of these pages and videos is prohibited. Furthermore, the content may neither be copied nor made available to third parties for commercial purposes. Also subject to copyright are the images and videos that were made available to WAGO GmbH & Co. KG by third parties.