SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE WxM763

Operating Instructions

Introduction 1

Safety notices 2

Security recommendations 3

Description of the device 4

Installation and removal 5

Connection 6

Maintenance and cleaning 7

Troubleshooting 8

Technical data 9

Dimension drawings 10

Approvals 11

08/2023
C79000-G8976-C653-04

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C653-04
Ⓟ 08/2023 Subject to change

Copyright © Siemens AG 2022 - 2023.
All rights reserved

Table of contents

1 Introduction 5

1.1 Purpose of the Operating Instructions 5

1.2 Scope of the manual 5

1.3 Supplementary documentation 5

1.4 Further documentation 6

1.5 Cybersecurity information 6

1.6 Firmware 7

1.7 Error/fault 7

1.8 Decommissioning 7

1.9 Recycling and disposal 8

1.10 Marken 8

2 Safety notices 9

3 Security recommendations 11

3.1 Security recommendations 11

3.2 Available services 15

4 Description of the device 19

4.1 Structure of the type designation 19

4.2 Structure of the article number 19

4.3 Device view 20

4.4 Components of the product 21

4.5 Terminals 22

4.6 Accessories 23
4.6.1 Installation 23
4.6.2 CLP 23
4.6.3 Industrial Ethernet 24
4.6.4 Flexible connecting cables, antennas and accessories 25
4.6.4.1 Flexible connecting cables 25
4.6.4.2 Lightning protection 26
4.6.4.3 Terminating resistor 26
4.6.4.4 Cabinet feedthrough 26
4.6.4.5 Antennas 26

4.7 LED display 28

4.8 Reset button 31

4.9 Configuration License PLUG 32

5 Installation and removal 35
5.1 Safety during mounting 35
5.2 Types of installation 38
5.3 Wall mounting 39
5.4 Installing on the DIN rail 41
5.4.1 Mounting directly on the DIN rail 41
5.4.2 Mounting rotated by 90° with DIN rail mounting adapter 42
5.5 Installing on an S7-300 mounting rail 45
5.6 Installing on an S7-1500 mounting rail 46
6 Connection 49
6.1 Safety when connecting up 49
6.2 Power supply 55
6.3 Ethernet 56
6.4 Antennas 57
6.5 Digital input/output 58
6.6 Grounding 60
6.7 Replacing a CLP 61
7 Maintenance and cleaning 63
8 Troubleshooting 65
8.1 Downloading new firmware using TFTP without WBM and CLI 65
8.2 Restoring the factory settings 66
9 Technical data 69
10 Dimension drawings 73
11 Approvals 75
Index 77

Introduction 1

1.1 Purpose of the Operating Instructions

Using the Operating Instructions, you will be able to install and connect the SCALANCE WxM763-1 correctly. The instructions are aimed primarily at planning, commissioning, maintenance and service personnel.

The configuration and the integration of the device in a WLAN are not described in these instructions.

1.2 Scope of the manual

These operating instructions cover the following products:

Product	Article number	Certification ID
Access points		
SCALANCE WAM763-1	6GK5763-1AL00-7DA0 (DI/DO) 6GK5763-1AL00-7DB0 (US) (DI/DO) 6GK5763-1AL00-7DC0 (ME) (DI/DO)	MSAX-W1-RJ-E2
Client		
SCALANCE WUM763-1	6GK5763-1AL00-3AA0 6GK5763-1AL00-3AB0 (US)	MSAX-W1-RJ-E2-NO
	6GK5763-1AL00-3DA0 (DI/DO) 6GK5763-1AL00-3DB0 (US) (DI/DO)	MSAX-W1-RJ-E2

These operating instructions apply to the following firmware version:

- SCALANCE W700 IEEE 802.11ax as of version 2.2

Definition

An access point is a node in a WLAN that also performs administrative functions in the network and, for example, provides client modules with a connection to wired networks, to other client modules in the same wireless cell or in other wireless cells.

1.3 Supplementary documentation

Documentation on the Internet

You can find the current version of the document on the Internet at (https://support.industry.siemens.com/cs/de/en/ps/28575/man)

Enter the name or article number of the product in the search filter.

Documentation on configuration

You can find detailed information on configuring and planning the devices in the following configuration manuals:

- SCALANCE W700 nach IEEE 802.11ax Web Based Management
- SCALANCE W700 nach IEEE 802.11ax Command Line Interface
- SCALANCE W700 802.11ax approvals
- Performance data SCALANCE W700 802.11ax

1.4 Further documentation

In the system manuals "Industrial Ethernet / PROFINET Industrial Ethernet" and "Industrial Ethernet / PROFINET passive network components", you will find information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network.

There, you will find among other things optical performance data of the communications partner that you require for the installation.

You will find the system manuals here:

- On the Internet pages of Siemens Industry Online Support under the following entry IDs:
  - 27069465 (https://support.industry.siemens.com/cs/de/en/view/27069465)
    Industrial Ethernet / PROFINET Industrial Ethernet System Manual
  - 84922825 (https://support.industry.siemens.com/cs/de/en/view/84922825)
    Industrial Ethernet / PROFINET - Passive network components System Manual

The RCoax system manual contains both an explanation of the basic technical aspects as well as a description of the individual RCoax components and their mode of operation. Installation/ commissioning and connection of RCoax components and their operating principle are explained. The possible applications of the various SIMATIC NET components are described.

You can find the RCoax system manual on the Internet pages of Siemens Industry Online Support under the following entry ID:

- 109480869 (https://support.industry.siemens.com/cs/de/en/view/109480869)
  SIMATIC NET: Industrial Wireless LAN RCoax

1.5 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected

to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/global/en/products/services/cert.html (https://new.siemens.com/global/en/products/services/cert.html).

1.6 Firmware

The firmware is available on the Internet pages of the Siemens Industry Online Support: (https://support.industry.siemens.com/cs/ww/en/ps/28575/dl)

Note on firmware/software support

Check regularly for new firmware/software versions or security updates and apply them. After the release of a new version, previous versions are no longer supported and are not maintained.

1.7 Error/fault

If a fault develops, send the device to your SIEMENS representative for repair. Repairs on-site are not permitted.

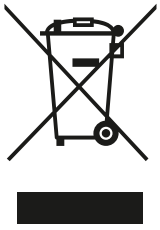
1.8 Decommissioning

Shut down the device properly to prevent unauthorized persons from accessing confidential data in the device memory.

To do this, restore the factory settings on the device.

Also restore the factory settings on the storage medium.

1.9 Recycling and disposal



The products are low in pollutants, can be recycled and meet the requirements of the WEEE directive 2012/19/EU for the disposal of electrical and electronic equipment.

Do not dispose of the products at public disposal sites.

For environmentally friendly recycling and the disposal of your old device contact a certified disposal company for electronic scrap or your Siemens contact (Product return (https://support.industry.siemens.com/cs/ww/en/view/109479891)).

Note the different national regulations.

1.10 Marken

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SCALANCE, RCoax

Safety notices

2

⚠ CAUTION

To prevent injury and damage, read the manual before using the device.

Read the safety notices

Note the following safety notices. These relate to the entire working life of the device.

You should also read the safety notices relating to handling in the individual sections, particularly in the sections "Installation" and "Connecting up".



⚠ WARNING

Hot surfaces

Electric devices have hot surfaces. Do not touch these surfaces. They could cause severe burns.

- Allow the device to cool down before starting any work on it.

⚠ WARNING

EXPLOSION HAZARD

Do not open the device when the supply voltage is turned on.

Security recommendations 3

3.1 Security recommendations

To prevent unauthorized access to the device and/or network, observe the following security recommendations.

General

- Check the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate the security of your location and use a cell protection concept with suitable products (https://www.siemens.com/industrialsecurity).
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- No product liability will be accepted for operation in a non-secure infrastructure.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (IPsec, OpenVPN).
- Separate connections correctly (WBM, SSH etc.).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central logging server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.

WLAN

- We recommend that you ensure redundant coverage for WLAN clients.
- More information on data security and data encryption for SCALANCE W is available in SCALANCE W: Setup of a Wireless LAN in the Industrial Environment (https://support.industry.siemens.com/cs/ww/en/view/22681042)

Authentication

Note

Accessibility risk - Risk of data loss

Do not lose the passwords for the device. Access to the device can only be restored by resetting the device to factory settings which completely removes all configuration data.

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- Define rules for the assignment of passwords.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
  This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that passwords are protected and only disclosed to authorized personnel.
- Do not use the same passwords for multiple user names and systems.
- Store the passwords in a safe location (not online) to have them available if they are lost.
- Regularly change your passwords to increase security.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- When user authentication is performed via RADIUS, make sure that all communication takes place within the security environment or is protected by a secure channel.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP or IPv4. An attacker could use vulnerabilities in these protocols to attack hosts, switches and routers connected to your layer 2 network, for example, through manipulation (poisoning) of the ARP caches of systems in the subnet and subsequent interception of the data traffic. Appropriate security measures must be taken for non-secure layer 2 protocols to prevent unauthorized access to the network. Physical access to the local network can be secured or secure, higher layer protocols can be used, among other things.

Certificates and keys

- There is a preset SSL/TLS (RSA) certificate with 4096 bit key length in the device. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate via the WBM ("System > Load and Save").
- Use certificates with a key length of 4096 bits.
- Use the certification authority including key revocation and management to sign the certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.
- Use password-protected certificates in the format "PKCS #12".
- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Physical/remote access

- Operate the devices only within a protected network area. Attackers cannot access internal data from the outside when the internal and the external network are separate from each other.
- Limit physical access to the device exclusively to trusted personnel.
  The memory card or the PLUG (C-PLUG, KEY-PLUG, CLP) contains sensitive data such as certificates and keys that can be read out and modified. An attacker with control of the device's removable media could extract critical information such as certificates, keys, etc. or reprogram the media.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.
- We highly recommend that you keep the protection from brute force attacks (BFA) activated to prevent third parties from gaining access to the device. For more information, see the configuration manuals, section "Brute Force Prevention".
- For communication via non-secure networks, use additional devices with VPN functionality to encrypt and authenticate communication.
- When you establish a secure connection to a server (e.g. for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTP, HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it. For more information, refer to "Decommissioning (Page 7)".
- We recommend formatting a PLUG that is not being used.

Hardware / Software

- Use VLANs whenever possible as protection against denial-of-service (DoS) attacks and unauthorized access.
- Restrict access to the device by setting firewall rules or rules in an access control list (ACL).
- Selected services are enabled by default in the firmware. It is recommended to enable only the services that are absolutely necessary for your installation.
  For more information on available services, see "List of available services (Page 15)".
- To ensure you are using the most secure encryption methods available, use the latest web browser version compatible with the product. Also, the latest web browser versions of Mozilla Firefox, Google Chrome, and Microsoft Edge have 1/n-1 record splitting enabled, which reduces the risk of attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (for example, BEAST).
- Ensure that the latest firmware version is installed, including all security-related patches. You can find the latest information on security patches for Siemens products at the Industrial Security (https://www.siemens.com/industrialsecurity) or ProductCERT Security Advisories (https://www.siemens.com/cert) website.
  For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.
- Enable only those services that are used on the device, including physical ports. Free physical ports can potentially be used to gain access to the network behind the device.

- Use the authentication and encryption mechanisms of SNMPv3 if possible. Use strong passwords.
- Configuration files can be downloaded from the device. Ensure that configuration files are adequately protected.
  Configuration files can be password protected during download. You enter passwords on the WBM page "System > Load & Save > Passwords".
- When using SNMP (Simple Network Management Protocol):
  - Configure SNMP to generate a notification when authentication errors occur.
    For more information, see WBM "System > SNMP > Notifications".
  - Ensure that the default community strings are changed to unique values.
  - Use SNMPv3 whenever possible. SNMPv1 and SNMPv2c are considered non-secure and should only be used when absolutely necessary.
  - If possible, prevent write access.
- Use the security functions such as address translation with NAT (Network Address Translation) or NAPT (Network Address Port Translation) to protect receiving ports from access by third parties.
- Use WPA2/ WPA2-PSK / WPA3-SAE with AES to protect the WLAN. You can find additional information in the configuration manual Web Based Management "Security menu".
- Use PMF (Protected Management Frames) to cryptographically protect the management telegrams. You can find additional information in the configuration manual Web Based Management "Security menu".

Secure/ non-secure protocols

- Use secure protocols if access to the device is not prevented by physical protection measures.
- Disable or restrict the use of non-secure protocols. While some protocols are secure (e.g. HTTPS, SSH, 802.1X, etc.), others were not designed for the purpose of securing applications (e.g. SNMPv1/v2c, etc.).
  Therefore, take appropriate security measures against non-secure protocols to prevent unauthorized access to the device/network. Use non-secure protocols on the device using a secure connection (e.g. SINEMA RC).
- If non-secure protocols and services are required, ensure that the device is operated in a protected network area.

- Check whether use of the following protocols and services is necessary:
  - Non-authenticated and unencrypted ports
  - LLDP
  - Syslog
  - DHCP options 66/67
  - TFTP
  - Telnet
  - HTTP
  - SNMP v1/2c
  - SNTP
- The following protocols provide secure alternatives:
  - SNMPv1/v2c → SNMPv3
    Check whether use of SNMPv1/v2c is necessary. SNMPv1/v2c is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options.
    If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
    Use SNMPv3 in conjunction with passwords.
  - HTTP → HTTPS
  - Telnet → SSH
  - TFTP → SFTP
  - Syslog Client → Syslog Client TLS
- Using a firewall, restrict the services and protocols available to the outside to a minimum.
- For the DCP function, enable the "Read Only" mode after commissioning.

3.2 Available services

List of available services

The following is a list of all available services and their ports through which the device can be accessed.

The table includes the following columns:

- **Service**
  The services that the device supports.
- **Protocol/port number**
  Port number assigned to the protocol.
- **Default status**
  The default status of the ports/service (e.g. open, closed, outgoing only).

- **Configurable port/service**
  Indicates whether the port number or the service can be configured via WBM / CLI.
- **Authentication**
  Specifies whether the communication partner is authenticated.
  If "optional", the authentication can be configured as required.
- **Encryption**
  Specifies whether the transfer is encrypted.
  If "optional", the encryption can be configured as required.

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [1]
			Port	Service		
DHCP Client IPv4	UDP/68	Outgoing only	--	✓	--	--
DHCP Client IPv6	UDP/546	Outgoing only	--	✓	--	--
DNS Client	TCP/53 UDP/53	Outgoing only	--	✓	--	--
HTTP	TCP/80	Open	✓	✓	✓	--
HTTPS	TCP/443	Open	✓	✓	✓	✓
NTP- Client	UDP/123	Outgoing only	✓	✓	--	--
Packet Capture	TCP/2002 TCP/2003 [2]	Closed	--	✓	--	--
PROFINET	UDP/34964 UDP/49154 UDP/49155	Open	--	✓	--	--
RADIUS	UDP/1812	Outgoing only	✓	✓	✓	--
SFTP Server	TCP/22	Closed	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	--	--
SMTP (secure)	TCP/465	Closed	✓	✓	Optional	✓
SNMPv1/v2c	UDP/161	Open	✓	✓	--	--
SNMPv3	UDP/161	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outgoing only	--	✓	--	--
SNTP Client	UDP/123	Outgoing only	✓	✓	--	--
SSH	TCP/22	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Closed	✓	✓	--	--
Syslog Client TLS	TCP/6514	Closed	✓	✓	--	✓
Telnet	TCP/23	Closed	✓	✓	✓	--
TFTP Server	UDP/69	Closed	✓	✓	--	--
TCP Event	TCP/26864	Closed	✓	✓	✓	--

[1] You can find additional information on the encryption methods used in the WBM appendix "Ciphers used".

[2] The basic port of Packet Capture for the communication to Wireshark is TCP/2002. For each enabled interface, another port is enabled. Each additional port is an increment of TCP/2002, i.e. TCP/2003, TCP/2004, TCP/2005 etc.

The following is a list of all available Layer 2 services through which the device can be accessed.

The table includes the following columns:

- **Layer 2 service**
  The Layer 2 services that the device supports**.**
- **Default status**
  The default status of the service (open or closed).
- **Service configurable**
  Indicates whether the service can be configured via WBM / CLI.

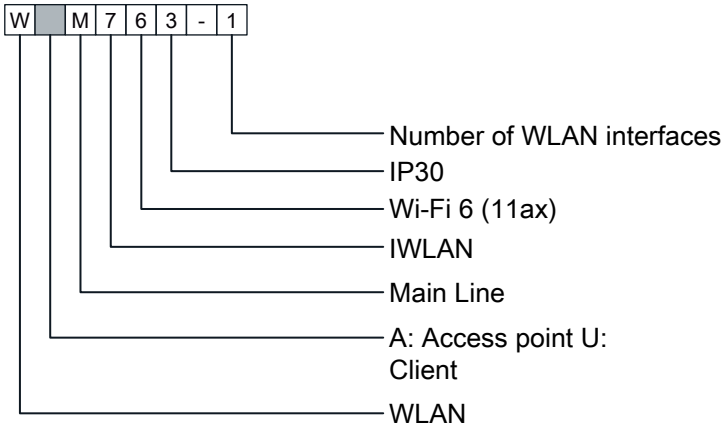
Layer 2 service	**Default status**	**Service configurable**
DCP	Open	✓
LLDP	Open	✓
RSTP	Closed	✓
iPRP	Closed	✓
MSTP	Closed	✓
SIMATIC NET TIME	Closed	✓
802.1x	Closed	✓

Description of the device

4

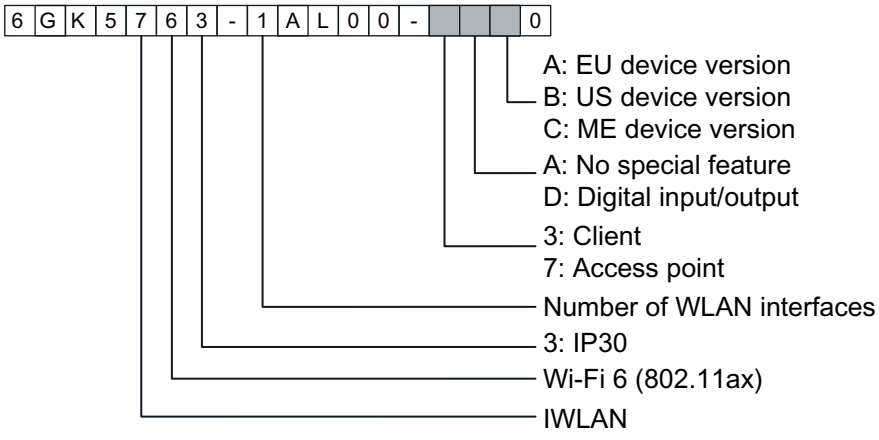
4.1 Structure of the type designation

The type designation of the device is made up of several parts that have the following meaning:

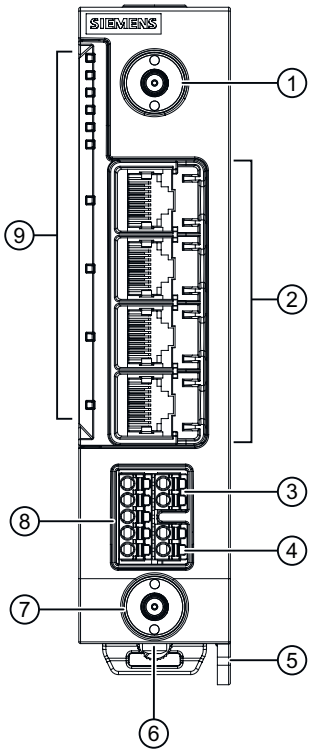


4.2 Structure of the article number

The article number of the device is made up of several parts that also reflect the properties of the device:



4.3 Device view



① Antenna connector R1A1, type R-SMA
② Ethernet connectors (P1, P2, P3, P4)
③ Digital input (DI)
Only SCALANCE WxM763-1 with DI/DO; see Scope of the manual (Page 5)
④ Digital output (DO)
Only SCALANCE WxM763-1 with DI/DO; see Scope of the manual (Page 5)
⑤ Eye for grounding (diameter 4.6 mm) / wall mounting
⑥ On the bottom of the device behind the screw-on cover:
- PLUG slot (CLP)
- Reset button
  For the position, see "Reset button (Page 31)".

On the bottom of the device at the location of the screw-on cover:
- Two mounting holes for mounting the mounting adapter for the 90^0 mounting on a DIN rail

⑦ Antenna connector R1A2, type R-SMA
⑧ Power supply connection
⑨ LED display

4.4 Components of the product

The following components are supplied with the product:

- One SCALANCE W device
- One cover for CLP slot
- A 5-pin plug-in terminal block for the power supply
- Two covers for R-SMA connectors

The device variant with digital input/output also includes:

- A 2-pin plug-in terminal block for the digital output
- A 2-pin plug-in terminal block for the digital input

Please check that the consignment you have received is complete. If the consignment is incomplete, contact your supplier or your local Siemens office.

Note

Not included with the product

The following components do not ship with the product:

- Removable data storage medium CLP
- Antennas
- Mounting adapter for 90^0 mounting on an DIN rail

You will find more detailed information in "Accessories (Page 23)".

4.5 Terminals

The device has a 5-pin plug-in terminal block for the power supply. The device variant with DI/DO also has two 2-pin plug-in terminal blocks for the digital input and output.

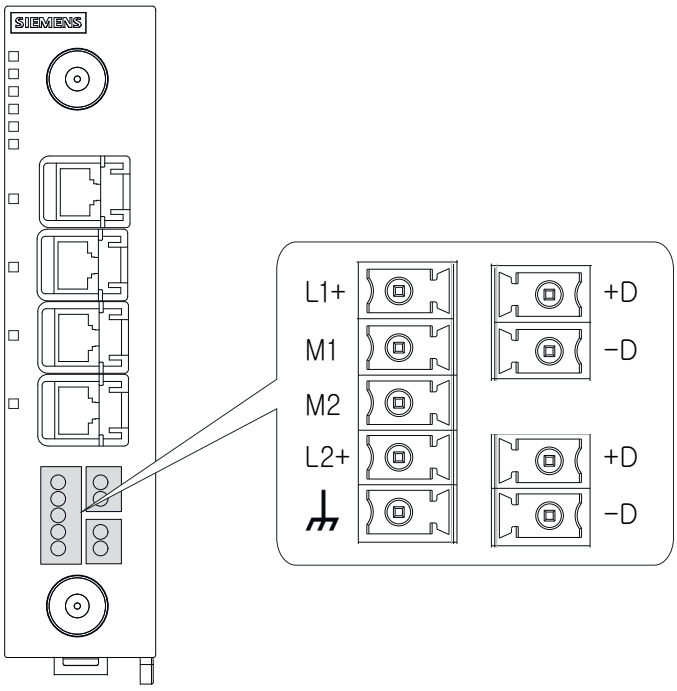


Figure 4-1 SCALANCE WxM763-1 with DI/DO

Connectors and terminal markings

L1, M1, L2, M2	Input for the supply voltage	Terminal block with five terminal connectors
⏚	Functional grounding	
+DI, -DI (only for device variant with DI/DO)	Digital input	Terminal block with two terminal connectors
+DO, -DO (only for device variant with DI/DO)	Digital output	Terminal block with two terminal connectors

Terminals and wiring

Connectors	+DI, -DI /+D0, -DO	L1, M1, L2, M2
AWG	AWG18-16	AWG16
Wire end ferrule without plastic collar according to DIN 46228/1	0.2 mm^2	1.5 mm^2

Wire end ferrule with plastic collar according to DIN 46228/4	0.2 mm^2	1.5 mm^2
Stripped length	7 mm	7 mm

Note

Wire end ferrules

Use crimp shapes with smooth surfaces, such as provided by square and trapeze shaped crimp cross sections.

Crimp shapes with wave-shaped profile are unsuitable.

4.6 Accessories

Technical data subject to change.

You will find further information on the range of accessories in the Industry Mall (https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10021486)

Use the TIA Selection Tool (https://mall.industry.siemens.com/tst/) for configuring the device.

4.6.1 Installation

Component	Description	Article number
DIN rail mounting adapter	Adapter for mounting on a 35 mm DIN rail according to DIN EN 50 022, with fixing screws	6GK5798-8MF00-0AA1

4.6.2 CLP

Component	Description	Article number
CLP Configuration License PLUG	Exchangeable storage medium for saving configuration data	
	SCALANCE CLP 2GB	6GK1900-0UB00-0AA0
	SCALANCE CLP EEC 2GB	6GK1900-0UQ00-0AA0
	SCALANCE CLP 32GB	6GK1900-0UB40-0AA0
CLP iFeatures	Exchangeable storage medium for saving configuration data and enabling iFeatures	
	SCALANCE CLP 2GB W700 AP iFeatures	6GK5907-8UA00-0AA0
	SCALANCE CLP 2GB W700 Client iFeatures	6GK5907-4UA00-0AA0

4.6.3 Industrial Ethernet

You will find information on the cabling for communication networks in the industry on the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/109766358).

Cables Industrial Ethernet (sold by the meter)

Component	Description	Article number
IE FC TP Standard Cable GP 4x2 (AWG 24)	8-wire shielded TP installation cable for universal application Sold by the meter	6XV1878-2A
IE FC TP Flexible Cable GP 4x2 (AWG24)	8-wire shielded TP installation cable for occasional movement Sold by the meter	6XV1878-2B
IE TP Train Cable GP 4x2 (AWG 24)	8-wire shielded TP installation cable for use in rail vehicles and buses, with railway approval Sold by the meter	6XV1878-2T

RJ45 plug-in connector Industrial Ethernet

Component	Description	Article number
IE FC RJ45 Plug 180 4X2 (Gigabit Ethernet)	RJ45 plug-in connector (10/100/1000 Mbps) with rugged metal housing and FC connector technology, for IE FC Cable 4x 2 (24 AWG); 180° cable outlet	
	1 connector per package	6GK1901-1BB11-2AA0
	10 connectors per package	6GK1901-1BB11-2AB0
	50 connectors per package	6GK1901-1BB11-2AE0

Cables Industrial Ethernet (pre-assembled)

Component	Description	Article number
IE Connecting Cable IE FC RJ45 Plug-180/IE FC RJ45 Plug-180	IE FC Flexible GP 4x2 Cable pre-assembled with 2x IE FC RJ45 Plug 180 4 x 2	
	Length 2m	6XV1878-5BH20
	Length 3m	6XV1878-5BH30
	Length 5m	6XV1878-5BH50
	Length 10m	6XV1878-5BN10
	Length 15m	6XV1878-5BN15
	Length 20m	6XV1878-5BN20
	Length 25m	6XV1878-5BN25

4.6.4 Flexible connecting cables, antennas and accessories

You will find an overview of the IWLAN products and their accessories in the Order overview (https://support.industry.siemens.com/cs/ww/en/view/109766333).

4.6.4.1 Flexible connecting cables

Flexible connecting cable N-Connect/R-SMA

Flexible connecting cable for connecting an antenna to a SCALANCE W device with R-SMA connectors, preassembled with a connector N-male and R-SMA male

Length	Article number
0.3 m	6XV1875-5CE30
1 m	6XV1875-5CH10
2 m	6XV1875-5CH20
5 m	6XV1875-5CH50
10 m	6XV1875-5CN10

For railway applications, the following connecting cable are available:

Length	Article number
1 m	6XV1875-5TH10
2 m	6XV1875-5TH20
5 m	6XV1875-5TH50

Flexible connecting cable N-Connect/N-Connect

Flexible connecting cable for connecting an antenna to other connecting elements, such as lightning protection or control cabinet bushings.

Pre-assembled with two N male connectors:

Length	Article number
1 m	6XV1875-5AH10
2 m	6XV1875-5AH20
5 m	6XV1875-5AH50
10 m	6XV1875-5AN10

For railway applications, the following connecting cable are available:

Length	Article number
1 m	6XV1875-5SH10
2 m	6XV1875-5SH20
5 m	6XV1875-5SH50

4.6.4.2 Lightning protection

Component	Description	Article number
LP798-1N	Lighting protector with N/N female/female connector with gas discharge technology	6GK5798-2LP00-2AA6
LP798-2N	Lighting protector with N/N female/female connector with quarter wave technology	6GK5798-2LP10-2AA6

4.6.4.3 Terminating resistor

Component	Description	Article number
TI795-1R	Electrical connection R-SMA male termination impedance 2.4 and 5 GHz, IP65, 0...6 GHz pack of 3	6GK5795-1TR10-0AA6

4.6.4.4 Cabinet feedthrough

Component	Description	Article number
N-Connect/SMA Female/ Female Panel Feedthrough	Cabinet feedthrough, 2.4 GHz and 5 GHz for wall thickness max. 5.5 mm Pack of 1	6GK5798-0PT00-2A

4.6.4.5 Antennas

Note

When you select an antenna, keep in mind:

- The antennas with national approval for your device You will find further information on this on the Internet pages of Siemens Industry Online Support (https://www.siemens.com/wireless-approvals).
- The country-specific and channel-dependent maximum permissible antenna gain You will find further information on this in the reference document "Approvals SCALANCE W700 802.11ax" on the Internet pages of the Siemens Industry Online Support (https://support.industry.siemens.com/cs/de/en/view/109802595).

Antennas

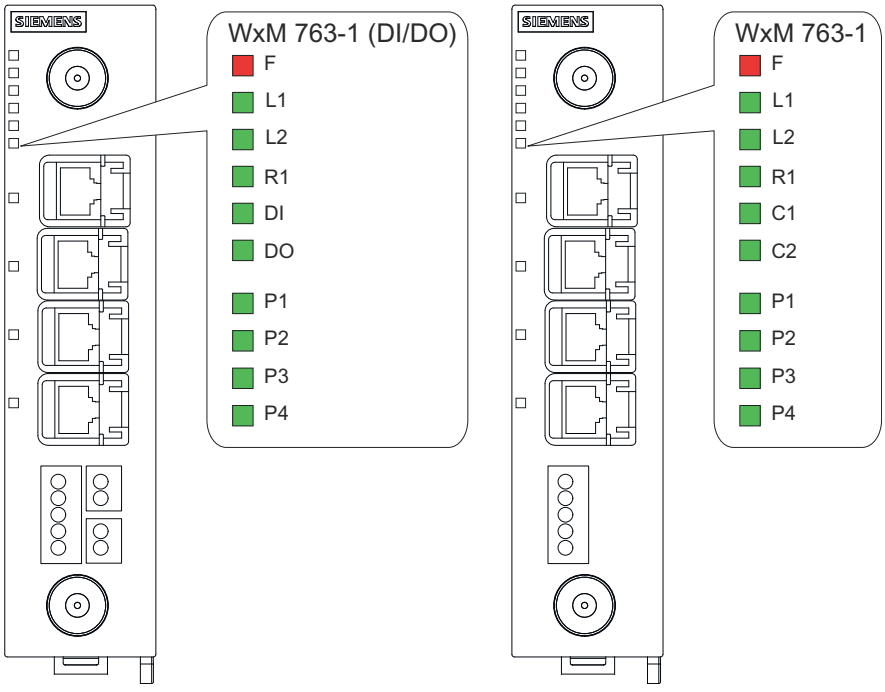
Type	Properties	Article number
ANT792-4DN	RCoax helical antenna, circular polarization, 4 dBi, 2.4 GHz, N-Connector female	6GK5792-4DN00-0AA6
ANT792-6MN	Omni antenna, mast/wall mounting, 6 dBi 2.4 GHz, N-Connector female	6GK5792-6MN00-0AA6

Type	Properties	Article number
ANT792-8DN	Directional antenna, mast/wall mounting, 14 dBi 2.4 GHz, N-Connector female	6GK5792-8DN00-0AA6
ANT793-6DG	Wide angle antenna, mast/wall mounting, 9 dBi 5 GHz, 2 x N-Connector female	6GK5793-6DG00-0AA0
ANT793-8DJ	Directional antenna, mast/wall mounting, 18 dBi 5 GHz, 2 x N-Connector female	6GK5793-8DJ00-0AA0
ANT793-8DK	Directional antenna, mast/wall mounting, 23 dBi 5 GHz, 2 x N-Connector female	6GK5793-8DK00-0AA0
ANT793-8DL	Directional antenna vertical-horizontal polarized, 5 GHz, 14dBi, IP66, 2 x N-Connector female	6GK5793-8DL00-0AA0
ANT793-8DP	Directional antenna, mast/wall mounting, 13 / 13.5 dBi 4.9 GHz and 5 GHz, N-Connector female	6GK5793-8DP00-0AA0
IWLAN RCoax ANT793-4MN	RCoax λ4 antenna with vertical polarization for RCoax systems, 6 dBi, 5 GHz, IP65, N-Connector female	6GK5793-4MN00-0AA6
ANT795-4MA	Omni antenna, 3/5 dBi, 2.4 GHz and 5 GHz, IP30; RSMA connector, radially rotatable, with additional joint; mounting directly to SCALANCE W with RSMA connection technology	6GK5795-4MA00-0AA3
ANT795-4MB	Omni antenna, 2/3 dBi, 2.4 GHz and 5 GHz, IP65; RSMA connector, radially rotatable, with additional joint; mounting directly to SCALANCE W with RSMA connection technology	6GK5795-4MB00-0AA0
ANT795-4MX	Omnidirectional antenna, 2/2.5 dBi, 2.4 GHz and 5 GHz, IP69K, N-Connector male	6GK5795-4MX00-0AA0
ANT795-6DC	Wide angle antenna, mast/wall mounting, 9 dBi 2.4 GHz and 5 GHz, N-Connector female	6GK5795-6DC00-0AA0
ANT795-6MN	Omni antenna, mounted on roof/vehicle, 6/8 dBi 2.4 GHz and 5 GHz, N-Connector female	6GK5795-6MN10-0AA6
ANT795-6MP	Omnidirectional antenna, 5/7 dBi, 2.4 GHz and 5 GHz, IP65/67, N-Connector female	6GK5795-6MP00-0AA0
ANT897-4ME	Omnidirectional antenna for use in public and private mobile wireless networks and IWLAN networks in indoor and outdoor applications worldwide; 2 ... 6 dBi, 0.6 ... 6 GHz, IP65, N-Connector female	6GK5897-4ME00-0AA0
IWLAN RCoax Cable 2,4 GHz PE 1/2"	Omni antenna, 0 dBi 2.400 - 2.485 GHz, N-Connector female	6XV1875-2A
IWLAN RCoax Cable 5 GHz PE 1/2"	Omni antenna, 0 dBi 5.150 – 5.875 GHz, N-Connector female	6XV1875-2D

4.7 LED display

The figure shows the arrangement of the LEDs:

- Left: for device version with DI/DO (6GK5763-1AL00-xDA0)
- Right: for device version without DI/DO (6GK5763-1AL00-3AA0)



LED	Color	Meaning
F	Off □	No fault/error.
	Yellow ■	Sleep mode is active.
	Red ■	The device is booting, an error has occurred or the bootloader is waiting for a new firmware file, which you can load via TFTP, see "Loading new firmware via TFTP without WBM and CLI".
	Flashing red  Interval: 2000 ms on / 200 ms off	Firmware on PLUG: The device is performing a firmware update or downgrade.
	Red ■ Simultaneous R1 flashing yellow 	A competing radar signal was found on all enabled channels.
L1	Off □	Power supply L1 too low.
	Green ■	Power supply L1 is applied.
L2	Off □	Power supply L2 too low.
	Green ■	Power supply L2 is applied.

LED	Color	Meaning
R1	Off	The WLAN interface 1 is deactivated.
	Green 	*Access Point mode:* The WLAN interface 1 is initialized and ready for operation.
		Client mode: There is a connection over the WLAN interface 1.
	Flashing green and yellow 	Data transfer over the WLAN interface 1.
	Flashing yellow 	*Client mode:* The client is searching for a connection to an access point.
	Flashing yellow  Interval: 100 ms on / 100 ms off	*Access Point mode:* With DFS (802.11h), the channel is scanned for one minute for competing radar signals before the channel can be used for data traffic.
DI	Off 	Digital input inactive.
	Green 	Digital input active.
DO	Off 	Digital output inactive.
	Green 	Digital output active.
C1 C2	Off 	The functionality of these LEDs is configurable for different applications. It is disabled by default.
P1 P2 P3 P4	Off 	There is no connection over the Ethernet interface.
	Green 	There is a connection via the Ethernet interface (Link).
	Flashing green and yellow 	Data transfer via the Ethernet interface

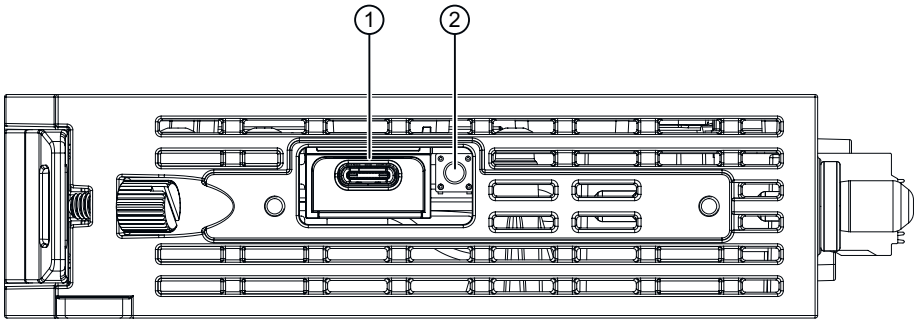
LED	Color	Meaning
R1 DI DO	Flashing green 	Depending on the device version, the following LEDs are flashing to determine the location of the device: • R1, DI and DO (device version with DI/DO) • R1, C1 and C2 (device version without DI/DO) The "Flash LED" function is activated: • Either with SINEC PNI • Or via the WBM page "Discovery and Set via DCP"
R1 C1 C2		

4.8 Reset button

Position

NOTICE
Loss of the degree of protection
When the cover is not mounted correctly, the device loses its degree of protection IP30.

The Reset button is located behind the screw-on cover on the underside of the housing.



① PLUG slot (CLP)
② Reset button

Function

The reset button has the following functions:

- **Restarting the device**
  To restart the device, press the reset button briefly.

  Note

  If you make changes to the configuration and restart immediately afterwards with the reset button, the changes may be lost. If you restart the device using the WBM (menu command "System > Restart") or using the CLI (command "restart" in the Privileged EXEC Modus), the configuration changes are always retained.

- **Loading a firmware file via TFTP**
  If the normal procedure with the "Load & Save" menu of Web Based Management is unsuccessful, the reset button can be used to load new firmware. This situation can occur if there is a power outage during the normal firmware update. You can find more detailed information in the section "Downloading new firmware using TFTP without WBM and CLI (Page 65)".
- **Resetting the device to factory settings**
  If you reset, all the settings you have made will be overwritten by factory defaults. If a PLUG has been inserted in the device, the PLUG is also reset to default settings. You can find more detailed information in the section "Restoring the factory settings (Page 66)".

NOTICE
Inadvertent reset An inadvertent reset can cause disturbances and failures in a configured network with further consequences.

4.9 Configuration License PLUG

The CLP (Configuration License PLUG) is used to transfer the configuration of the old device to the new device when a device is replaced. The CLP is also referred to as PLUG in the description.

The PLUG is available in the following variants:

- PLUG Configuration: The exchangeable storage medium only saves the configuration data of the device.
- PLUG License: In addition to the configuration data, the exchangeable storage medium contains a license with which special functions are enabled, e.g. iFeatures.

NOTICE
Loss of the degree of protection When the cover is not mounted correctly, the device loses its degree of protection IP30.

Position

The CLP slot is at the bottom of the device enclosure under a cover, see Reset button (Page 31).

Function

Devices with a CLP slot support the following operating modes:

- **Without CLP**
  The device saves the configuration data in the internal memory. This mode is active when no CLP is inserted.
- **With CLP**
  In the startup phase:
  - When an **empty** CLP (delivery state) is inserted into the device, the device automatically backs up the configuration data on the CLP during startup. After that, it behaves like a CLP with data.
  - When a CLP **with data** is plugged into a device, the device automatically adopts the configuration of the CLP during the startup phase. The prerequisite for this is that the configuration data was written by a compatible device type.
    One exception to this can be the IP configuration if it is set using DHCP and the DHCP server has not been reconfigured accordingly. Reconfiguration is necessary if you use functions based on MAC addresses.
  - If the CLP contains a license, additional functions are also enabled.

    Note

    If the device was configured at some time with a CLP license, the device can no longer be used without this CLP. To be able to use the device again, reset the device to the factory settings.

  During operation:
  - During operation, changes to the configuration are saved on the CLP and in the internal memory.
  - The configuration data of the device is stored in a secured memory area of the CLP. This secured memory area can only be accessed via the authentication of the Siemens device.
  - The device checks whether a CLP is inserted at one second intervals. If the device detects that the CLP has been removed, it restarts automatically.

NOTICE
Operating risk - Danger of data loss Only pull and plug the CLP when the device is de-energized.

  - The device signals deviations from normal operation of the CLP (e.g., incompatible data, incorrect operation or malfunctions) via the existing diagnostics mechanisms (e.g., LEDs or user interfaces).

The procedure for inserting and removing the CLP can be found in the section "Replacing a CLP (Page 61)".

Installation and removal

5

5.1 Safety during mounting

Safety notices

When installing the device, keep to the safety notices listed below.

NOTICE
Improper mounting Improper mounting may damage the device or impair its operation. • Before mounting the device, always ensure that there is no visible damage to the device. • Mount the device using suitable tools. Observe the information in the respective section about mounting.

⚠ CAUTION
Minimum distance to antennas Fit the device so that there is a minimum clearance of 20 cm between antennas and persons.

⚠ WARNING
If a device is operated in an ambient temperature of more than 50 °C, the temperature of the device housing may be higher than 70 °C. The device must therefore be installed so that it is only accessible to service personnel or users that are aware of the reason for restricted access and the required safety measures at an ambient temperature higher than 50 °C.

⚠ WARNING
If the device is installed in a cabinet, the inner temperature of the cabinet corresponds to the ambient temperature of the device.

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

⚠ WARNING
The device is intended for indoor use only.

WARNING

When used in hazardous environments corresponding to Class I, Division 2 or Class I, Zone 2, the device must be installed in a cabinet or a suitable enclosure.

WARNING

EXPLOSION HAZARD

Replacing components may impair suitability for Class 1, Division 2 or Zone 2.

WARNING

The device may only be operated in an environment of contamination class 1 or 2 (see EN/IEC 60664-1, GB/T 16935.1).

Notes for use in hazardous locations according to ATEX, IECEx, UKEX and CCC Ex

If you use the device under ATEX, IECEx, UKEX or CCC Ex conditions you must also keep to the following safety instructions in addition to the general safety instructions for protection against explosion:

WARNING

To comply with EU Directive 2014/34 EU (ATEX 114), UK-Regulation SI 2016/1107 or the conditions of IECEx or CCC-Ex, the housing or cabinet must meet the requirements of at least IP54 (according to EN/IEC 60529, GB/T 4208) in compliance with EN IEC/IEC 60079-7, GB 3836.3.

Safety notices when using according to FM

If you use the device under FM conditions you must also keep to the following safety notices in addition to the general safety notices for protection against explosion:

WARNING

EXPLOSION HAZARD

The equipment is intended to be installed within an enclosure/control cabinet. The inner service temperature of the enclosure/control cabinet corresponds to the ambient temperature of the module. Use cables with a maximum permitted operating temperature of at least 20 °C higher than the maximum ambient temperature.

WARNING

Wall mounting is only permitted if the requirements for the housing, the installation regulations, the clearance and separating regulations for the control cabinets or housings are adhered to. The control cabinet cover or housing must be secured so that it can only be opened with a tool. An appropriate strain-relief assembly for the cable must be used.

WARNING

Wall mounting outside of the control cabinet or housing does not fulfill the requirements of the FM approval.

Note

You must not install the device on a wall in hazardous areas.

Safety notices when using the device as industrial control equipment according to UL 61010-2-201

If you use the device under UL 61010-2-201 conditions you must also keep to the following safety notices in addition to the general safety notices for protection against explosion:

WARNING

Open equipment

The devices are "open equipment" according to the standard IEC 61010-2-201 or UL 61010-2-201 / CSA C22.2 No. 61010-2-201. To fulfill requirements for safe operation with regard to mechanical stability, flame retardation, stability, and protection against contact, the following alternative types of installation are specified:

- Installation in a suitable cabinet.
- Installation in a suitable enclosure.
- Installation in a suitably equipped, enclosed control room.

WARNING

If the temperature at the cable or housing socket or at the branching points of the cables exceeds 60 °C, special precautions must be taken. If the equipment is operated at ambient temperatures in excess of 40 °C, only use cables with permitted operating temperature of at least 80 °C.

⚠ WARNING

Improper disassembly

Improper disassembly may result in a risk of explosion in hazardous areas.

For proper disassembly, observe the following:

- Before starting work, ensure that the electricity is switched off.
- Secure remaining connections so that no damage can occur as a result of disassembly if the system is accidentally started up.

5.2 Types of installation

For the device, you have the following options:

- Wall mounting
- Installation on a 35 mm DIN rail
  - direct
  - rotated by 90^0 with a DIN rail mounting adapter (see Accessories (Page 23))
- Installation on the S7-300 mounting rail
- Installation on the S7-1500 mounting rail

Note

Observe country-specific regulations when selecting the type of installation. You will find additional information on this in the reference document "Approvals SCALANCE W700 802.11ax" on the Internet pages of the Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/109802595).

⚠ CAUTION

Danger of injury by falling objects

If the SCALANCE W is subjected to very strong vibration (> 10 m/s^2), mounting on a DIN rail or S7-300 / S7-1500 mounting rail does not provide adequate support. Under such conditions, the device can come out of the mounting and may cause injury.

In this case, install the device on a wall.

Permitted mounting position

- Vertical mounting position (ventilation openings at the top and bottom)
- Horizontal mounting position (ventilation openings to the right and left)

Strain relief for the cables

Regardless of the type of installation, make sure that there is suitable strain relief for the connecting cable.

Shielding of cables

If cables are installed permanently, it is advisable to remove the insulation of the shielded cable and to establish contact on the shield/PE conductor bar.

Permitted mounting position

You can find information about the ambient temperature under Permitted ambient conditions. (Page 69)

Keep to the minimum clearances to other components or to walls of a housing so that the convection ventilation of the device is not blocked.

- Above at least 10 cm
- Below at least 10 cm

Note

Antennas, in particular directional antennas, must be mounted in keeping with their characteristics (refer to the technical specifications of the antenna --> Radiation pattern diagrams).

5.3 Wall mounting

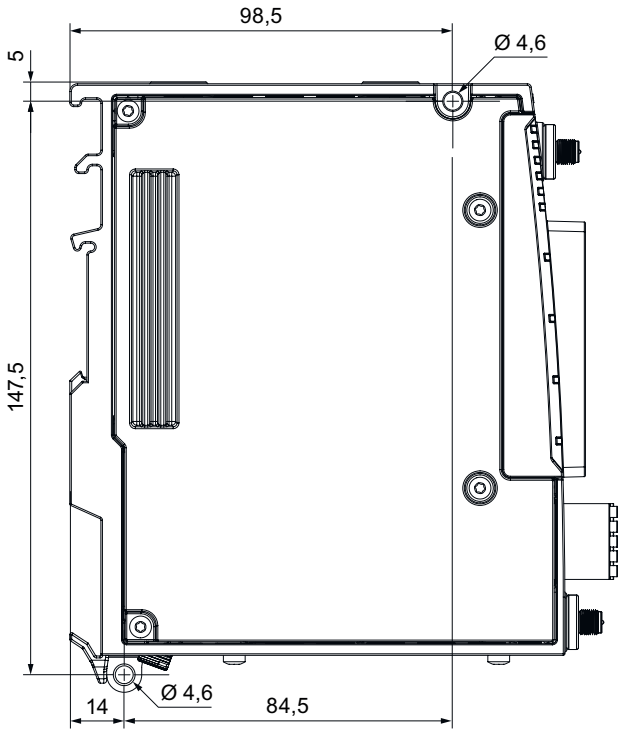
Note

The wall mounting must be capable of supporting at least four times the weight of the device.

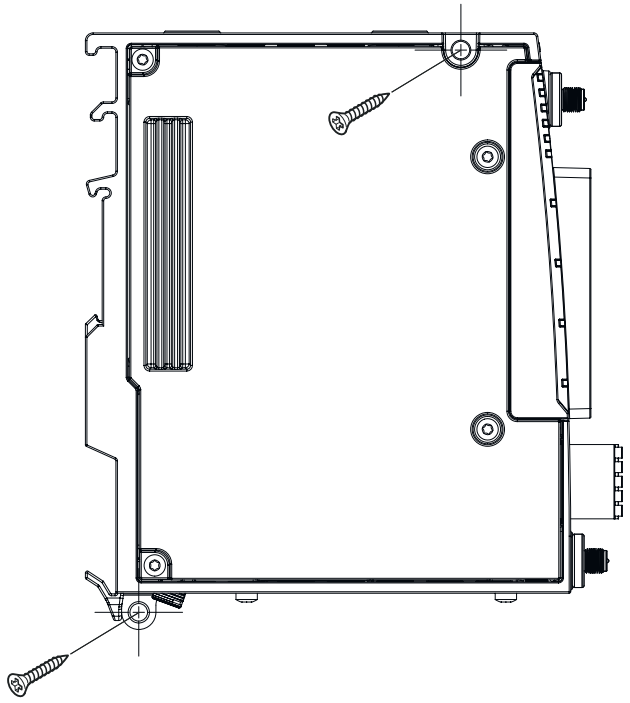
Use suitable fittings depending on the mounting surface.

Drilling template

The figure shows the location of the holes for wall mounting of the device:



Procedure



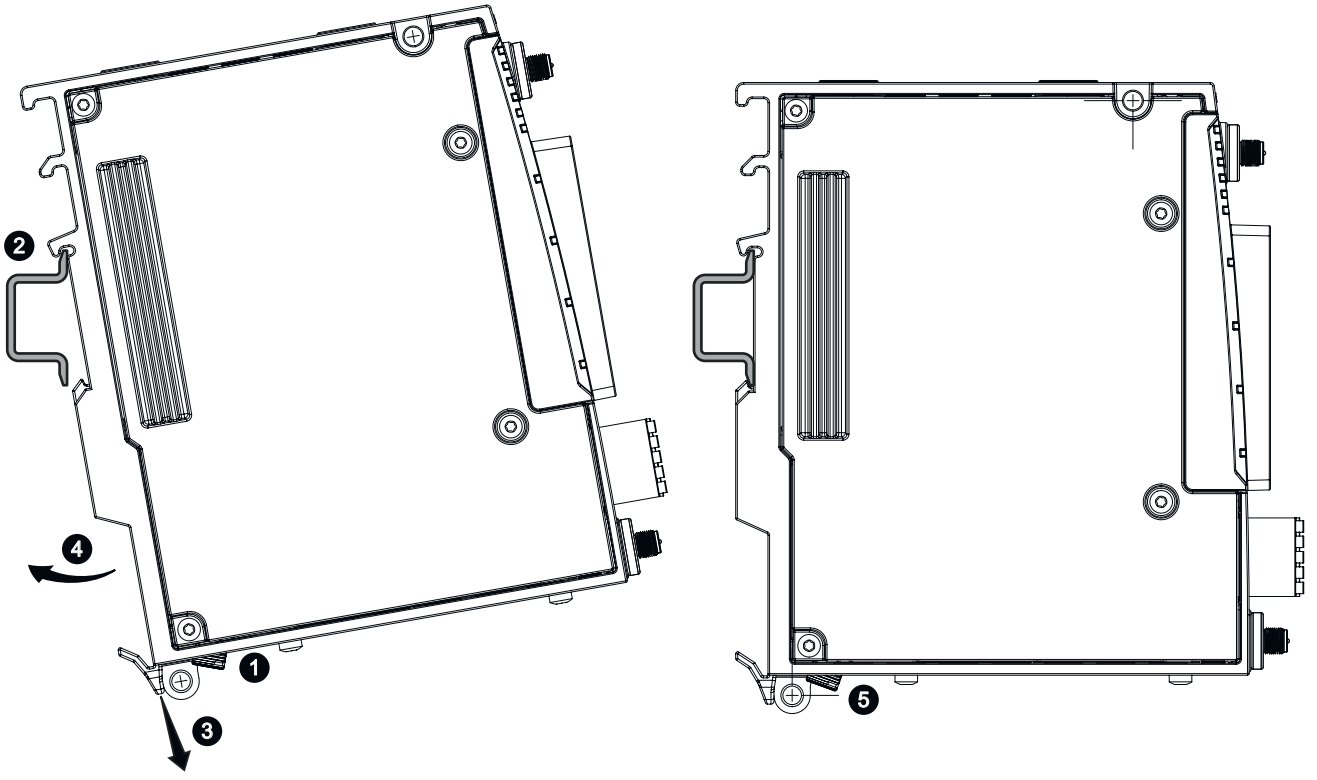
Follow the steps below to mount the device to the wall:

1. Prepare the drill holes for wall mounting. The precise dimensions are listed in the drilling template, refer to section "Drilling template".
2. Secure the device to the wall with two screws. The screws are not supplied with the device. The type and length of the screws depend on the type of wall.
3. Connect the device; see section "Connecting (Page 49)".

5.4 Installing on the DIN rail

5.4.1 Mounting directly on the DIN rail

Installation



Follow the steps below to mount the device on a DIN rail:

1. Loosen the knurled screw with your hand or a screwdriver.
2. Place the third housing guide of the device on the top edge of the DIN rail.
3. Using a screwdriver, pull the securing bar down as far as it will go.
4. With the securing bar pulled, swivel the device to the DIN rail and press it against the DIN rail until the spring-mounted securing bar locks into place.

5. Tighten the knurled screw to secure the device additionally (torque 0.5 Nm).
6. Connect the device; see section "Connecting (Page 49)".

Uninstalling

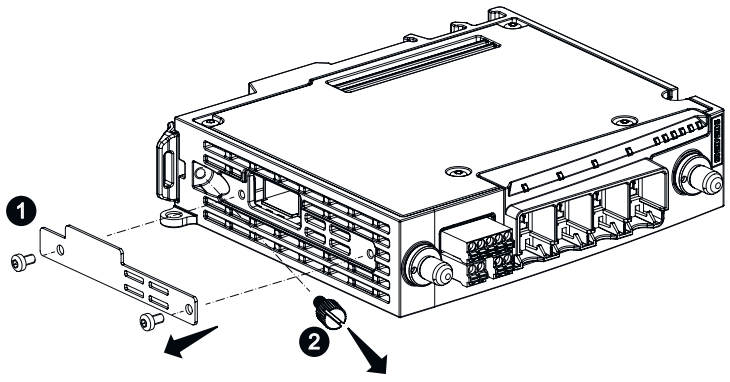
1. Turn off the power to the device.
2. Disconnect all connected cables.
3. If necessary, loosen the knurled screw with your hand or a screwdriver.
4. Using a screwdriver, pull down the catch on the rear of the device.
5. Pull lower part of the device away from the DIN rail.

5.4.2 Mounting rotated by 90° with DIN rail mounting adapter

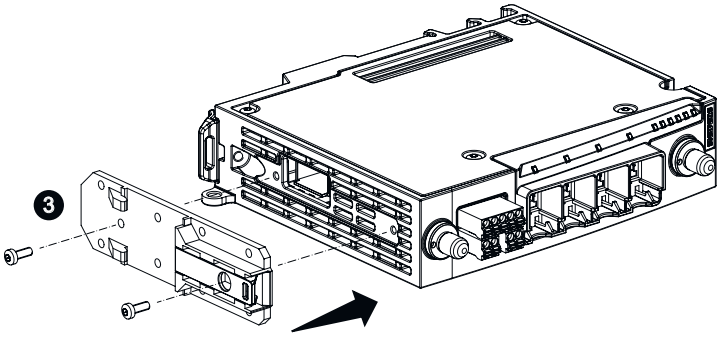
The DIN rail mounting adapter is not included with the product, see Accessories (Page 23).

Installation

1. Loosen the two M3 screws and remove the cover of the CLP slot ❶.
2. Remove the knurled screw ❷.

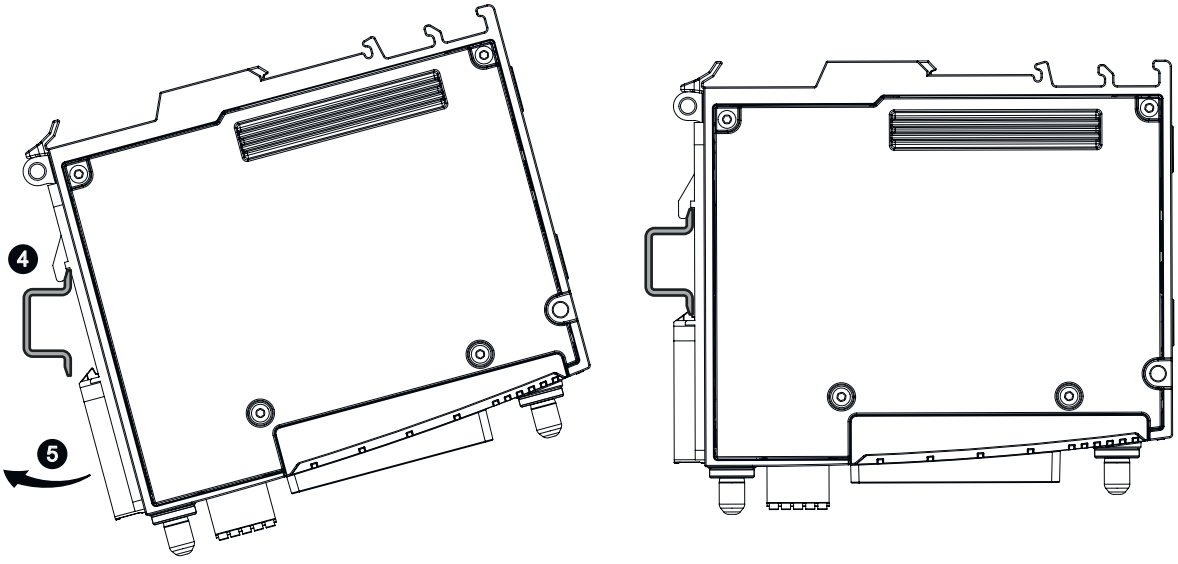


3. Screw the DIN rail mounting adapter ❸ to the bottom of the device (M3 x 8, tightening torque 0.8 Nm). The mounting material is supplied with the DIN rail mounting adapter.



4. Place the device on the upper edge of the DIN rail ❹.

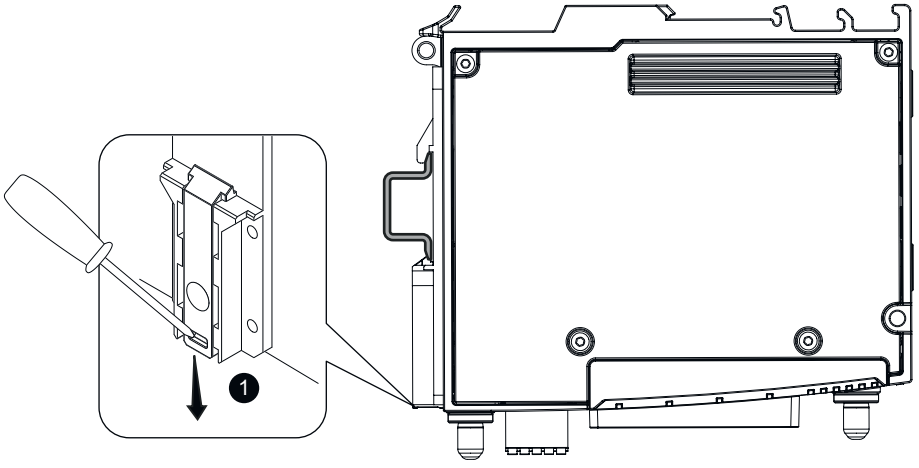
5. Press the device against the DIN rail ❺ until the DIN rail slider catch locks in place.



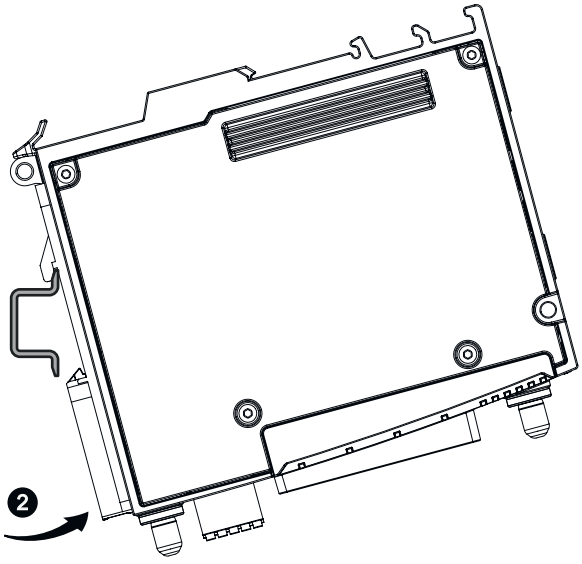
6. Connect the power supply, refer to the section "Power supply (Page 55)".
7. Fit the antennas, refer to the section "Antennas (Page 57)".

Uninstalling

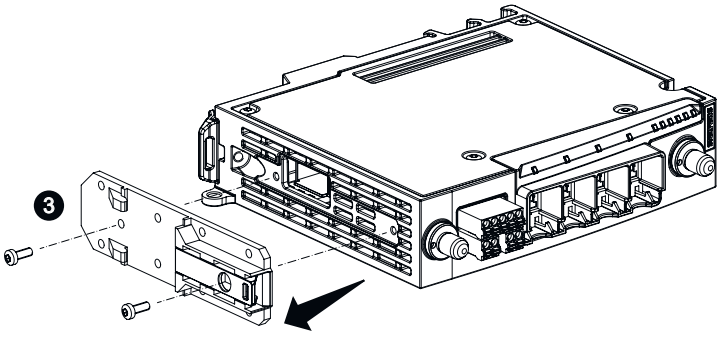
1. Turn off the power to the device.
2. Disconnect all connected cables.
3. Pull the DIN rail slider down with a screwdriver ❶.



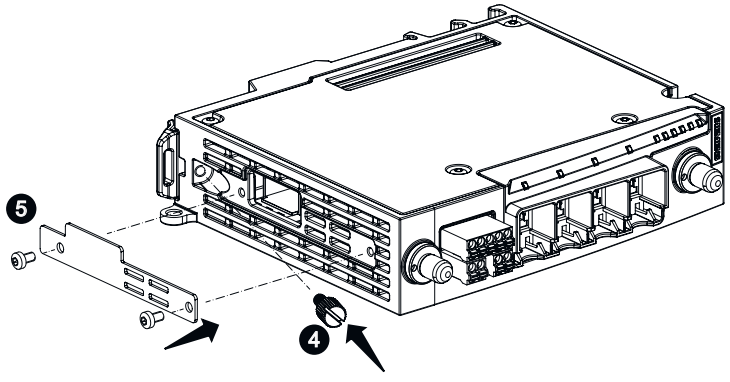
4. Tilt the device forward ❷ and remove the device from the DIN rail.



5. Loosen the screws of the DIN rail mounting adapter ❸ completely and remove it.

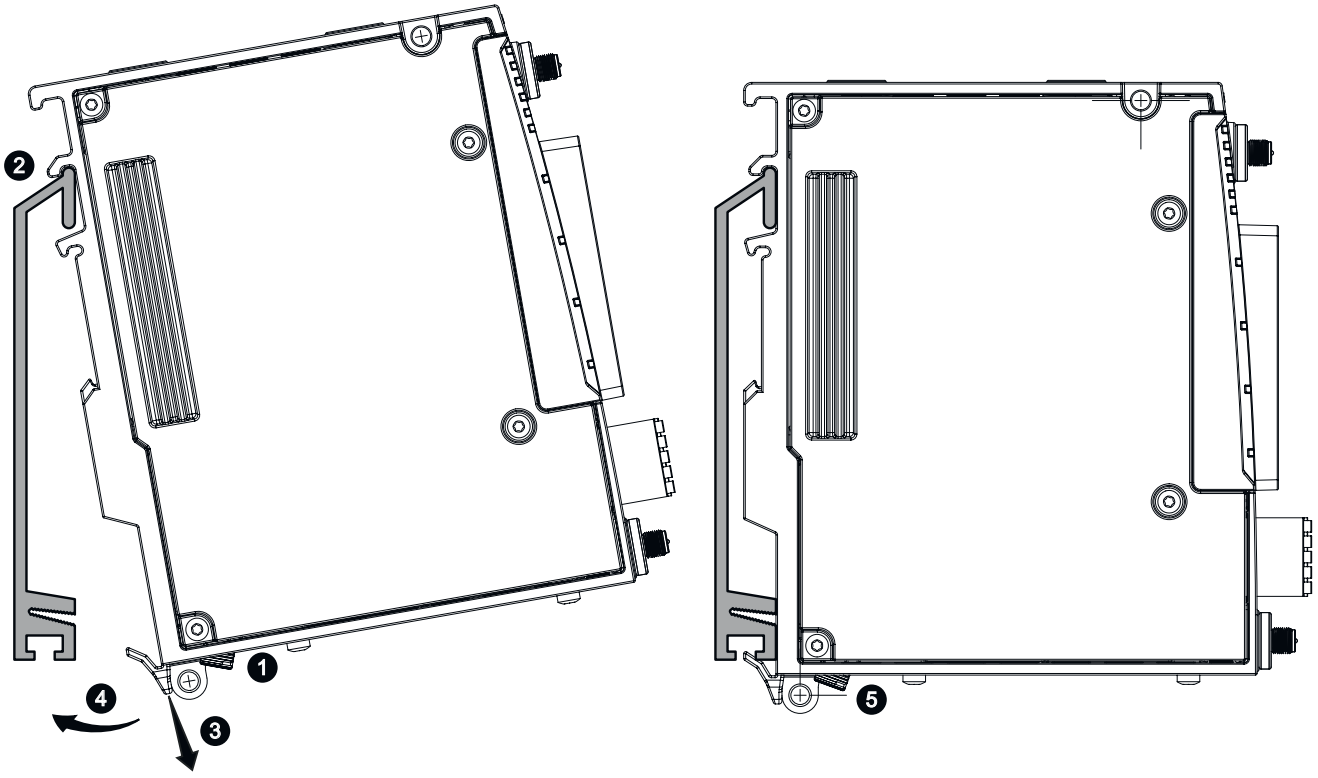


6. Install the knurled screw ❹.
7. Attach the cover of the CLP slot ❺ again.



5.5 Installing on an S7-300 mounting rail

Installation



Follow the steps below to mount the device on an S7-300 mounting rail:

1. Loosen the knurled screw with your hand or a screwdriver.
2. Place the first housing guide of the device on the top edge of the mounting rail.
3. Using a screwdriver, pull the securing bar down as far as it will go.
4. With the securing bar pulled, swivel the device to the mounting rail and press it against the mounting rail until the spring-mounted securing bar locks into place.
5. Tighten the knurled screw to secure the device additionally (torque 0.5 Nm).
6. Connect the device; see section "Connecting (Page 49)".

Uninstalling

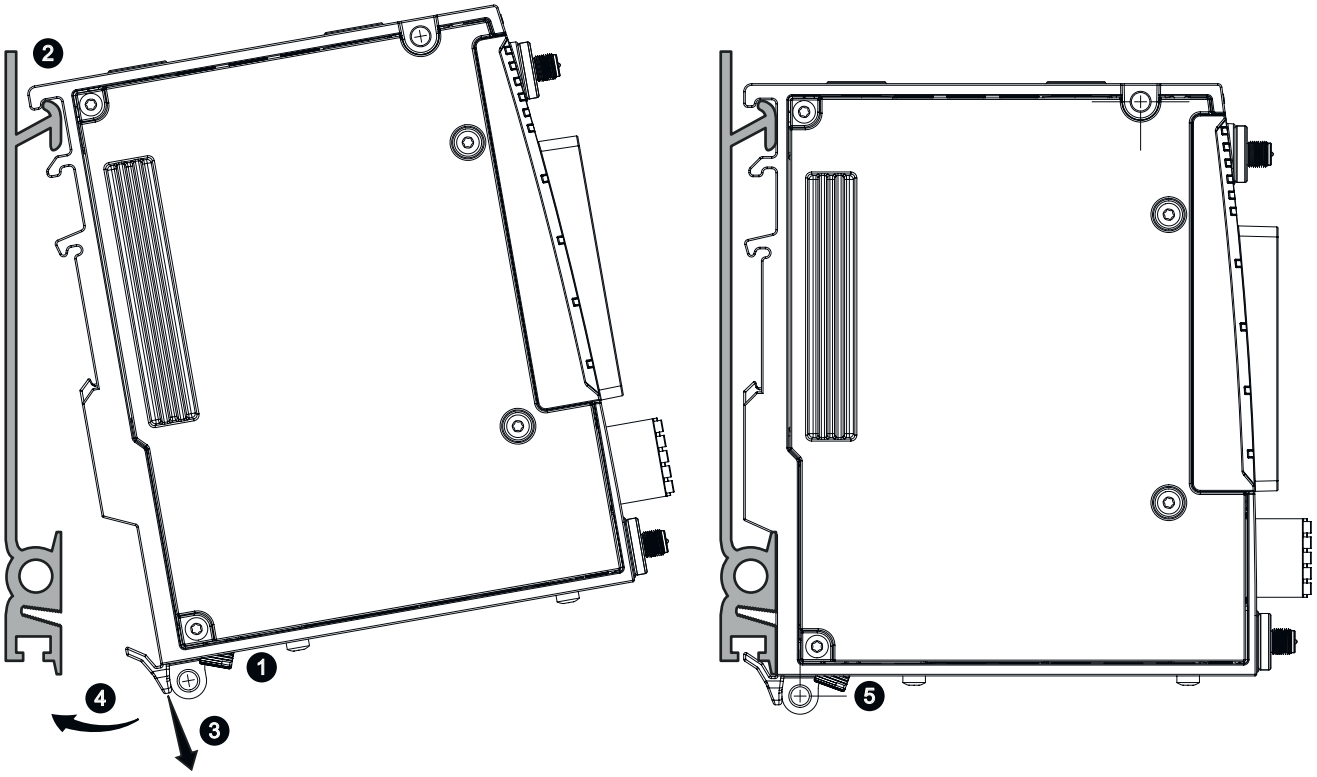
To remove the device from the mounting rail, follow these steps:

1. Turn off the power to the device.
2. Disconnect all connected cables.
3. If necessary, loosen the knurled screw with your hand or a screwdriver.

4. Using a screwdriver, pull the securing bar down as far as it will go.
5. Remove the device from the mounting rail with the bar pulled.

5.6 Installing on an S7-1500 mounting rail

Installation



Follow the steps below to mount the device on an S7-1500 mounting rail:

1. Loosen the knurled screw with your hand or a screwdriver.
2. Place the first housing guide of the device on the top edge of the mounting rail.
3. Using a screwdriver, pull the securing bar down as far as it will go.
4. With the securing bar pulled, swivel the device to the mounting rail and press it against the mounting rail until the spring-mounted securing bar locks into place.
5. Tighten the knurled screw to secure the device additionally (torque 0.5 Nm).
6. Connect the device; see section "Connecting (Page 49)".

Uninstalling

To remove the device from the mounting rail, follow these steps:

1. Turn off the power to the device.
2. Disconnect all connected cables.
3. If necessary, loosen the knurled screw with your hand or a screwdriver.
4. Using a screwdriver, pull the securing bar down as far as it will go.
5. Remove the device from the mounting rail with the bar pulled.

Connection

6

6.1 Safety when connecting up

Safety notices

When connecting up the device, keep to the safety notices listed below.

Note

Use of outdoor antennas

Observe country-specific regulations on using antennas outdoors. You will find additional information on this in the reference document "Industrial Wireless LAN Approvals SCALANCE W700 802.11ax" on the Internet pages of the Siemens Industry Online Support: (https://support.industry.siemens.com/cs/de/de/view/109802595/en)

Note

Strain relief for the Ethernet cables

In order to avoid mechanical stress on the Ethernet cables and resulting interruption of the contact, fasten the cables at a short distance from the connector using a cable guide or busbar.

Lightning protection



⚠ WARNING

Danger due to lightning strikes

Antennas installed outdoors must be within the area covered by a lightning protection system. Make sure that all conducting systems entering from outdoors can be protected by a lightning protection potential equalization system.

When implementing your lightning protection concept, make sure you adhere to the VDE 0182 or IEC 62305 standard.

Suitable lightning protectors are available in the accessories (Page 26) of SIMATIC NET Industrial WLAN.

Note

We recommend that you use the maintenance-free lightning protector LP798-2N.

Exception: When there is also DC power supplied via the antenna cable. In this case, only the lightning protector LP798-1N can be used.



⚠ WARNING

Danger due to lightning strikes

Installing this lightning protector between an antenna and a SCALANCE W device is not adequate protection against a lightning strike. The LP798-1N lightening protector only works within the framework of a comprehensive lightning protection concept. If you have questions, ask a qualified specialist company.

Note

The requirements of EN61000-4-5, surge immunity tests on power supply lines, are met only when a Blitzductor is used with 24 VDC:

BVT AVD 24
article number: 918 422
Manufacturer: DEHN+SÖHNE GmbH+Co.KG, Hans Dehn Str. 1, Postfach 1640, D - 92306 Neumarkt, Germany

Supply voltage

⚠ WARNING

Power supply

The device is designed for operation with a directly connectable safety extra-low voltage (SELV) or protective extra low voltage (PELV) from a limited power source (LPS).

The power supply therefore needs to meet at least one of the following conditions:

- Only safety extra low voltages SELV/PELV with limited power source LPS complying with IEC 62368-1 / EN 62368-1 / VDE 62368-1 may be connected to the power supply terminals.
- The power supply unit for the device must meet NEC Class 2 according to the National Electrical Code (r) (ANSI / NFPA 70).

If the equipment is connected to a redundant power supply (two separate power supplies), both must meet these requirements.

Grounding



⚠ WARNING

Danger to life from overvoltage, fire hazard

When using outdoor antennas, the shared or grounded pin of the circuit must be connected to the shield of the coaxial cable and to all touchable conductive parts and circuits. Otherwise, there may be impermissibly high voltages on touchable parts in the event of a fault.

NOTICE

Damage to the device due to potential differences

To fully eliminate the influence of electromagnetic interference, the device must be grounded. There must be no potential difference between the following parts, otherwise the device or other connected device could be severely damaged:

- Housing of the SCALANCE W device and the ground potential of the antenna.
- Housing of the SCALANCE W device and the ground potential of a device connected over Ethernet.
- Housing of the SCALANCE W device and the shield contact of the connected Ethernet cable.

Connect both grounds to the same foundation earth or use an equipotential bonding cable.

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

⚠ WARNING

EXPLOSION HAZARD

Do not connect or disconnect cables to or from the device when a flammable or combustible atmosphere is present.

⚠ WARNING

EXPLOSION HAZARD

Do not press the reset button if there is a potentially explosive atmosphere.

WARNING

Unsuitable cables or connectors

Risk of explosion in hazardous areas

- Only use connectors that meet the requirements of the relevant type of protection.
- If necessary, tighten the connector screw connections, device fastening screws, grounding screws, etc. according to the specified torques.
- Close unused cable openings for electrical connections.
- Check the cables for a tight fit after installation.

WARNING

Lack of equipotential bonding

If there is no equipotential bonding in hazardous areas, there is a risk of explosion due to equalizing current or ignition sparks.

- Ensure that equipotential bonding is available for the device.

WARNING

Unprotected cable ends

There is a risk of explosion due to unprotected cable ends in hazardous areas.

- Protect unused cable ends according to IEC/EN 60079-14.

WARNING

Improper installation of shielded cables

There is a risk of explosion due to equalizing currents between the hazardous area and the non-hazardous area.

- Ground shielded cables that cross hazardous areas at one end only.
- Lay a potential equalization conductor when grounding at both ends.

WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

- When connecting intrinsically safe and non-intrinsically safe circuits, ensure that the galvanic isolation is performed properly in compliance with local regulations (e.g. IEC 60079-14).
- Observe the device approvals applicable for your country.

Notes for use in hazardous locations according to ATEX, IECEx, UKEX and CCC Ex

If you use the device under ATEX, IECEx, UKEX or CCC Ex conditions you must also keep to the following safety instructions in addition to the general safety instructions for protection against explosion:

WARNING

Transient overvoltages

Take measures to prevent transient overvoltages of more than 40% of the rated voltage (or more than 119 V). This is guaranteed if you only operate the devices with SELV (safety extra-low voltage) or PELV (protective extra low voltage).

WARNING

Suitable cables at high ambient temperatures in hazardous area

At an ambient temperature of ≥ 60 °C, use heat-resistant cables designed for an ambient temperature at least 20 °C higher. The cable entries used on the enclosure must comply with the IP degree of protection required by EN IEC / IEC 60079-0, GB 3836.1.

General notes on use in hazardous areas according to UL-HazLoc

If you use the device under UL-HazLoc conditions, you must also adhere to the following safety notices in addition to the general safety notices for protection against explosion:

WARNING

WARNING - EXPLOSION HAZARD -

DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS AREA IS KNOWN TO BE NON-HAZARDOUS.

WARNING

Restricted area of application

This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D or non-hazardous locations only.

WARNING

Restricted area of application

This equipment is suitable for use in Class I, Zone 2, Group IIC or non-hazardous locations only.

Safety information when using in accordance with UL 61010-2-201

If you use the device under UL 61010-2-201 conditions you must also keep to the following safety notices in addition to the general safety notices for protection against explosion:

NOTICE

Suitable fusing for the power supply cable

The current at the connecting terminals must not exceed 3 A. Use a fuse for the power supply that protects against currents > 3 A.

- In areas where NEC or CEC are used, the following requirements must be met:
  - Suitable for DC (min. 60 V / max. 3 A)
  - Breaking current min. 10 kA
  - UL/CSA listet (UL 248-14 / CSA 22.2 No. 248.14)
  - Classes R, J, L, T or CC
- In other areas, the following requirements must be met:
  - Suitable for DC (min. 60 V / max. 3 A)
  - Breaking current min. 10 kA
  - Permitted for electric circuits according to IEC / EN 60947-1/2/3
  - Breaking characteristics: B or C for circuit-breakers or fuses

You do not need a fuse for the power supply cable if you use a voltage source according LPS or NEC Class 2.

NOTICE

Grounding

A PELV circuit contains a connection to ground. Without a connection to ground, or in case there is a fault in the connection to the ground, the voltage for the circuit is not stabilized (limited).

NOTICE

The "Limited Energy" circuit and other circuits must be separated by at least basic insulation.

NOTICE

The digital outputs are not permitted to come into contact with hazardous voltages and non-energy limited circuits. The permissible nonhazardous voltages are SELV/PELV as per UL 61010-2-201. The energy limited circuit as per clause 9.4 of UL 61010-1 or LPS of UL 60950 or Class 2 of UL 1310 or UL 5085-1 & UL 5085-3 are considered as equivalent.

6.2 Power supply

⚠ WARNING

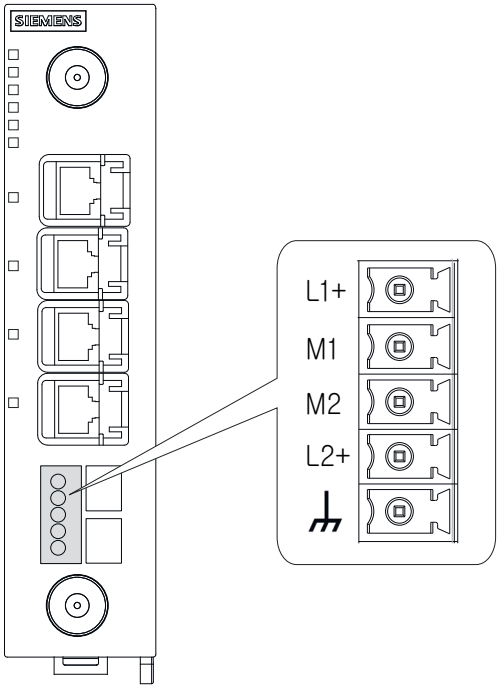
Impermissible power supply

Never operate the device with AC voltage or DC voltage higher than 32 V DC.

Note

The device can be disconnected from the power supply by removing the terminal block.

The power supply is connected using a 5-pin plug-in terminal block. The power supply is non-floating.



Contact	Assignment
L1+	24 VDC
M1	Ground
M2	Ground
L2+	24 VDC
⏚	Functional grounding, refer to the section "Grounding (Page 60)"

Use copper cables with the following properties to wire the power connector:

- Two-wire cable with 0.5 to 1.5 mm^2 Cross-section per wire
- Permitted tensile load at least 10 N. - UL
- List of cables according to the national installation regulations. In areas where NEC or CEC applies: Type PTLC or ITC

You can find more information in the section "Terminals (Page 22)".

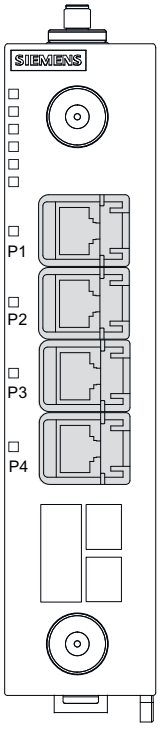
The "L1" and "L2" LEDs indicate whether a power supply is connected; see section "LEDs (Page 28)".

6.3 Ethernet

The device has four Ethernet interfaces located on the front of the device. Connection to Industrial Ethernet uses RJ45 connection technology with MDI-X assignment.

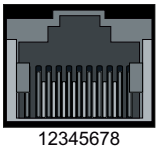
Position

The figure shows the position of the connectors to Industrial Ethernet with 10/100/1000 Mbps.



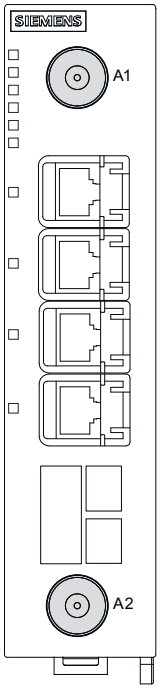
Pin assignment

The following table shows the pin assignment of the RJ45 connectors.

Pin number	Pin assignment	RJ45 connector
	10/100/1000 Mbps	
Pin 1	D1+	
Pin 2	D1-	
Pin 3	D2+	
Pin 4	D3+	
Pin 5	D3-	
Pin 6	D2-	
Pin 7	D4+	
Pin 8	D4-	

6.4 Antennas

The device has two antenna connectors of the type R-SMA, which are located on the front of the device.



A1 Antenna connector R1 A1

A2 Antenna connector R1 A2

Procedure

Follow the steps below to connect a cable for an external antenna to the device:

1. Insert the connector on the antenna cable into the R-SMA socket and tighten the sleeve nut of the plug on the socket (key size SW8, tightening torque 1 Nm).
   If you only use one antenna, you need to connect this to the device via antenna connector R1 A1 (position A1).

NOTICE
The R-SMA socket may be damaged When securing an antenna to the device, only the screw cap of the antenna can be rotated. Rotating the entire antenna could damage the R-SMA connector on the device.

2. Screw a terminating resistor to the unused antenna connector R1 A2 (position A2) if you are only using one antenna.

NOTICE
UL approval only for use in buildings Where NEC and CEC apply, the device and the antennas connected to it may only be used in a closed building. For this reason, do not lead antennas into the outdoor area if you need to meet UL requirements.

Note

Cabinet installation

When installing the device in a cabinet, you need to use detached antennas. A suitable flexible connecting cable for the connection between the device and a detached antenna are available from SIMATIC NET. You can find detailed information in section "Flexible connecting cables, antennas and accessories (Page 25)".

6.5 Digital input/output

You can find article numbers for the device variants that have a digital input and output in the Scope of validity (Page 5). The device version is marked with "DI/DO".

The digital input and output are connected using a 2-pin plug-in terminal block in each case. Two terminal blocks ship with the device.

NOTICE
Damage due to voltage being too high or too low The voltage at the digital input/output must not exceed 30 VDC and not fall below -30 VDC, otherwise the digital input/output will be destroyed.

Note

Interference pulse

To avoid evaluating an interference pulse, the pulse for the signal 1 (TRUE / HIGH) must be at least 200 ms.

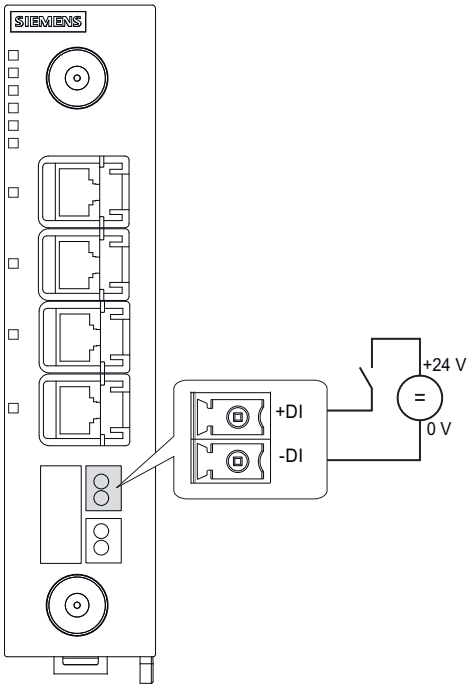
Wiring rules

- To wire the digital input/output, use a copper cable of category AWG18-16 or a cable with a cross-section of 0.75 to 1.5 mm^2.
- Always wire the digital input/output in pairs.
- The maximum permissible cable length is 30 m.

You can find more information in the section "Terminals (Page 22)".

Digital input

The 2-pin terminal block has the following assignment:



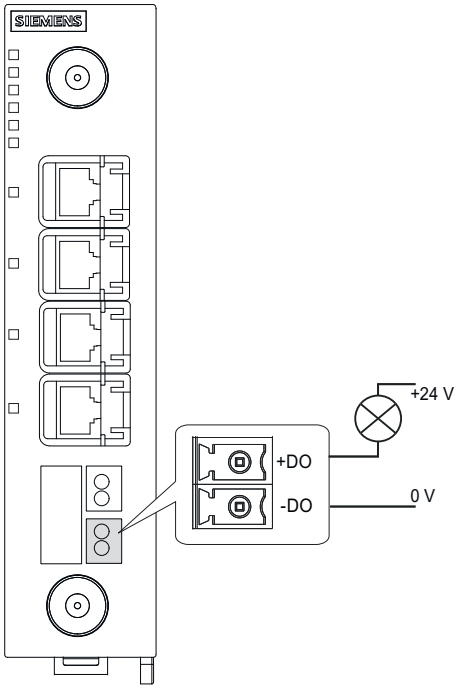
Contact	Assignment
+DI	Input
-DI	Ground

The voltage applied to the "DI" contact is converted to a digital status by the device as follows:

Voltage	Status
-30 to +3 V DC	0
+10 to +30 V DC	1

Digital output

The 2-pin terminal block has the following assignment:



Contact	Assignment
+DO	Switching signal
-DO	Ground

The output is a switch that switches the signal at +DO to -DO.

6.6 Grounding

Grounding for wall mounting

The device is grounded by the fixing screw via the unpainted eyelet, position see section "Device view (Page 20)".

In addition to grounding via the fixing screw, you can also ground the device using the terminal block. The terminal is identified by the symbol for the functional ground ⏚; for the position, see section "Terminals (Page 22)". Connect the terminal of the device with as short

a cable as possible ≤ 150 mm and with the required cross-sectional area to a grounded part of the system.

If the device is mounted on a non-conductive base, grounding must be connected either via the functional ground on the terminal block or via a grounding cable.

The grounding cable is not supplied with the device. Connect the paint-free surface of the device to the nearest grounding point using the grounding cable.

Grounding when installing on a DIN rail / S7 mounting rail

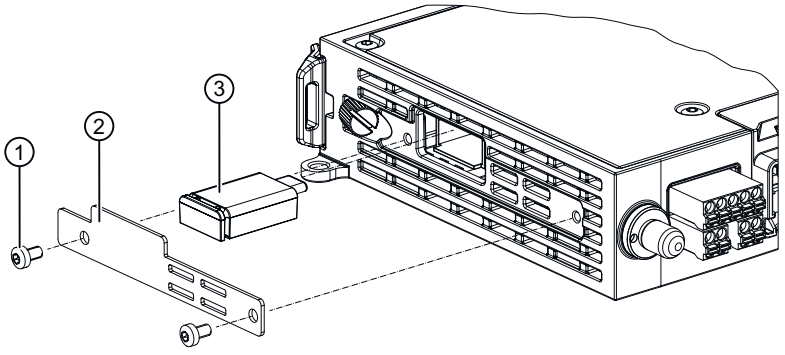
The device is grounded via the rear of the device.

You can also ground the device via the terminal block. The terminal is identified by the symbol for the functional ground ⏚; for the position, see section "Terminals (Page 22)". Connect the terminal of the device with as short a cable as possible ≤ 150 mm and with the required cross-sectional area to a grounded part of the system.

6.7 Replacing a CLP

Position

The CLP slot is at the bottom of the device under a cover, see Reset button (Page 31).



① M3 screws (Torx T10)
② Slot cover
③ CLP

Removing a CLP

Note

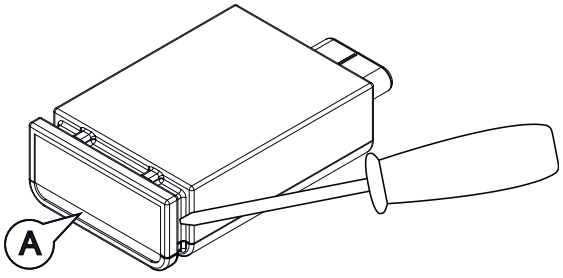
Loss of the configuration

The reset button is located directly beside the slot for the CLP. The reset button cannot be used to remove the CLP.

If you press and hold down the reset button you reset all the settings of the device to the factory defaults.

To remove a CLP from the device, follow the steps below:

1. Turn off the power to the device.
2. Loosen the screws M3 ① with a Torx screwdriver T10 and remove the slot cover ②.
3. To release the CLP ③, insert a screwdriver between the front edge of the CLP (A) and the slot.

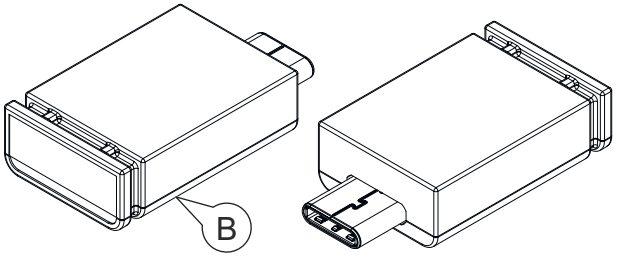


4. Remove the CLP from the slot.
5. Close the slot cover (torque 0.8 Nm) to ensure that the device maintains the degree of protection IP30.

Inserting the CLP

To insert a CLP into the device, follow the steps below:

1. Turn off the power to the device.
2. Loosen the screws M3 ① with a Torx screwdriver T10 and remove the slot cover ②.
3. The housing of the CLP has a rounded underside (B). Accordingly, the slot opening has a rounded edge. Note this orientation when inserting the CLP.
   Insert the CLP ③ in the correct orientation into the slot.



4. Close the slot cover (torque 0.8 Nm) to ensure that the device maintains the degree of protection IP30.

Maintenance and cleaning

7

WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

- Repair work may only be performed by personnel authorized by Siemens.

WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

- Only use original accessories (Page 23) and original spare parts.
- Observe all relevant installation and safety instructions described in the manuals for the device or supplied with the accessories or spare parts.



CAUTION

Hot surfaces

Risk of burns during maintenance work on parts with a surface temperature above 70 °C (158 °F).

- Take appropriate protective measures, for example, wear protective gloves.
- Once maintenance work is complete, restore the touch protection measures.

NOTICE

Cleaning the housing

If the device is not in a hazardous area, only clean the outer parts of the housing with a dry cloth.

If the device is in a hazardous area, use a slightly damp cloth for cleaning.

Do not use solvents.

Troubleshooting

8

8.1 Downloading new firmware using TFTP without WBM and CLI

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

You can download new firmware to the device using TFTP. To do this, the device does not need to be reachable either using Web Based Management (WBM) or using the Command Line Interface (CLI). This can be the case if there was a power failure during a firmware update.

When pressing the button, make sure you adhere to the instructions in the section "Reset button (Page 31)".

To load a new firmware via TFTP, follow these steps:

1. Turn off the power to the device.
2. Loosen the screws of the cover.
3. Remove the cover.
4. Press and hold down the reset button.
5. Connect the device to the power supply again while holding down the button.
6. Hold down the button until the red fault LED "F" starts to flash after approximately 2 seconds (500ms on/500ms off).
7. Release the button. The F-LED lights continuously red.
   The bootloader waits in this state for a new firmware file that you can download using TFTP.
8. Connect a PC to the device over the Ethernet interface.
9. Assign an IP address to the device using DHCP or the SINEC PNI.
10. Open a DOS box and change to the directory where the file with the new firmware is located and then execute the following command:
    `tftp -i <IP address> put <firmware file>`
    As an alternative, you can use a different TFTP client.
    Once the firmware has been transferred completely to the device, there is an automatic restart on the device. This process can take several minutes.
11. Close the cover (torque 0.8 Nm) to ensure that the device maintains the degree of protection IP30.

8.2 Restoring the factory settings

NOTICE
Previous settings If you reset, all the settings you have made will be overwritten by factory defaults.

NOTICE
Inadvertent reset An inadvertent reset can cause disturbances and failures in a configured network with further consequences.

With the reset button

When pressing the button, make sure you adhere to the instructions in the section "Reset button (Page 31)".

To reset the device to the factory defaults during the startup phase, follow the steps below:

1. Turn off the power to the device.
2. Loosen the screws of the cover.
3. Remove the cover.
4. Press the reset button and reconnect the device to the power supply while holding down the button.
5. Hold down the button until the red error LED "F" stops flashing after approximately 10 seconds and is permanently lit.
6. Release the button and wait until the fault LED "F" goes off.
   The device starts automatically with the factory settings.
7. Close the cover (torque 0.8 Nm) to ensure that the device maintains the degree of protection IP30.

With SINEC PNI

Follow the steps below to reset the device parameters to the factory settings with the SINEC PNI:

1. Select the device whose parameters you want to reset.
2. Click the "Reset device" button.
3. Select the "Reset to factory settings" option in the following dialog.

Via the configuration

You will find detailed information on resetting the device parameters using the WBM and CLI in the configuration manuals:

- Web Based Management, section "Restart"
- Command Line Interface, section "Reset and Defaults"

Technical data

9

The following technical specifications apply to the following devices:

- SCALANCE WAM763-1
- SCALANCE WUM763-1

Note

You will find detailed information on the transmit power and receiver sensitivity in the document "Performance data SCALANCE W700 802.11ax" on the Internet at (https://support.industry.siemens.com/cs/de/en/view/109797829).

Technical specifications		
Data transfer		
Ethernet transfer rate		10/100/1000 Mbps
Wireless transmission rate		1 ... 1201 Mbps
Wireless standards supported		IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax
Attachment to Industrial Ethernet		
	Quantity	4
	Design	RJ45 socket
	Properties	Half duplex/full duplex, autocrossover, autonegotiation, autosensing, floating
Permissible cable lengths (Ethernet)	**Alternative combinations per length range**	
	IE TP torsion cable	0 ... 55 m 0 ... 45 m + 10 m TP cord
	IE FC TP marine cable IE FC TP trailing cable IE FC TP flexible cable	0 ... 85 m 0 ... 75 m + 10 m TP cord
	IE FC TP standard cable	0 ... 100 m 0 ... 90 m + 10 m TP cord
Wireless interface		

Technical specifications		
Antenna connector	Quantity	2
	Design	R-SMA female
	Impedance	50 Ω nominal
	Permitted antenna wire lengths	< 30 m
Frequency range		2412 ... 2480 MHz 4920 ... 5875 MHz
Electrical data		
Direct 24 VDC supply	Supply voltage from socket	24 V DC Safety Extra Low Voltage (SELV)/ Protective Extra Low Voltage (PELV)
	Type of current	⎓
	Permitted range ±30 %	16.8 to 31.2 VDC
	Design	Terminal block, 5-pin
	Properties	Not galvanically isolated
Fusing		2.5 A / 24 V DC
Current consumption	24 V DC/ maximum	550 mA
	24 V DC Sleep Mode / maximum	12.5 mA
Active power loss	24 V DC/ maximum	13.2 W
	24 V DC Sleep Mode / maximum	300 mW
Digital input Only SCALANCE WxM763-1 with DI/DO	Quantity	1
	Design	Terminal block, 2-pin
	Rated voltage	24 V DC safety extra-low voltage (SELV)
	Status "0"	-30 to 3 V DC
	Status "1"	10 to 30 V DC
	Max. input current	8 mA
	Max. cable length	< 30 m Cables should be routed in pairs
	Properties	Input isolated from electronics
Digital output Only SCALANCE WxM763-1 with DI/DO	Quantity	1
	Design	Terminal block, 2-pin
	Rated voltage	24 V DC safety extra-low voltage (SELV)
	Max. input voltage	30 V DC safety extra-low voltage (SELV)
	Fuse	0.5 A
	Max. cable length	< 30 m Cables should be routed in pairs
	Properties	Relay, internally not current limited Output isolated from electronics
Permissible ambient conditions		

Technical specifications		
Ambient temperature	During operation	-30 °C ... +60 °C
	During storage	-40 °C to +85 °C
	During transportation	-40 °C to +85 °C
Relative humidity	During operation	≤ 90% at 25 °C, no condensation
Operating altitude	During operation	≤ 2000 m above sea level
Contaminant concentration		According to ISA-S71.04.-2013 Class G3
Degree of pollution		2
Degree of protection		IP30
Dimensions and weight		
Dimensions	W x H x D	35 x 157 x 137 mm
Weight		0.65 kg
Installation options		
	• Wall mounting • Mounting on a DIN rail – direct – rotated by 90° with accessories • Mounting on an S7-300 mounting rail • Mounting on an S7-1500 mounting rail • Mounting on a pedestal	
Mean time between failure (MTBF)		
	at 40 °C ambient temperature	26 years

Dimension drawings

10

Note

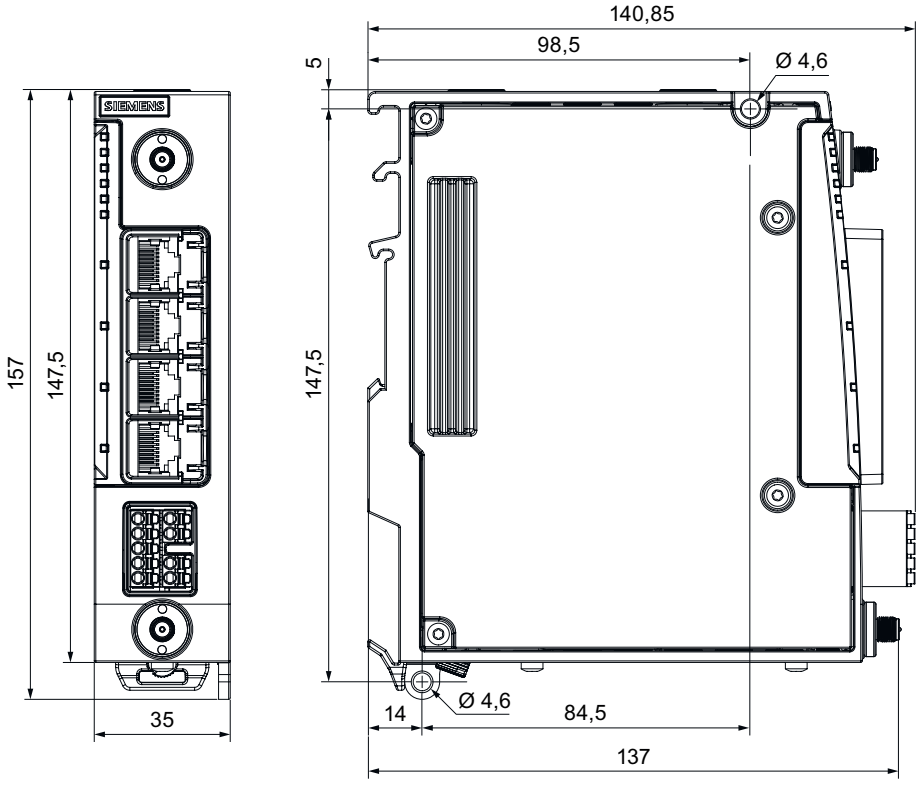
CAx data

You can find the CAx data on the Internet at (https://www.automation.siemens.com/bilddb/index.aspx?lang=en)

1. Click on the "CAx data" link in the "Direct Links" area.
   The Industry Image Database page is loaded.
2. Enter the name or article number of the product in the search filter.
   You can refine your search using the "Motif type" selection list.

Note

Dimensions are specified in mm.



Approvals

11

You will find the approvals of the products in the reference work "Approvals SCALANCE W700 802.11ax" on the Internet pages of the Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/109802595).

You will find the current approvals for the product on the Internet pages of the Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/28575/cert).

Enter the article number of the product as the search term.

Index

A

Accessories, 23
Antenna cables, 25
Antennas, 25
    Connecting, 57
Article number, 5
    Structure, 19

B

Button
    Reset, 31

C

Cables
    Permitted lengths, 69, 70, 71
CAx data, 73
Certification ID, 5
CLP, 32
    Function, 33
    Replacing, 61
Components of the product, 21
Configuration manuals, 6, 67
Connecting
    Antennas, 57
    Digital input, 59
    Digital output, 60
    Ethernet, 56
    Grounding, 60
    Power supply, 22, 55

D

Device view, 20
Digital input, 59
Digital output, 60
Dimension drawing, 73
DIN rail, 41
Documentation on the Internet, 5
Drilling template, 40

E

Ethernet
    Connectors, 56

F

Factory defaults, 66
Factory setting, 66

G

Grounding, 51, 60

I

Installation
    DIN rail, 41
    S7-1500 mounting rail, 46
    S7-300 mounting rail, 45
    Wall mounting, 40
Interfaces, 69, 70, 71

L

LEDs, 28
Lightning protection, 49

P

Pin assignment, 57
PLUG, 32
    Function, 33
    Replacing, 61
Power supply, 22, 55

R

Reset button, 31
Reset device, 66

S

S7-1500 mounting rail, 46

S7-300 mounting rail, 45
Safety extra low voltage, 50
Safety notices
for installation, 35
general, 9
Use in hazardous areas, 9, 35, 49
when connecting up, 49
Scope of validity, 5
System manual, 6

T

Technical specifications, 69, 70, 71
Terminals, 22
Type designation, 19

W

Wall mounting, 40
Wiring, 22