SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE WxM766

Operating Instructions

11/2021

C79000-G8976-C617-03

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-C617-03
Ⓟ 10/2021 Subject to change

Table of contents

Introduction

1

Validity of the Operating Instructions

These operating instructions cover the following products:

Product	Article number	Certification ID
Access points		
SCALANCE WAM766-1	6GK5766-1GE00-7DA0 6GK5766-1GE00-7DB0 (USA)	MSAX65-W1-M12-E2
SCALANCE WAM766-1 EEC	6GK5766-1GE00-7TA0 6GK5766-1GE00-7TB0 (USA)	MSAX65-W1-M12-E2
Client		
SCALANCE WUM766-1	6GK5766-1GE00-3DA0 6GK5766-1GE00-3DB0 (USA)	MSAX65-W1-M12-E2

These operating instructions apply to the following software version:

- SCALANCE WxM76x with firmware version 1.2

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.

Purpose of the Operating Instructions

Using the Operating Instructions, you will be able to install and connect the SCALANCE WxM766 correctly. The configuration and the integration of the device in a WLAN are not described in these instructions.

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/15859/man)

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

Security information

Siemens provides products and solutions with industrial security 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 security concept. Siemens' products and solutions form one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. These systems, machines and components should only be connected to the enterprise network or the Internet if and only to the extent necessary and with appropriate security measures (firewalls and/or network segmentation) in place.

You can find more information on protective measures in the area of industrial security by visiting:
https://www.siemens.com/industrialsecurity
(https://www.siemens.com/industrialsecurity).

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/industrialsecurity
(https://www.siemens.com/industrialsecurity).

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.

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.

Device defective

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

Trademarks

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, read the manual before use.

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.

Security recommendations

3

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 your plant as a whole in terms of security. Use a cell protection concept with suitable products (https://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx).
- 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, Telnet, 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

- The device contains a pre-installed X.509 certificate with key. Replace this certificate with a self-made 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 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".
- Use certificates with a key length of 4096 bits.

- 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 (for example 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 5)".
- 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 11)".
- Use the latest web browser version compatible with the product to ensure you are using the most secure encryption methods available. 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/en/cert-security-advisories.htm) 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.
- For optimal security, use SNMPv3 authentication and encryption mechanisms whenever possible, and use strong passwords.
- Configuration files can be downloaded from the device. Ensure that configuration files are adequately protected. The options for achieving this include digitally signing and encrypting the files, storing them in a secure location, or transmitting configuration files only through secure communication channels.

  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 above all.
- 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 with AES to protect the WLAN. 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, RSTP, 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
  - Syslog
  - 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.

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 port status**

- **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
			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	✓	✓	--	--
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	✓	✓	--	✓

Service	Protocol /	Default	Configurable		Authenticati	Encryption
Telnet	TCP/23	Closed	✓	✓	✓	--
TFTP Server	UDP/69	Closed	✓	✓	--	--
TCP Event	TCP/26864	Closed	✓	✓	✓	--

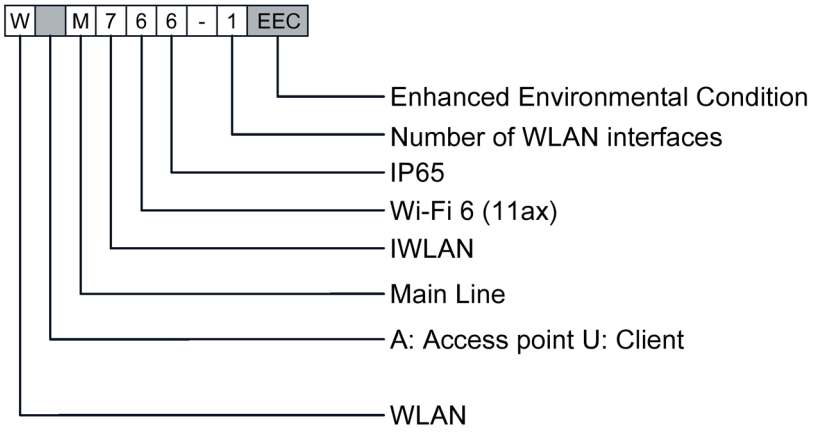
Layer 2	Default Status	Configurable
DCP	Open	✓
LLDP	Open	✓
RSTP	Closed	✓
iPRP	Closed	✓
MSTP	Closed	✓
SIMATIC NET TIME	Closed	✓
802.1x	Closed	✓

Description of the device

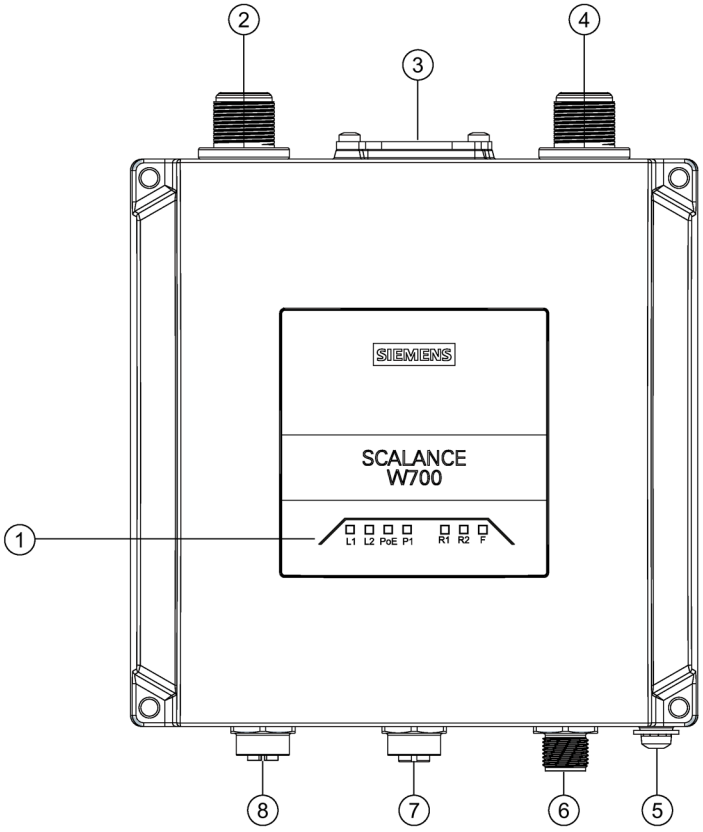
4

Structure of the type designation

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



4.1 Device view



① LED display
② R1A1 antenna connector, female N-Connect type
③ Screw-down cover:
- for the reset button and
- for the PLUG slot (CLP)
④ R2A1 antenna connector, female N-Connect type
⑤ Ground connector (thread M4) on the bottom
⑥ Connector for power supply (L1, L2)
⑦ Digital input (DI) / Digital output (DQ)
⑧ Ethernet connector P1 (PoE capability)

4.2 Components of the product

The following components are supplied with the product:

- One SCALANCE W device
- One cover for CLP slot
- Two protective caps for the antenna sockets
- Three protective caps for the M12 sockets
  - 1 x Ethernet
  - 1 x power supply
  - 1 x digital input/digital output
- One grounding screw

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
- DIN rail adapter

You will find more detailed information in "Accessories (Page 21)".

4.3 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)

4.3.1 Installation

Component	Description	Article number
Mounting adapter DIN rail	Adapter for mounting on a 35mm DIN rail according to DIN EN 50 022	6GK5798-8MF00-0AA1
Angle adapter	90° angle adapter for rail mounting, only in conjunction with SCALANCE MUM856-1, WAM/ WUM766-1; Scope of delivery: Bracket with mounting rail adapter for 35 mm standard mounting rail, fixing screws	6GK5798-8MF00-0AB1

4.3.2 CLP

PLUG

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
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

4.3.3 Industrial Ethernet

Cables Industrial Ethernet (pre-assembled)

Component	Description	Article number
IE TP Cord M12-180/RJ45-180	IE Flexible Cable, with 1 x M12 plug (X-coded) 180 degree cable outlet and 1 x RJ45 plug; 180 degree cable outlet	
	Length 0.5m	6XV1878-5TE50
	Length 1m	6XV1878-5TH10
	Length 1.5m	6XV1878-5TH15
	Length 2m	6XV1878-5TH20
	Length 3m	6XV1878-5TH30
	Length 5m	6XV1878-5TH50
	Length 10m	6XV1878-5TN10

Component	Description	Article number
	Length 15m	6XV1878-5TN15
IE TP Cord M12-90/RJ45-180	IE Flexible Cable, with 1 x M12 plug (X-coded) 90 degree cable outlet and 1 x RJ45 plug; 180 degree cable outlet	
	Length 0.5m	6XV1878-5SE50
	Length 1m	6XV1878-5SH10
	Length 1.5m	6XV1878-5SH15
	Length 2m	6XV1878-5SH20
	Length 3m	6XV1878-5SH30
	Length 5m	6XV1878-5SH50
	Length 10m	6XV1878-5SN10
	Length 15m	6XV1878-5SN15

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

M12 plug-in connector Industrial Ethernet

Component	Description	Article number
IE FC M12 PLUG PRO 4x2	M12 data plug-in connector for IE FC TP cables 4x2, IP65/67, X-coded, axial cable outlet	
	1 connector per package	6GK1901-0DB30-6AA0
	8 connectors per package	6GK1901-0DB30-6AA8
IE FC M12 CABLE CONNECTOR PRO 4X2	M12 plug-in connector (X-coded) can be assembled in the field, 8-pin, metal housing, FC fast connection technology, socket insert	
	1 connector per package	6GK1901-0DB40-6AA0
	8 connectors per package	6GK1901-0DB40-6AA8

4.3.4 Digital input / digital output

Cables digital input / digital output (pre-assembled)

Component	Description	Article number
Control Connecting Cable M12-180/M12-180 (A-coded)	5-wire; IO-Link port class B; pre-assembled with M12 plug and M12 socket (A-coded); straight cable outlet Pack of 1	
	Length 0.5m	6XV1801-2CE50
	Length 1m	6XV1801-2CH10
	Length 1.5m	6XV1801-2CH15
	Length 2m	6XV1801-2CH20
	Length 3m	6XV1801-2CH30
	Length 5m	6XV1801-2CH50
	Length 10m	6XV1801-2CN10
	Length 15m	6XV1801-2CN15

Cables DI/DO interface (sold by the meter)

Component	Description	Article number
SIMATIC NET CONTROL CABLE	5-wire power cable, stranded wire, 5 x AWG24; package item: max. 1000m, minimum order quantity 20m Sold by the meter	6XV1801-2C

M12 plug-in connector digital input / digital output

Component	Description	Article number
Control M12 Plug PRO	Control M12 Plug PRO; field-assembled connector for connecting IO-Link sensors/actuators; 5-pin; A-coded Pack of 1	6GK1908-0DB10-6AA0

4.3.5 Power supply

Power cables (pre-assembled)

Component	Description	Article number
M12 connecting cable, L-coded, 4-pin M12-180	Flexible plug-in energy cable to connect the power supply 24 V DC, 4-wire, preassembled with a 4-pin M12 plug and an M12 socket (L-coded)	6XV1801-6D*
M12 connecting cable, L-coded, 4-pin M12-90	Flexible plug-in energy cable to connect the power supply 24 V DC, 4-wire, preassembled with a 4-pin M12 plug and an M12 socket (L-coded)	6XV1801-6G*

* Available in different lengths

Power cable (sold by the meter)

Component	Description	Article number
Energy Cable 4 x 1.5	Power cable for connecting the 24 V DC power supply, 4-wire, stranded 4 x 1.5 mm^2, trailing type, not assembled Sold by the meter	6XV1801-2B

M12 plug-in connector power supply

Component	Description	Article number
Power M12 Cable Connector Pro	Power M12 Cable Connector PRO axial cable outlet for field assembly, female contact insert, L-coded (socket) Pack of 1	6GK1906-0EB00

Cabinet feedthrough

Component	Description	Article number
IE M12 Panel Feedthrough 4x 2	Cabinet feedthrough for conversion from M12 connector technology (X-coded, IP65/67) to RJ-45 connector technology (X-coded, IP20) pack of 5	6GK1901-0DM40-2AA5
N-Connect/N-Connect Female/Female Panel Feedthrough	Panel feedthrough for wall thicknesses up to a maximum of 4.5 mm, two N-Connect female connectors.	6GK5798-2PP00-2AA6
N-Connect/SMA Female/Female Panel Feedthrough	Panel feedthrough for wall thicknesses up to a maximum of 5.5 mm, two N-Connect/SMA female connectors.	6GK5798-0PT00-2AA0

4.3.6 Flexible connecting cables and antennas

4.3.6.1 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 a SCALANCE W device with N-Connect connectors.
Preassembled 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

Flexible connecting cable IWLAN QMA/N-Connect male/female

Adapter cable for connecting a MIMO antenna with QMA connectors with the flexible connecting cables. Preassembled with two connectors QMA male and N-Connect female. pack of 3

Length	Article number
1 m	6XV1875-5JH10

For railway applications, the following connecting cable is available Note: Scope of delivery: Pack of 1

Length	Article number
1 m	6XV1875-5VH10

4.3.6.2 Lightning protection

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

4.3.6.3 Terminating resistor

Terminating resistor

Component	Description	Article number
TI795-1N	Electrical connection N-Connect, male Pack of 1	6GK5795-1TN00-1AA0

4.3.6.4 Antennas

Note

When you select an antenna, keep in mind:

- The antennas with national approval for your device You can find additional information on this at (https://www.siemens.com/wireless-approvals).
- The country-specific and channel-dependent maximum permissible antenna gain You can find additional information on this in the reference document "Approvals for SCALANCE W700 802.11ax".

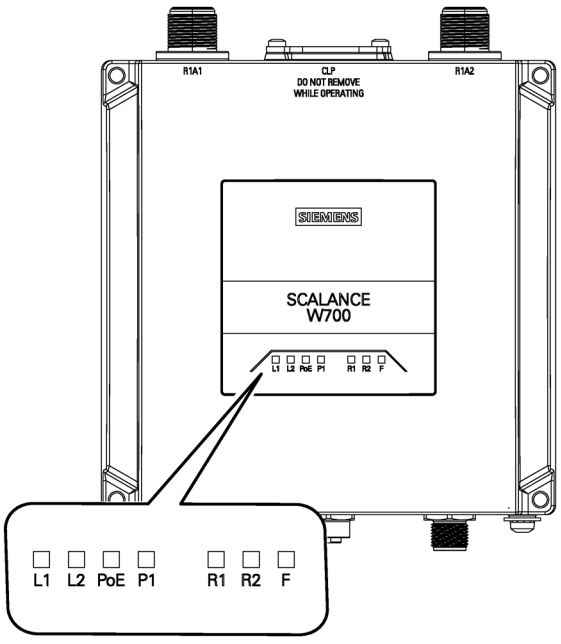
Type	Properties	Article number
ANT792-4DN	RCoax helical antenna, circular polarization, 4 dBi, 2.4 GHz, N-Connect female.	6GK5792-4DN00-0AA6
ANT792-6MN	Omni antenna, mast/wall mounting, 6 dBi 2.4 GHz, N-Connect female	6GK5792-6MN00-0AA6
ANT792-8DN	Directional antenna, mast/wall mounting, 14 dBi 2.4 GHz, N-Connect female	6GK5792-8DN00-0AA6
ANT793-6DG	Wide angle antenna, mast/wall mounting, 9 dBi 5 GHz, 2 x N-Connect female	6GK5793-6DG00-0AA0
ANT793-8DJ	Directional antenna, mast/wall mounting, 18 dBi 5 GHz, 2 x N-Connect female	6GK5793-8DJ00-0AA0
ANT793-8DK	Directional antenna, mast/wall mounting, 23 dBi 5 GHz, 2 x N-Connect female	6GK5793-8DK00-0AA0
IWLAN RCoax ANT793-4MN	RCoax λ 4 antenna with vertical polarization for RCoax systems, 6 dBi, 5 GHz, IP65, N-Connector female	6GK5793-4MN00-0AA6
ANT795-4MC	Omnidirectional antenna, 3/5 dBi, 2.4 GHz and 5 GHz, IP65, N-Connect male for direct installation on the device, straight connector.	6GK5795-4MC00-0AA3
ANT795-4MD	Omnidirectional antenna, 3/5 dBi, 2.4 GHz and 5 GHz, IP65, N-Connect male for direct installation on the device, 90° connector.	6GK5795-4MD00-0AA3
ANT795-6DC	Wide angle antenna, mast/wall mounting, 9 dBi 2.4 GHz and 5 GHz, N-Connect female	6GK5795-6DC00-0AA0
ANT795-6MN	Omni antenna, mounted on roof/vehicle, 6/8 dBi 2.4 GHz and 5 GHz, N-Connect female	6GK5795-6MN10-0AA6
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-Connect female	6GK5793-8DP00-0AA0

Type	Properties	Article number
ANT795-4MX	Omnidirectional antenna, 2/2.5 dBi, 2.4 GHz and 5 GHz, IP69K, N-Connector male	6GK5795-4MX00-0AA0
ANT795-6MP	Omnidirectional antenna, 5/7 dBi, 2.4 GHz and 5 GHz, IP65/67, N-Connector female	6GK5795-6MP00-0AA0
IWLAN RCoax Cable 2,4 GHz PE 1/2"	Omni antenna, 0 dBi 2.400 - 2.485 GHz, N-Connect female	6XV1875-2A
IWLAN RCoax Cable 5 GHz PE 1/2"	Omni antenna, 0 dBi 5.150 – 5.875 GHz, N-Connect female	6XV1875-2D

4.4 LED display

Information on operating status and data transfer

On the front of the housing, several LEDs provide information on the operating status of the device:



LED	Color	Meaning
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.
PoE	Off □	The device is not supplied using PoE.
	Green ■	The device is supplied using PoE. Note: If the device is simultaneously connected to 24V voltage (L1/L2), the power supply to the device is via L1/L2.
P1	Off □	There is no connection over the Ethernet interface P1.

LED	Color	Meaning
	Green 	There is a connection over the Ethernet interface P1 (link).
	Flashing green and yellow 	Data transfer over the Ethernet interface P1.
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 	*Client mode:* The client is connected to the access point.
	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.
R2	Off 	The functionality of this LED will be configurable for different applications. It is disabled by default.
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 (Page 65)".
	Flashing red  Interval: 2000 ms on / 200 ms off	Firmware on PLUG: The device is performing a firmware update or downgrade.

LED	Color	Meaning
	Red  Simultaneous R1 yellow flashing 	A competing radar signal was found on all enabled channels.
R1 R2	Flashing yellow 	The port LEDs flash for detection of device location. The "Blink Own LEDs" function is activated: • Either with SINEC PNI • Or via the WBM page "Discovery and Set via PROFINET Discovery and Configuration Protocol (DCP)".
	Flashing green 	The LEDs R1 and R2 are flashing green simultaneously in the following cases: • The WxM766 device scans the selected Ethernet interface for the devices with the Discovery Configuration Protocol (DCP) in the same subnet. You select the interface in the WBM, "System > DCP Discovery" menu. • An LED flashing test is performed via SINEC PNI to test the availability of the WxM766 device. You can find more detailed information in the SINEC PNI manual, section "Device list".

Note

Primary user (radar) on all enabled channels

If the device detects a primary user (for example radar signals) on all enabled channels of the WLAN interface, the LED **F** is lit and **R1** flashes. No data traffic is then possible for the next 30 minutes. After this time, the device runs the scan again and checks whether a primary user still exists. If no primary user is detected, data traffic is possible again.

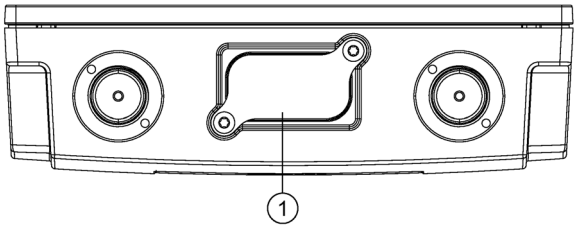
The wait time of 30 minutes is necessary due to legal requirements and cannot be shortened even by restarting the device.

4.5 Reset button

Position

NOTICE
Loss of water and dust protection
If the cover is not mounted correctly, the device is not water and dust proof.

The reset button ① is located behind the screw-down cover on the top of the housing.



① PLUG slot with the reset button (covered)

Functions

The reset button has the following functions:

- **Restart of 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 new firmware**

  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. For more detailed information, refer to section "Upkeep and maintenance (Page 63)".

- **Restoring the default parameters (factory defaults)**

  For more detailed information, refer to section "Upkeep and maintenance (Page 63)".

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

Assembly and disassembly

5

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.

5.1 Disassembly

⚠ 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.

⚠ 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

The device may only be operated in an environment of pollution degree class 2.

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.

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 3836.8.

⚠ WARNING

The equipment shall only be used in an area of not more than pollution degree 2, as defined in EN/IEC 60664-1, GB/T 16935.1.

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 cable or housing socket exceeds 70 ° C or the branching point of the cables exceeds 60 ° C, special precautions must be taken. If the equipment is operated in an air ambient in excess of 40 ° C, only use cables with admitted maximum operating temperature of at least 80 °C.

5.2 Types of installation

Note

The device is only approved for operation in closed rooms. Note the following environmental conditions.

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

For the device the following types of installation are permitted:

- Wall mounting
- Ceiling mounting

- Mounting on VESA bracket 75 x 75 mm
- Mounting on a DIN rail

  The device can be mounted on a DIN rail with

  – A DIN rail mounting adapter

  – A bracket support and the DIN rail mounting adapter for space-saving installation (90° installation)

Note

Installation in the upward position when using the device according to UL

Operation in the upward position (e.g. desktop operation) has not been tested according to UL for this device and is therefore not permitted.

5.3 Wall mounting

Note

Depending on the mounting surface, use suitable fittings.

Note

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

To mount the device on a wall, follow the steps below:

1. Prepare the drill holes for wall mounting. For the precise dimensions, refer to the section "Dimension drawing (Page 73)".
2. Secure the device to the wall with four screws. The screws are not supplied with the device.
3. Connect the power supply, refer to the section "Power supply (Page 52)".
4. Fit the antennas, refer to the section "Antennas (Page 55)".

5.4 Mounting on VESA bracket

For mounting the device on the VESA 75 x 75 mm wall holder, 4x M4 threaded holes with a thread depth of 8.5 mm are provided on the back of the device, see the "Dimension drawing (Page 73)" section. The wall holder and M4 screws are not included in the scope of delivery of the device.

Note

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

To install the device on the wall holder, follow the steps below:

1. Screw the device to the wall holder with four M4 screws.
2. Connect the power supply, refer to the section "Power supply (Page 52)".
3. Fit the antennas, refer to the section "Antennas (Page 55)".

5.5 DIN rail mounting

5.5.1 Installation with the DIN rail mounting adapter

The DIN rail mounting adapter is not included with the product, see Accessories (Page 22).

Mounting

1. Screw (M3 x 8, tightening torque 0.8 Nm) the DIN rail mounting adapter ❶ onto the rear of the device. The mounting material is supplied with the DIN rail mounting adapter.

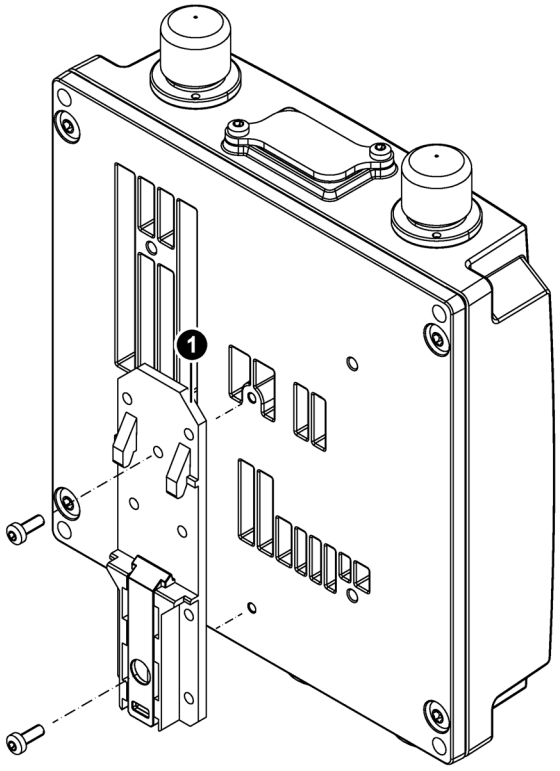
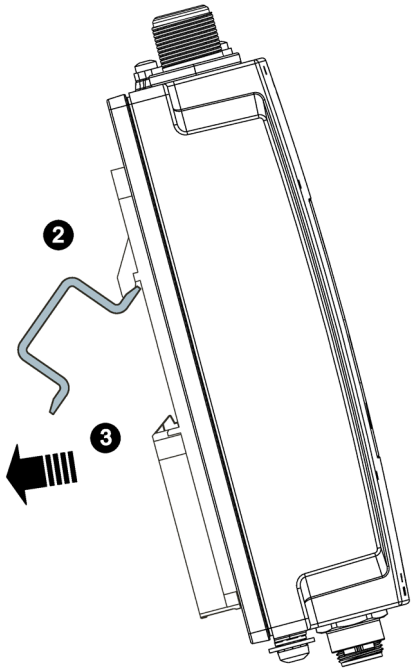


Figure 5-1 W7x8 with adapter plate

2. Place the device on the upper edge of the DIN rail ❷.

3. Press the device against the DIN rail ❸ until the DIN rail slider catch locks in place.

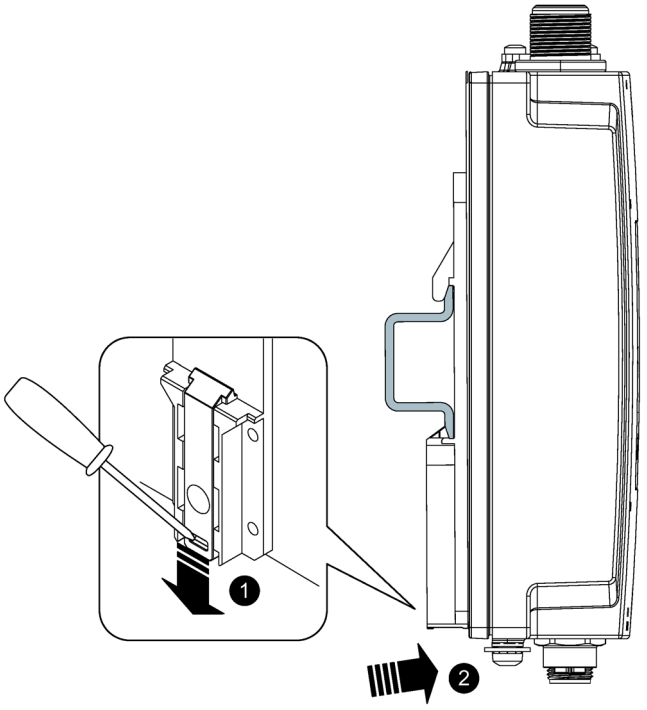


4. Connect the power supply, refer to the section "Power supply (Page 52)".
5. Fit the antennas, refer to the section "Antennas (Page 55)".

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.

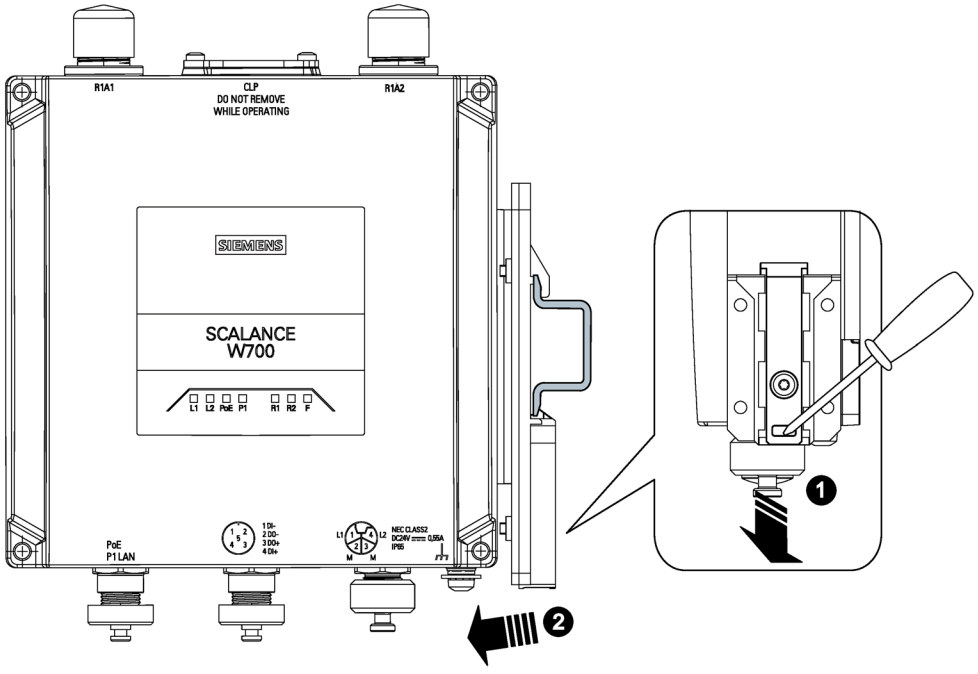
4. Tilt the device forward ❷ and remove the device from the DIN rail.



5. Loosen the screws of the DIN rail mounting adapter completely.

5.5.2 Mounting with bracket support

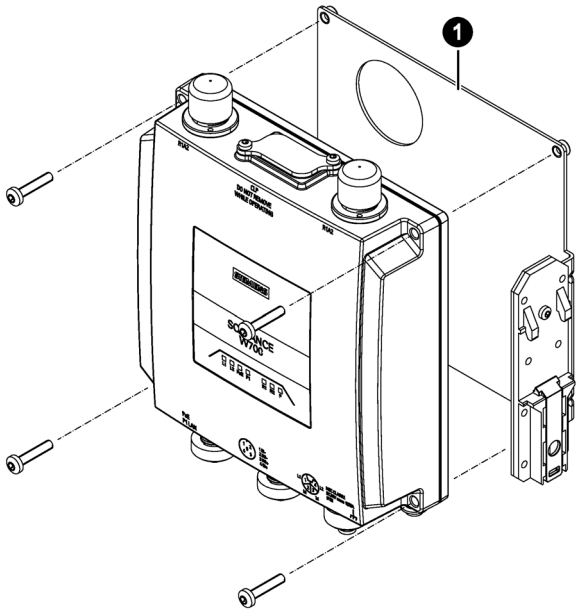
With the bracket support the device can be mounted on a DIN rail rotated through 90°



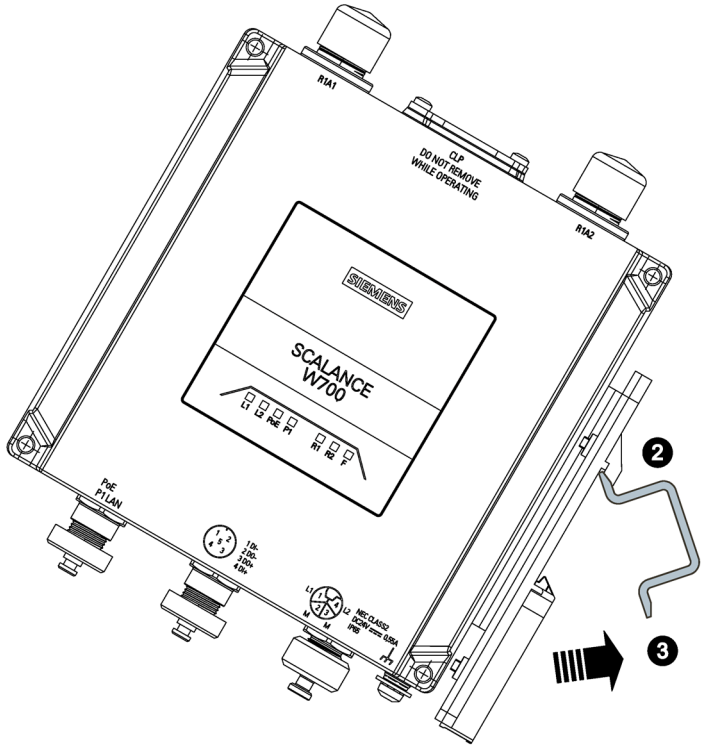
The DIN rail mounting adapter and bracket holder are not included with the product, see Accessories (Page 22).

Mounting

1. Screw (M4 x 20, tightening torque 1.8 Nm) the angle bracket ❶ onto the rear of the device.



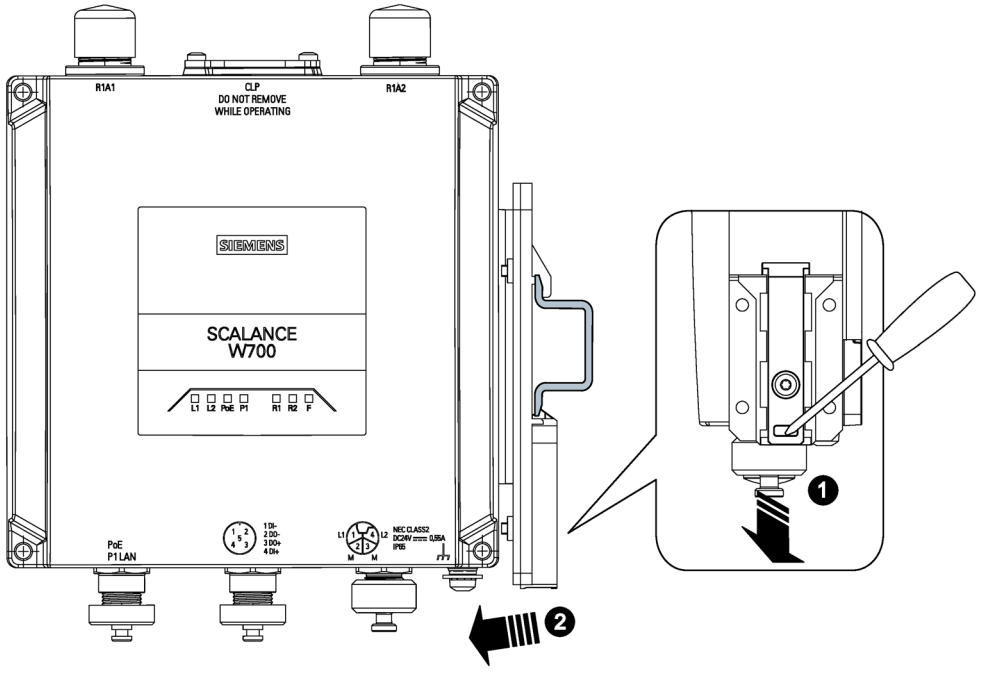
2. Place the device on the upper edge of the DIN rail ❷.
3. Press the device ❸ against the DIN rail until the DIN rail slider catch locks in place.



4. Connect the power supply, refer to the section "Power supply".
5. Fit the antennas, refer to the section "Antennas".

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 completely.

Connection

6

Safety notices

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

⚠ WARNING

EXPLOSION HAZARD

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

⚠ WARNING

EXPLOSION HAZARD

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

Note

Close unused sockets

Close all unused M12 sockets with protective caps (tightening torque at least 0.4 Nm) to achieve the specified type of protection.

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 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) from a limited power source (LPS).

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

- Only safety extra low voltage (SELV) with limited power source (LPS) complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 or 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.

WARNING

Transient overvoltages

It must be ensured that the transient protection is set to a value which does not exceed 140% of the rated peak voltage value and 119 V at the supply terminals of the device. Operate the devices only with SELV (safety extra low voltage).

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

Protective ground

A PELV circuit contains a connection to protective ground. Without a connection to protective ground, or in case there is a fault in the connection to the protective 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.

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.

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 the case if you only operate devices with SELV (safety extra-low voltage).

WARNING

At an ambient temperature of more than 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

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.

6.1 Power supply

Note

Galvanic isolation of the power supply unit

To ensure dielectric strength according to IEEE 802.3, the supplying 24 V power supply unit must be galvanically isolated with a dielectric strength of 1500 VAC. The galvanic isolation must also not be bridged by other devices connected to the same power supply unit.

Note

All power supplies (24 V power supply unit or PoE) must not be connected to a mains supply higher than 300 V and the overvoltage category II.

Information on the power supply

There are two options for the power supply:

- Power over Ethernet via the 8-pin M12 Ethernet interface P1 (position ①).

  The power supply cannot be connected redundantly.

- Direct infeed via the 4-pin M12 socket (position ②)

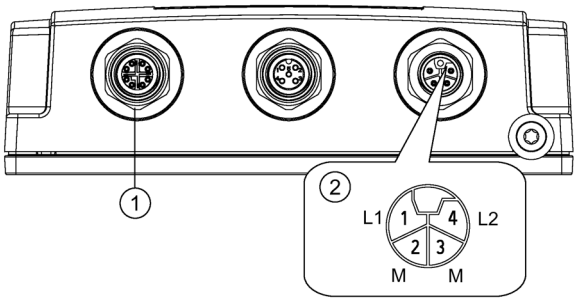
  The power supply can be connected redundantly. The inputs L1/L2 are decoupled There is no distribution of load. The power supply unit with the higher output voltage supplies the device alone.

For the direct feed-in of the power supply use copper cables with the following properties:

- Round cable cross-section with 6 to 8 mm diameter.
- Two-wire cable with 0.5 (AWG20) to 1.5 mm^2 (AWG20) cross-section per wire. The temperature stability must be at least 105 ° C.
- With redundant power supply: Four-wire cable with 0.5 (AWG20) to 1.5 mm^2 (AWG20) cross-section per wire. The temperature stability must be at least 105 ° C.
- Permitted tensile load at least 100 N.
- Listing of the cables according to the national installation regulations. In areas where NEC or CEC applies: Type PTLC or ITC

To connect the functional ground, use a copper cable of category 20 AWG or a cable with a cross-section ≥ 0.75 mm².

Position and pin assignment



① M12 Ethernet interface P1 LAN PoE, X-coded, 8-pin
The power can also be supplied via this interface (Power over Ethernet).
Pin assignment, see Ethernet (Page 54)

② M12 interface, direct infeed, L-coded, 4-pin

The four-pin M12 socket has the following pin assignment:

Pin	Signal	Assignment
1	L1+	24 V DC
2	M	Ground
3	M	Ground
4	L2+	24 V DC

Connecting/disconnecting the power supply

⚠ WARNING

Danger from electric shock

Turn off the power supply before you insert or remove the plug of the power supply.

1. Connect the plug and socket. Make sure that they lock in place correctly.
2. Tighten the knurled screw (tightening torque 1 Nm).

Power over Ethernet (PoE)

Note

Before you pull a plug via which the device is supplied with power using PoE, disable the relevant PoE power supply.

Note

No power sourcing equipment (PSE)

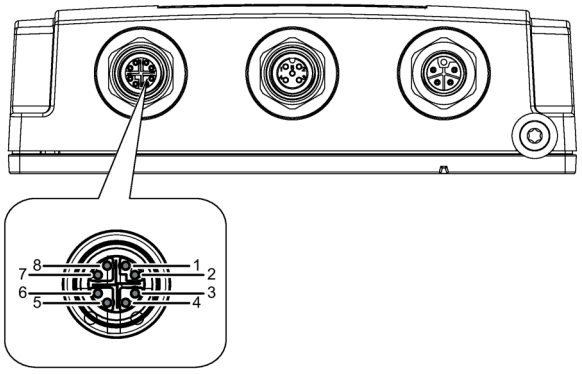
The SCALANCE WxM766-1 devices cannot be used as PoE power supply for other devices.

6.2 Ethernet

For connection to Industrial Ethernet at 10/100/1000 Mbps, the device has an M12 interface: X-coded, 8-pin.

The power can also be supplied via this interface (Power over Ethernet)

Position and pin assignment



Pin	Assignment
1	D0+
2	D0-
3	D1+
4	D1-
5	D3+
6	D3-
7	D2-
8	D2+

Connecting Ethernet ports

1. Connect the plug and socket. Make sure that they lock in place correctly.
2. Tighten the knurled screw (torque 1 Nm).

6.3 Antenna connector

The SCALANCE WxM 766-1 has two antenna connectors of the female N-Connector type.

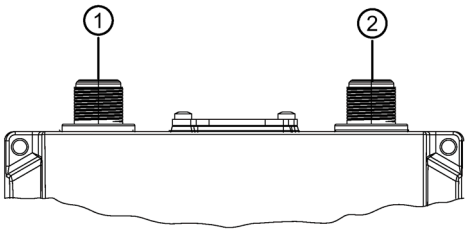


Figure 6-1 Antenna connectors

① Antenna connector R1 A1
② Antenna connector R1 A2

Procedure

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

1. Remove the protective cap from the affected N-Connector on the device.

   Note
   Keep the protective caps

   Keep the removed protective caps for later use.

2. You can connect an external antenna directly to the device or connect it with a flexible connecting cable.

   Place the antenna plug or the flexible connecting cable on the antenna connector and tighten the sleeve nut of the plug on the antenna connector (wrench SW19, torque 1.7 Nm).

3. An antenna must always be connected to R1 A1 ①. You can find additional information on configuration of antennas in the WBM / CLI.
4. Screw a terminating resistor onto the unused antenna connector.

Note
Terminating resistor

Any connections that are not in use must be fitted with a terminating resistor, see Accessories (Page 21).
An antenna must always be connected to the antenna connector as soon as the WLAN interface is switched on. Otherwise, there may be transmission disruptions.

Note

Cabinet installation

When installing the SCALANCE WxM766-1 in a cabinet, you need to use detached antennas. Use a suitable flexible connecting cable for a connection between SCALANCE WxM766-1 and a detached antenna. You will find detailed information in the section Accessories (Page 21).

NOTICE

UL approval only for use in buildings

Within the area of authority of the NEC and CEC, the SCALANCE WxM766-1 devices and the antennas connected to them 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 or CSA requirements.

6.4 Grounding

EMC disturbances are diverted to ground via the functional ground. This ensures the immunity of the data transmission.

The grounding screw is identified by the following symbol for the functional ground  .

Protective earth/functional ground

The connection of the reference potential surface with the protective earth system is normally in the cabinet close to the power feed-in. This earth conducts fault currents to ground safely and according to DIN/VDE 0100 is a protective earth to protect people, animals and property from too high contact voltages.

Apart from the protective earth, there is functional grounding in the cabinet. According to EN60204-1 (DIN/VDE 0113 T1) electrical circuits must be grounded. The chassis (0 V) is grounded at one defined point. Here, once again the grounding is implemented with the lowest leakage resistance to ground in the vicinity of the power feed-in.

With automation components, functional ground also ensures interference-free operation of a controller. Via the functional ground, interference currents coupled in via the connecting cables are discharged to ground.

Position

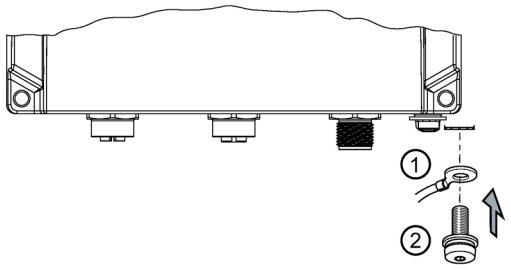
The functional ground is established via a grounding screw.

The connector for the grounding cable is located on the bottom of the device, see ⑤ of the device description (Page 20)

Connecting up functional ground

Follow the steps below to connect the functional ground:

1. Put the grounding terminal ①, and the screw ② together as shown in the drawing.



① Grounding terminal with cable
② Screw (M4 thread) with spring washer and washer

2. Screw in the screw ② with a maximum tightening torque of 1.5 Nm.

6.5 Digital input/output

The device features a digital input and output (M12 A-coded).

⚠ CAUTION

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

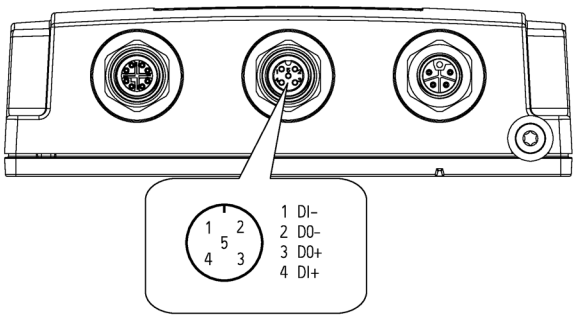
Interference pulse

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

Rules for user wiring

- Always wire the digital input/output in pairs.
- The maximum permitted cable length is ≤ 3 m.

Position / Assignment



1	DI-	Input ground
2	DO-	Relay 24 V DC / 0.5 A
3	DO+	Relay 24 V DC / 0.5 A
4	DI+	24 V DC
5	NC	Not connected

6.6 Inserting/removing the 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

Do not remove or insert a PLUG during operation!

A PLUG may only be removed or inserted when the device is turned off.
The device checks whether a PLUG is inserted at one second intervals. If it is detected that the PLUG was removed, there is a restart.

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

NOTICE

Loss of water and dust protection

If the cover is not mounted correctly, the device is not water and dust proof.

How it works

The device supports the following modes of operation:

- Without PLUG

  The device saves the configuration data in the internal memory. This mode is active when no PLUG is inserted.

- With PLUG

  If an empty PLUG (as supplied) is inserted in the device, the device automatically backs up the configuration data on the PLUG during startup. If the PLUG contains a license, additional functions are also enabled. Changes to the configuration are stored directly on the PLUG and in the internal memory.

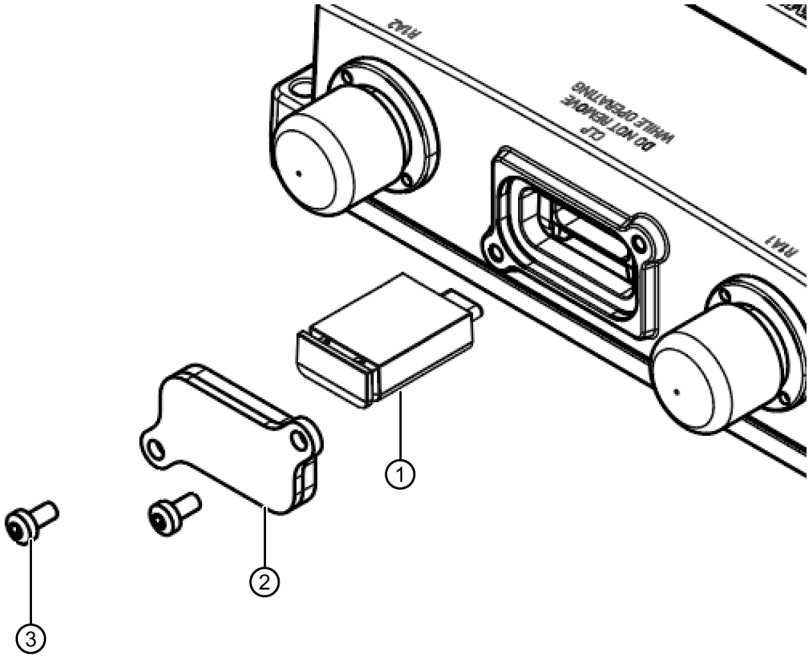
  The configuration stored on the PLUG is displayed over the user interfaces.

  When an unconfigured device starts up, it automatically adopts the configuration data of the inserted, written PLUG. 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.

Position

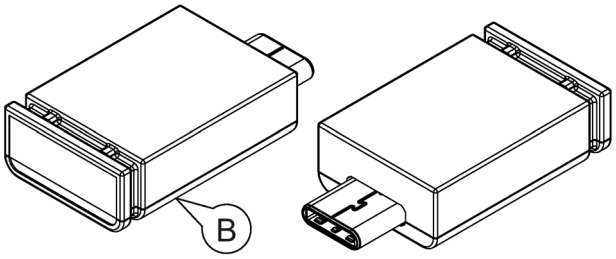
The PLUG slot is on the top of the device housing under a cover, see Reset key.



Inserting the PLUG

Follow the steps below to insert a PLUG in the device:

1. Turn off the power to the device.
2. The PLUG slot is on the bottom of the device housing under a cover, see Reset button.
3. Loosen the screws ③ of the slot cover and remove the slot cover ②. As an alternative, you can loosen only one of the screws ③ and swivel the slot cover ② to the side.
4. The housing of the PLUG has a rounded underside (B). The slot also has a rounded underside. Insert the PLUG in the correct orientation into the slot.

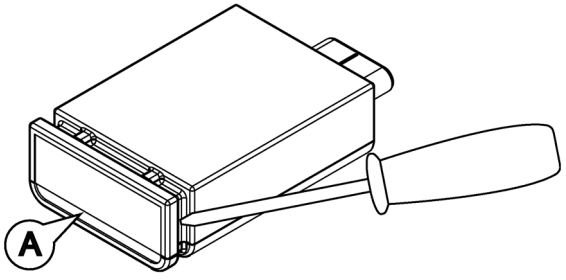


5. Close the slot cover (torque 0.8 Nm) to ensure that the device is closed, water-proof and dust-proof.

Removing the PLUG

Follow the steps below to remove a PLUG from the device:

1. Turn off the power to the device.
2. Loosen the screws ③ of the slot cover and remove the slot cover ②. As an alternative, you can loosen only one of the screws ③ and swivel the slot cover ② to the side.
3. Insert a screwdriver between the front edge of the PLUG (A) and the slot and release the PLUG ①.



4. Remove the PLUG ① from the slot.
5. Close the slot cover (torque 0.8 Nm) to ensure that the device is closed, water-proof and dust-proof.

Note

Loss of the configuration

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

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

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 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.

8.2 Downloading new firmware using TFTP without WBM and CLI

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 33)".

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 (tightening torque 0.8 Nm), to ensure that the device is closed and water and dust proof.

8.3 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 33)".

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 (tightening torque 0.8 Nm), to ensure that the device is closed and water and dust proof.

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 specifications

9

The following technical specifications apply to the following devices:

- SCALANCE WAM766-1
- SCALANCE WAM766-1 EEC
- SCALANCE WUM766-1

Note

You will find detailed information on the transmit power and receiver sensitivity in the document "Performance data SCALANCE W700 802.11ax" on the supplied data storage medium (NW_W700ax-RadioInterface_*.pdf).

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
Power supply for POE standards supported	Standards	IEEE802.3bt/ IEEE802.3at/ IEEE802.3af
	Class	Class 0 (0.44 ... 12.96 W)
Attachment to Industrial Ethernet		
	Quantity	1
	Design	M12 socket, X-coded
	Properties	Half duplex/full duplex, autocrossover, autonegotiation, autosensing, floating, PoE
Permitted 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	N-Connect socket
	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 VDC Safe Extra Low Voltage (SELV)
	Type of current	⎓
	Permitted range ±30 %	16.8 to 31.2 VDC
	Design	M12 socket, L-coded
	Properties	Not galvanically isolated
Supply voltage from PoE	Power supply	48 VDC
	Type of current	⎓
	Permitted range	36 to 57 VDC
	Design	M12 socket, X-coded
	Properties	Galvanically isolated
Fusing		2.5 A / 24 V DC
		1 A / 48 V PoE
Current consumption	24 V DC/ maximum	550 mA
	PoE 48 V / maximum	270 mA
	24 V DC Sleep Mode / maximum	12.5 mA
Effective power loss	24 V DC/ maximum	13.2 W
	PoE 48 V / maximum	12.96 W
	24 V DC Sleep Mode / maximum	300 mW
Digital input	Quantity	1
	Design	M12 socket, A-coded
	Status "0"	-30 to 3 V DC
	Status "1"	10 to 30 V DC
	Max. input current	8 mA
	Max. cable length	< 3 m Cables should be routed in pairs
	Properties	Input isolated from electronics
Digital output	Quantity	1
	Design	M12 socket, A-coded
	Fuse	0.5 A
	Max. cable length	< 3 m Cables should be routed in pairs
	Properties	Output isolated from electronics
Permitted ambient conditions		

Technical specifications			
Ambient temperature	During operation	Non-EEC variant	-30 ° C ... +60 ° C
		EEC variant	-30 °C to +75 °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 • Non EEC variant max. 60 ° C • EEC variant max. 75 ° C > 2000 m above sea level • Only EEC variant max. 70 ° C
Contaminant concentration			According to ISA-S71.04.-2013 Class G3
Degree of pollution			2
Degree of protection			IP65
Dimensions and weight			
Dimensions	W x H x D		150 x 179.4 x 45 mm
Weight			1.1 kg
Installation options			
Direct:	Wall mounting		
With additional adapter	Mounting on a DIN rail		
Mean time between failure (MTBF)			
	at 40 ° C ambient temperature		24 years

Dimension drawing

10

Note

CAx data

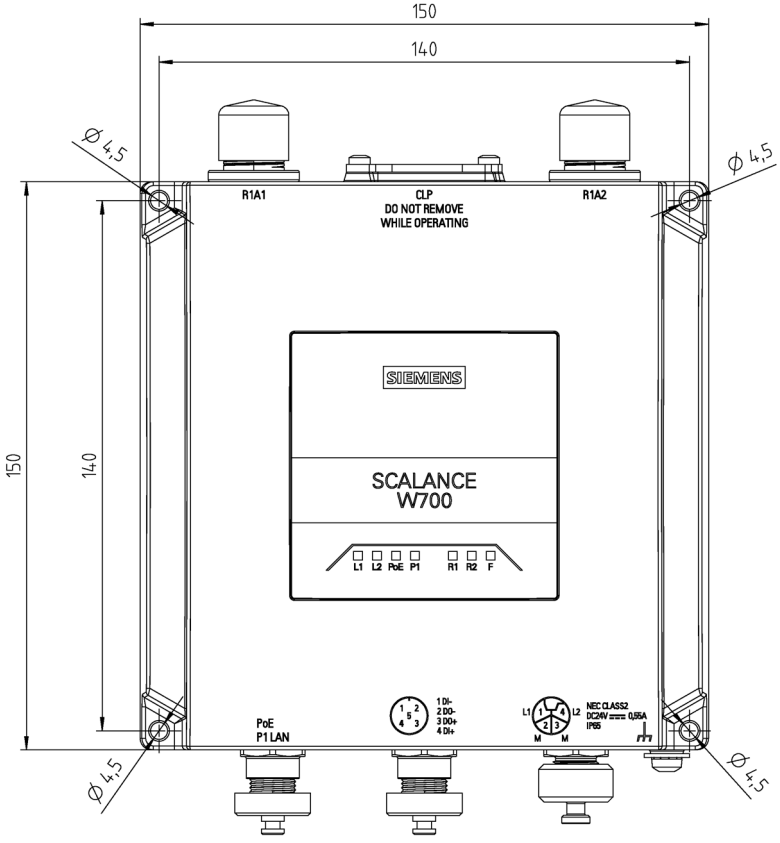
You can find the CAx data on the Internet at (https://www.automation.siemens.com/bilddb/index.aspx?lang=en)

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

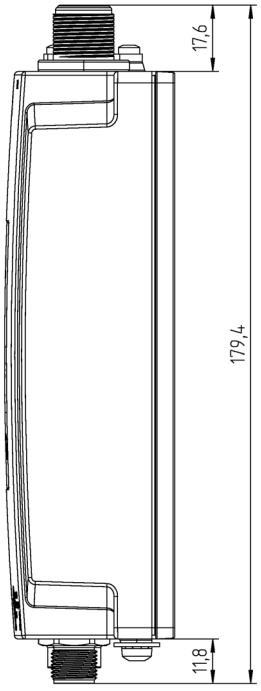
Dimensions are specified in mm.

Front view

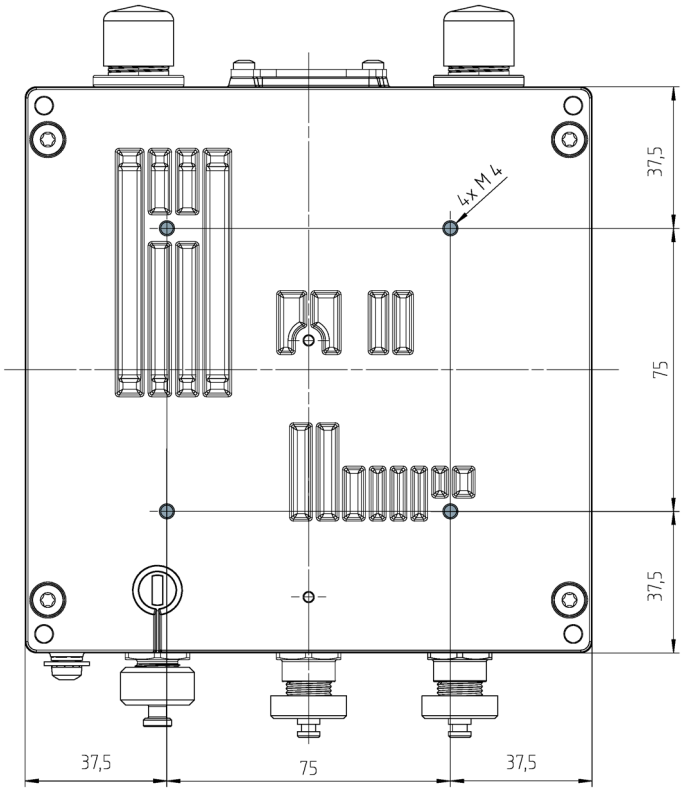


Width, height and dimensions for wall mounting

Side view



Rear view



Rear view with bore holes for VESA bracket 75 x 75, 4x M4, thread depth 8.5 mm

See also

Wall mounting (Page 39)

Mounting on VESA bracket (Page 40)

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:

- Using the search function at Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/)
- Using the search function at Industrial communication (https://support.industry.siemens.com/cs/ww/en/ps/15859/cert)

Enter the entry ID of the relevant manual as the search item.

You will find the documentation for the SIMATIC NET products relevant here on the data storage medium that ships with some products:

- Product CD / product DVD
- SIMATIC NET Manual Collection
- SIMATIC NET IWLAN CD

Index