SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE WxB762

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

05/2025
C79000-G8976-C675-05

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 Aktiengesellschaft. 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 Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: C79000-G8976-C675
Ⓟ 05/2025 Subject to change

Copyright © Siemens 2024 - 2025.
All rights reserved

Table of contents

1 Introduction 5

1.1 Scope of validity 5

1.2 QR code 5

1.3 Supplementary documentation 6

1.4 Further documentation 7

1.5 Service & Support 7

1.6 Training 8

1.7 Cybersecurity information 8

1.8 Firmware 9

1.9 Error/fault 9

1.10 Decommissioning 9

1.11 Recycling and disposal 9

1.12 Marken 9

2 Safety notices 11

3 Security recommendations 13

3.1 Security recommendations 13

3.2 Available services 18

4 Description of the device 21

4.1 Structure of the type designation 21

4.2 Structure of the article number 21

4.3 Device view 22

4.4 Components of the product 22

4.5 Accessories 23

4.5.1 Industrial Ethernet 23

4.5.2 Flexible connecting cables, antennas and accessories 24

4.5.2.1 Flexible connecting cables 24

4.5.2.2 Lightning protection 25

4.5.2.3 Terminating resistor 25

4.5.2.4 Cabinet feedthrough 25

4.5.2.5 Antennas 26

4.6 LED display 27

4.7 Reset button 30

5 Installation and removal 33
5.1 Safety when mounting 33
5.2 Type of mounting 36
5.3 Installing on a DIN rail / removing 37
6 Connection 39
6.1 Safety when connecting 39
6.2 Power supply 44
6.3 Ethernet 45
6.4 Antenna 47
6.5 Grounding 48
7 Maintenance and cleaning 51
8 Troubleshooting 53
8.1 Downloading new firmware using TFTP without WBM and CLI 53
8.2 Restoring the factory settings 53
9 Technical data 55
10 Dimension drawings 57
11 Approvals 59
11.1 General approvals 59
Index 63

Introduction

1

Using the operating instructions, you will be able to install and connect the SCALANCE WxB762-1 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.

1.1 Scope of validity

These operating instructions cover the following products:

Product	Article number	Model
Access points		
SCALANCE WAB762-1	6GK5762-1AJ00-6AA0	ELAX-W1-RJ-E1
Client		
SCALANCE WUB762-1	6GK5762-1AJ00-1AA0	ELAX-W1-RJ-E1
SCALANCE WUB762-1 iFeatures	6GK5762-1AJ00-2AA0	ELAX-W1-RJ-E1

These operating instructions apply to the following firmware version:

- SCALANCE W700 IEEE 802.11ax as of version V3.1

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.

1.2 QR code

Identification Link

There are multiple scannable codes, including a QR code, on the product. The QR code is an Identification Link (ID-Link), a globally unique product identifier according to IEC 61406-1. You can recognize the ID-Link from the frame, which has a black corner at the bottom right.

Disconnect the device from the power and scan the QR code with a smartphone camera, a bar code scanner or a read app. Open the ID-Link. The Siemens web page corresponding to the product opens with the digital nameplate.

In the digital nameplate, you will find product data, manuals, declarations of conformity, certificates, and other helpful information about your product.

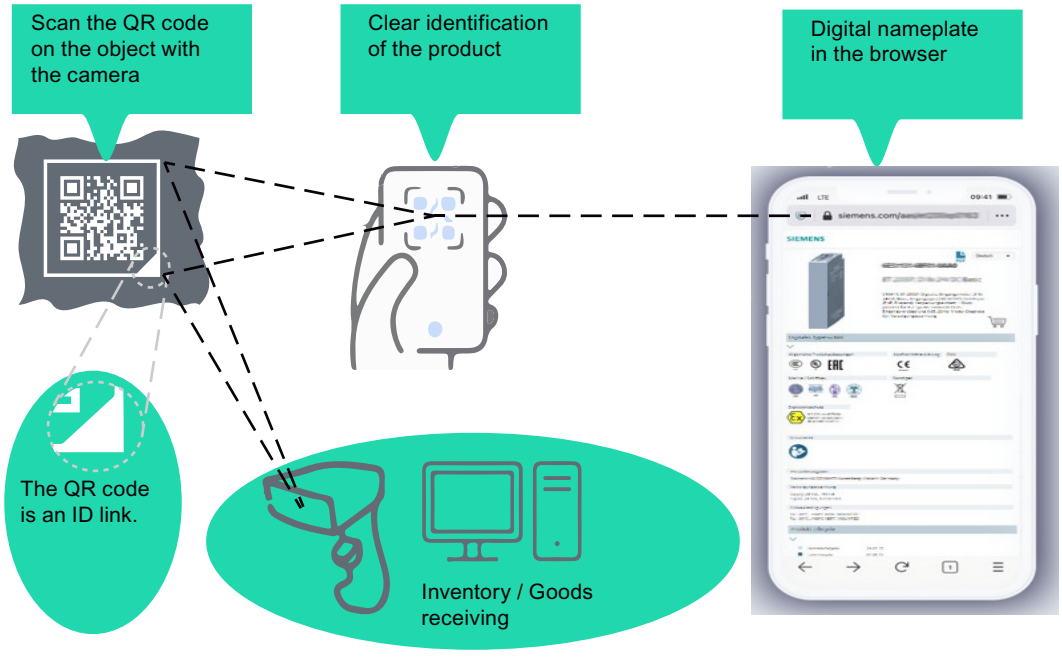


Figure 1-1 Application & functions of the Identification Link

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 according to IEEE 802.11ax Web Based Management
- SCALANCE W700 according to 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 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 Service & Support

Industry Online Support

In addition to the product documentation, you are supported by the comprehensive online information platform of Siemens Industry Online Support at the following Internet address:
Link: (https://support.industry.siemens.com/cs/de/en/)

Apart from news, there you will also find:

- Project information: Manuals, FAQs, downloads, application examples etc.
- Contacts, Technical Forum
- The option submitting a support query:
  Link: (https://support.industry.siemens.com/cs/my?lc=en-WW)
- Our service offer:
  Right across our products and systems, we provide numerous services that support you in every phase of the life of your machine or system - from planning and implementation to commissioning, through to maintenance and modernization.

You will find contact data on the Internet at the following address:
Link: (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en)

1.6 Training

SITRAIN - Training for Industry

The training offer includes more than 300 courses on basic topics, extended knowledge and special knowledge as well as advanced training for individual sectors - available at more than 130 locations. Courses can also be organized individually and held locally at your location.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address:

Link: (https://new.siemens.com/global/en/products/services/industry/sitrain/personal.html)

Industrial Networks Education

Training and certification for Industrial Networks

In our Industrial Networks Education courses you'll learn to design and implement wired and wireless data networks and connect them to a corporate network. You will also receive instruction on how to secure, diagnose and optimize communication networks. Certification can also be offered to supplement almost all training courses.

Link: (https://www.siemens.com/industrial-networks-education)

1.7 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/cybersecurity-industry (https://www.siemens.com/industrialsecurity).

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/cert (https://www.siemens.com/cert).

1.8 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.

1.9 Error/fault

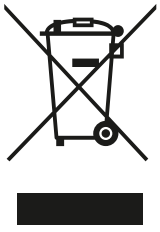
If a fault develops, send the device to your SIEMENS representative for repair. Repairs on-site are not permitted.

1.10 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.

1.11 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.

1.12 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 9)".
- 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 18)".
- 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.
- The names of the configuration files can be changed. To improve security, do not use spaces in the TFTP file name.
- 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
  - DCP
  - NTP
  - Syslog
  - DHCP options 66/67
  - TFTP
  - Telnet
  - HTTP
  - SNMP v1/2c
  - SNTP
  - STP, RSTP and MSTP
- 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
  - NTP → NTPsecure
  - Syslog Client → Syslog Client TLS
- Use secure protocols when access to the device is not secured by physical protection measures.
- If you require non-secure protocols and services, operate them only within a protected network area.
- Select a trusted DNS provider.
- Restrict the services and protocols available to the outside to a minimum.
- With authentication on the RADIUS server and RADIUS client, use the Message Authenticator attribute to check packets.
- If you use RADIUS for management access to the device, enable secure protocols and services.

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	✓	✓	-	-
NTP Client (secure)	UDP/123	Outgoing only	✓	✓	✓	-
Packet Capture	TCP/2002 TCP/2003 [2]	Closed	-	✓	-	-
PROFINET	UDP/34964 UDP/49154 UDP/49155	Open	-	✓	-	-
RADIUS Client	UDP/1812	Outgoing only	✓	✓	✓	-
SFTP Client	TCP/22	Outgoing only	✓	✓	✓	✓
SMTP Client	TCP/25	Outgoing only	✓	✓	-	-
SMTP Client (secure)	TCP/465	Outgoing only	✓	✓	Optional	✓
SNMPv1/v2c [3]	UDP/161	Open	✓	✓	-	-
SNMPv3	UDP/161	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outgoing only	-	✓	-	-

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [1]
			Port	Service		
SNTP Client	UDP/123	Outgoing only	✓	✓	-	-
SSH	TCP/22	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Outgoing only	✓	✓	-	-
Syslog Client TLS	TCP/6514	Outgoing only	✓	✓	-	✓
Telnet	TCP/23	Closed	✓	✓	✓	-
TFTP Client	UDP/69	Outgoing only	✓	✓	-	-
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.

[3] Read Only

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.

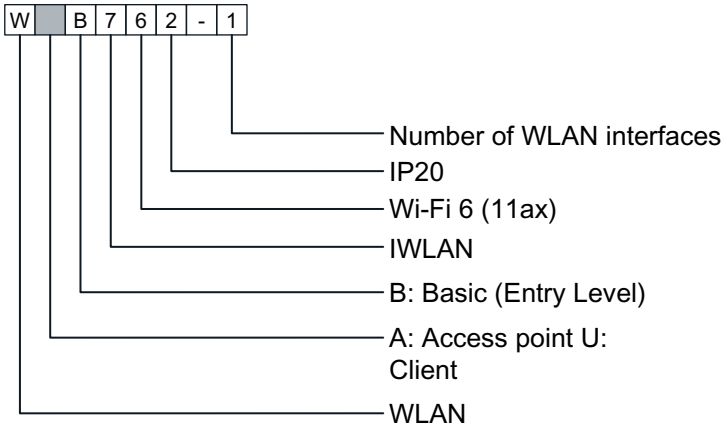
Layer 2 service	Default status	Service configurable
DCP	Open	✓
LLDP	Open	✓
RSTP	Closed	✓
iPRP	Closed	✓
MSTP	Closed	✓
SIMATIC NET TIME	Closed	✓
802.1x	Closed	✓

Description of the device

4

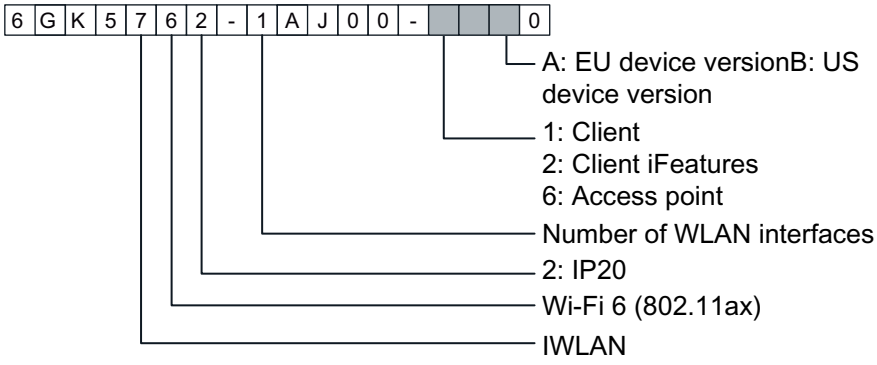
4.1 Structure of the type designation

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

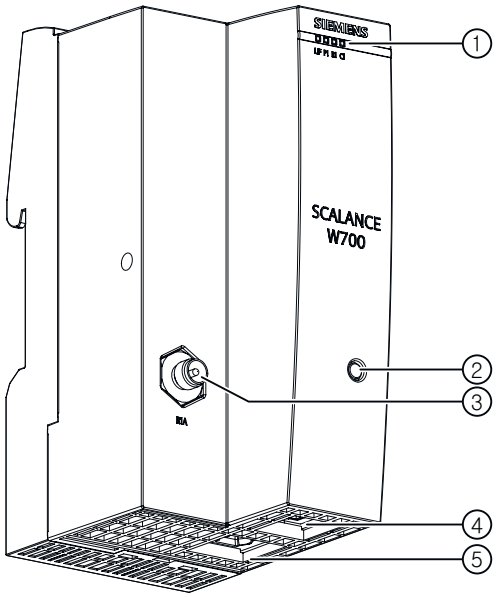


4.2 Structure of the article number

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 LED display
② Reset button
③ Antenna connector, R-SMA type
④ Ethernet connector
⑤ Connector for power supply and grounding

4.4 Components of the product

The following components are supplied with the product:

- One SCALANCE W device
- A cover for the R-SMA connector
- A 3-pin plug-in terminal block for the power supply

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:

- Antennas

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

4.5 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)

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

4.5.1 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

4.5.2 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).

4.5.2.1 Flexible connecting cables

Flexible connecting cable N-Connector/R-SMA

Flexible connecting cable for connecting an antenna to a SCALANCE W device with R-SMA connectors.

Preassembled with one 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

Flexible connecting cable R-SMA/SMA

Flexible connecting cable for connecting an antenna to a SCALANCE W device with R-SMA connectors or to further connecting elements, such as cabinet bushings.

Preassembled with one connector R-SMA/ SMA male/male:

Length	Article number
0.3 m	6XV1875-5DE30
2 m	6XV1875-5DH20

Flexible connecting cable N-Connector/N-Connector

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

4.5.2.2 Lightning protection

Note

Lightning protection elements can be used as bushings.

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

4.5.2.3 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

4.5.2.4 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

4.5.2.5 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/ww/en/ps/28575/man).

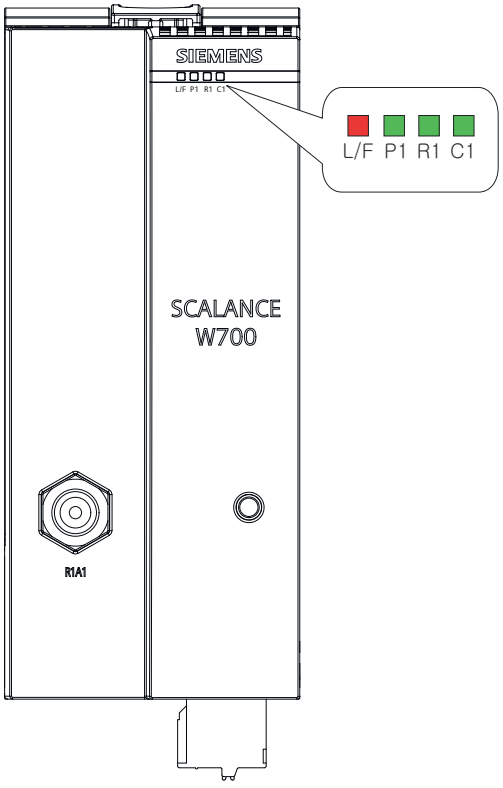
Type	Properties	Article number
ANT792-4DN	RCoax helical antenna, circular polarization, 4 dBi, 2.4 GHz, N-Connect female	6GK5792-4DN00-0AA6
ANT792-6MN	Omnidirectional antenna, mast/wall mounting, 6 dBi 2.4 GHz, N-Connect female	6GK5792-6MN00-0AA6
IWLAN RCoax ANT793-4MN	RCoax λ4 antenna with vertical polarization for RCoax systems, 6 dBi, 5 GHz, IP65, N-Connect female	6GK5793-4MN00-0AA6
ANT793-6DG	Wide angle antenna, 9 dBi, 5 GHz, IP66/67, 2 x N-Connect female, mast/wall mounting	6GK5793-6DG00-0AA0
ANT795-4MA	Omnidirectional antenna, 3/5 dBi, 2.4 GHz and 5 GHz, IP30; RSMA connection, radially rotatable, with additional joint; mounting directly to SCALANCE W with RSMA connection technology	6GK5795-4MA00-0AA3
ANT795-4MB	Omnidirectional antenna, 2/3 dBi, 2.4 GHz and 5 GHz, IP65; RSMA connection, 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, IP68/69K, N-Connect male, mounting directly to SCALANCE devices with N-Connect connection technology; railway approval	6GK5795-4MX00-0AA0
ANT795-6DC	Wide angle antenna, mast/wall mounting, 9 dBi, WLAN 2.4/ 5 GHz and private 5G networks, N-Connector female	6GK5795-6DC00-0AA0
ANT795-6MN	Omnidirectional antenna, mounted on roof/vehicle, 6/8 dBi 2.4 GHz and 5 GHz, N-Connect female	6GK5795-6MN10-0AA6
ANT795-6MP	Omnidirectional antenna, 5/7 dBi, 2.4 GHz and 5 GHz, IP65/67, N-Connect female, mast/wall mounting	6GK5795-6MP00-0AA0
	Omnidirectional antenna 5/8/8 dBi, 2.4 GHz/ 5 GHz/ 6GHz, N-Connect female, IP65/67, mast/wall mounting	6GK5795-6MP10-0AA0

Type	Properties	Article number
ANT897-4ME	Omnidirectional antenna for use in public and private mobile networks and IWLAN networks in indoor and outdoor applications worldwide; 2 ... 6 dBi, 0.6 ... 6 GHz, IP65, N-Connect female	6GK5897-4ME00-0AA0
ANT897-5PN	Omnidirectional antenna with 4 antenna elements for WLAN 2.4/ 5 GHz and private 5G mobile networks; 2.3 ... 7.2 GHz; antenna gain: 4 ... 6 dBi, incl. 4x cable with N-Connect female in staggered lengths 20 ... 27 cm; IP69K; mounting on roof, vehicle and ceiling	6GK5897-5PN00-0AA0
IWLAN RCoax Cable 2,4 GHz PE 1/2"	Omnidirectional antenna, 0 Bi 2.4 -2.485 GHz, N-Connect female	6XV1875-2A
IWLAN RCoax Cable 5 GHz PE 1/2"	Omnidirectional antenna, 0 Bi 5.150 -5.875 GHz, N-Connect female	6XV1875-2D

4.6 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
L/F	Off □	Power supply L too low. No fault/error.
	Green ■	Power supply L is applied. No fault/error.
	Red ■	Possible causes: • The device is booting • An error has occurred • 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 53)".
	Flashing red  Interval: 2000 ms on / 200 ms off	The device is performing a firmware update or downgrade.
	Flashing red  Interval: 1 s on/ 1 s off	The device is starting up for the first time or has been reset to factory settings.
	Red ■ Simultaneous R1 flashing yellow 	A competing radar signal was found on all enabled channels.
P1	Off □	There is no connection over the Ethernet interface P1.
	Green ■	There is a connection over the Ethernet interface P1 (link).
	Flashing green and yellow 	Data transfer over the Ethernet interface P1.

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 competing radar signals before the channel can be used for data traffic.
C1	Off 	The functionality of these LEDs is configurable for different applications. It is disabled by default.
C1 R1	Flashing green 	The port LEDs flash for detection of device location. The "LED flash" function is enabled • Either with SINEC PNI • Or on the WBM page "Discovery and Set via DCP".

Note

Primary user (radar) on all enabled channels (only when DFS is enabled)

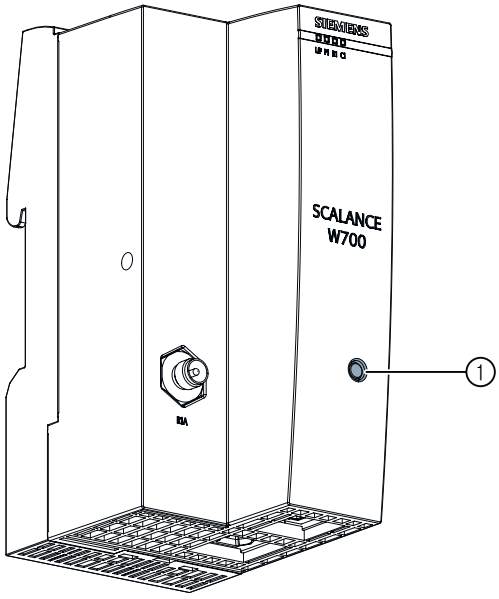
If the device detects competing radar signals on all enabled channels of the WLAN interface, the **L/F** LED is lit and **R1** flashes. No data traffic is then possible for the next 30 minutes. After this time, the device runs the scan again and checks whether a primary user still exists. If no primary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

4.7 Reset button

Position

The Reset button is on the front of the device:



① 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 53)".
- **Resetting the device to factory settings**
  If you reset, all the settings you have made will be overwritten by factory defaults. You can find more detailed information in the section "Restoring the factory settings (Page 53)".

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

Installation and removal

5

5.1 Safety when 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

The device shall only be used in an area with pollution degree 1 or 2 (according to EN/IEC 60664-1, GB/T 16935.1).

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/T 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.

WARNING

The IP20 degree of protection marking is not associated with 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 Type of mounting

The device is designed exclusively for mounting on a 35 mm DIN rail in vertical installation position with vents above and below.

⚠ CAUTION

Danger of injury by falling objects

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

NOTICE

Damage to the device due to exceeding the maximum permissible temperature

When the device is installed, the following minimum clearances must be observed so that the convection cooling of the device is not impaired:

- At least 10 cm clearance under the device
- At least 10 cm clearance above the device
- With ambient temperatures above 40 °C, at least 2 cm clearance to the right of the device (side with nameplate) in addition

Note

To protect the device against overheating, the maximum data throughput of the radio interface is reduced with increasing ambient temperature.

- Always ensure best possible cooling of the device.

You can find information about the ambient temperature under Permissible ambient conditions (Page 55).

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

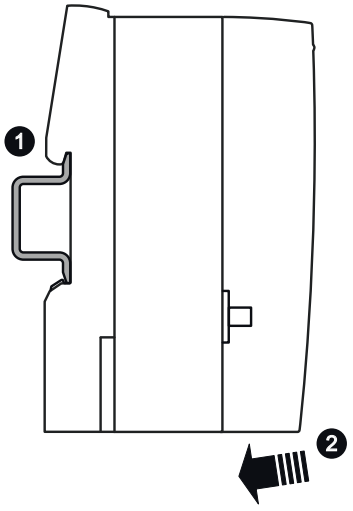
If cables are installed permanently, it is advisable to remove the insulation of the shielded cable and to establish contact on the shield/PE conductor bar.

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 Installing on a DIN rail / removing

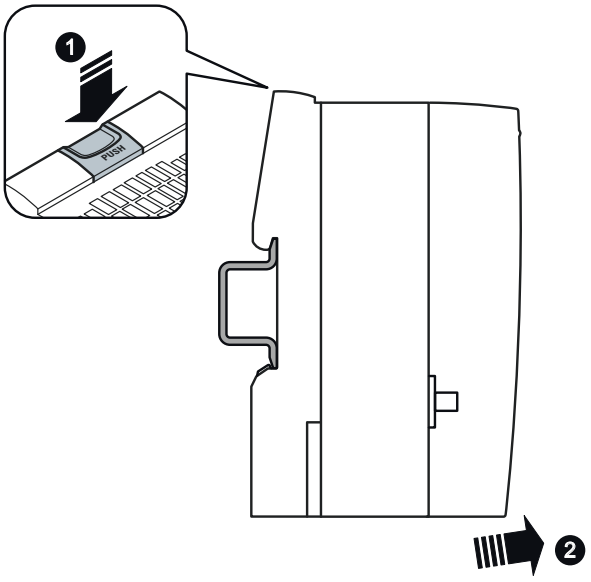
Procedure for installation



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

1. Place the device on the upper edge of the DIN rail as shown in the figure.
2. Press the device against the DIN rail until the DIN rail slider catch locks in place.
3. Mount the connecting cables and the antenna, see section "Connecting up (Page 39)".

Procedure when removing



Follow the steps below to uninstall the device:

1. Turn off the power to the device.
2. Disconnect all connected cables.
3. Press the release button on the top of the device to release the DIN rail catch.
4. Tilt the device forward and remove the device from the DIN rail.

Connection

6

6.1 Safety when connecting

Safety notices

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

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 25) 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

⚠ 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 that is connected to the supply connections therefore needs to meet at least one of the following conditions:

- Safety extra low voltage (SELV) with limited power source (LPS) complying with UL 60950-1 / IEC 60950-1 / EN 60950-1
  or
- Safety extra low voltage (SELV) with limited power source (LPS) complying with UL 62368-1 / IEC 62368-1 / EN IEC 62368-1
  or
- NEC Class 2 according to the National Electrical Code (r) (ANSI / NFPA 70)

If the device is connected to a redundant power supply (two separate power supplies), the combination of the two power supplies 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 surges of more than 40% of the rated voltage. Under no circumstances may transient surges exceed 119 V. This is the case if you only operate devices with SELV (safety 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 housing must comply with the IP degree of protection required by EN IEC / IEC 60079-0, GB/T 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.

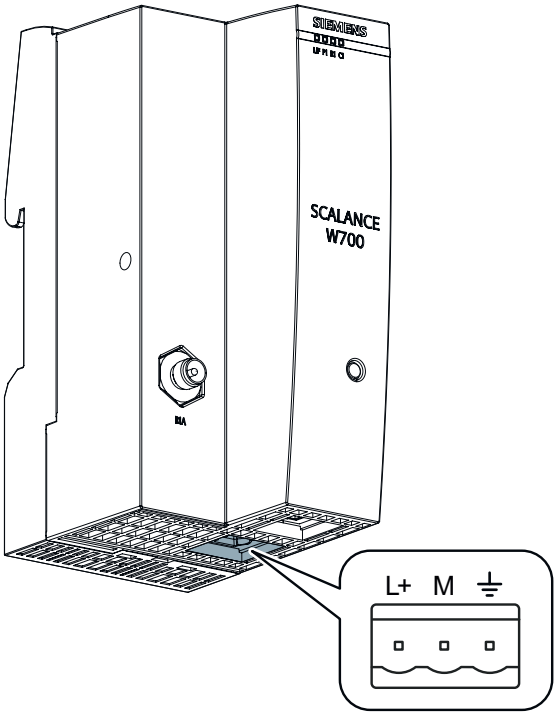
NOTICE
The "Limited Energy" circuit and other circuits must be separated by at least basic insulation.

NOTICE
The permissible non-hazardous voltages are SELV 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.

The power supply is connected using a 3-pin plug-in terminal block. The power supply is non-floating.



Contact	Assignment
L+	24 V DC
M	Ground
⏚	Functional grounding, refer to the section "Grounding (Page 48)"

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

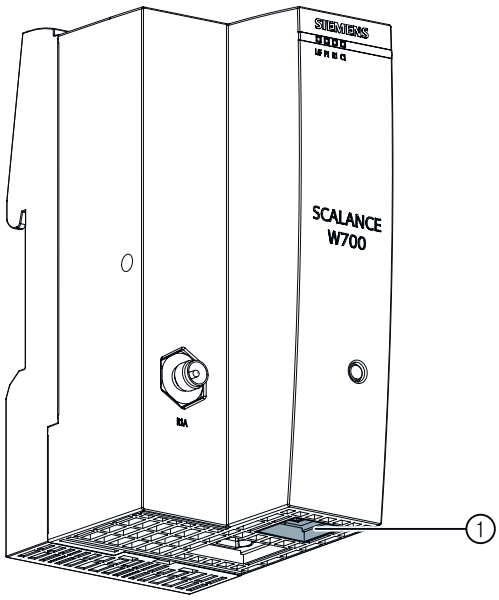
The "L/F" LED indicates whether a power supply is connected; see section "LED display (Page 27)".

6.3 Ethernet

The device has an Ethernet interface located on the underside 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.



① Ethernet interface, P1

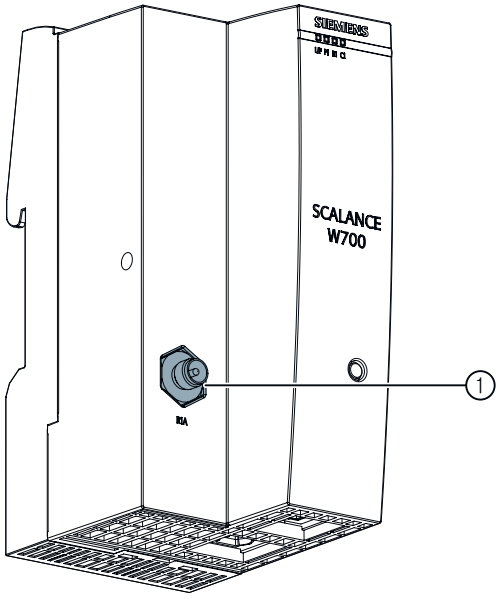
Pin assignment

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

Pin number	Pin assignment	RJ45 connector
	10/100/1000 Mbps	
Pin 1	D1+	 87654321
Pin 2	D1-	
Pin 3	D2+	
Pin 4	D3+	
Pin 5	D3-	
Pin 6	D2-	
Pin 7	D4+	
Pin 8	D4-	

6.4 Antenna

The device has an antenna connector R1 A1 of the type R-SMA located on the front of the device.



① Antenna connector R1 A1

Procedure

To connect a cable for an external antenna to the device, insert the connector of the antenna cable into the R-SMA socket R1 A1 ① and screw the screw cap of the connector onto the socket (key size SW8, tightening torque 1 Nm).

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.

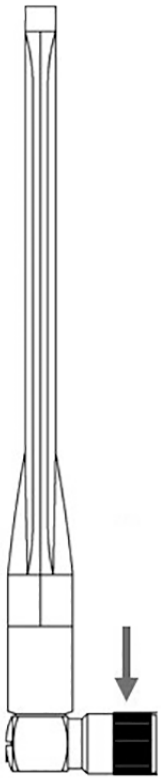


Figure 6-1 Figure of the ANT795-4MA; the arrow points to the screw cap.

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 a detached antenna. Suitable flexible connecting cables 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 24)".

6.5 Grounding

Functional grounding must be established from the 3-pin terminal block to the DIN rail; refer to section "Device view (Page 22)" or section "Power supply (Page 44)". The terminal is identified by the symbol for the functional ground ⏚.

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 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.

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.
- For function checks, maintenance and servicing work, you need to observe the requirements on checking and maintaining plants in hazardous areas according to the standards EN / IEC 60079-17.

⚠ 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 30)".

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

1. Turn off the power to the device.
2. Press and hold down the reset button.
3. Connect the device to the power supply again while holding down the button.
4. Hold down the button until the red "L/F" LED starts to flash after approximately 2 seconds (500 ms on/500 ms off).
5. Release the button. The "L/F" LED lights up red permanently.
   The bootloader waits in this state for a new firmware file that you can download using TFTP.
6. Connect a PC to the device over the Ethernet interface.
7. Assign an IP address to the device using DHCP or the SINEC PNI.
8. 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.

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 30)".

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. Press the reset button and reconnect the device to the power supply while holding down the button.
3. Hold down the button until the red "L/F" LED stops flashing after approximately 10 seconds and is permanently lit.
4. Release the button and wait until the "L/F" LED goes out.
   The device starts automatically with the factory settings.

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 "Restore Factory Defaults" 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 WAB762-1 (model ELAX-W1-RJ-E1)
- SCALANCE WUB762-1 iFeatures (model ELAX-W1-RJ-E1)

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/ww/en/ps/28575/man).

Technical specifications		
Data transfer		
Ethernet transfer rate		10 / 100 /1000 Mbps
Wireless transfer rate		1 ... 600.5 Mbps
Wireless standards supported		IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax
Connection to Industrial Ethernet		
	Quantity	1
	Design	RJ45 socket
	Properties	Half duplex/full duplex, autocrossover, auto-negotiation, 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
Radio interface		
Antenna port	Quantity	1
	Design	R-SMA female
	Impedance	50 Ω nominal

Technical specifications		
Frequency range [1]	Center frequency	2412 ... 2472 MHz 4920 ... 5865 MHz
Max. conducted power		20 dBm
Electrical data		
Direct 24 V DC supply	Supply voltage from socket	24 V DC Safety Extra Low Voltage (SELV)
	Type of current	⎓
	Permissible range ±20%	19.2 to 28.8 V DC
	Design	Terminal block, 3-pin
	Properties	Not galvanically isolated The connected power supply must meet the requirements of NEC Class 2.
Current consumption	24 V DC supply, max. (reached at 19.2V)	400 mA
Active power loss	24 V DC supply, maximum	8 W
Permissible ambient conditions		
Ambient temperature	During operation with the vertical installation position	0 °C to +40 °C
	During operation with the vertical installation position with 2 cm clearance on the right	0 °C to +55 °C
	During storage	-40 °C to +85 °C
	During transportation	-40 °C to +85 °C
Relative humidity	During operation	≤ 95% at 25 °C, no condensation
Operating altitude	During operation	≤ 2,000 m above sea level at max. 55 °C ambient temperature
Contaminant concentration		According to IEC 60721
Degree of pollution		2
Degree of protection		IP20
Dimensions and weight		
Dimensions	W x H x D	50 x 114 x 74 mm
Weight		145 g
Installation options		
	Mounting on a DIN rail	
Mean time between failure (MTBF)		
	at 40 °C ambient temperature	32 years

[1] Observe the country-specific restrictions. You can find more information on currently available country approvals in the "Approvals SCALANCE W700 802.11ax" document on the Internet under (https://support.industry.siemens.com/cs/ww/en/ps/28575/man).

Dimension drawings

10

Note

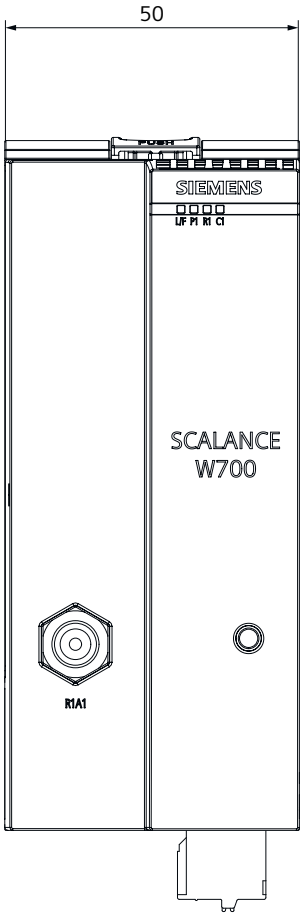
CAx data

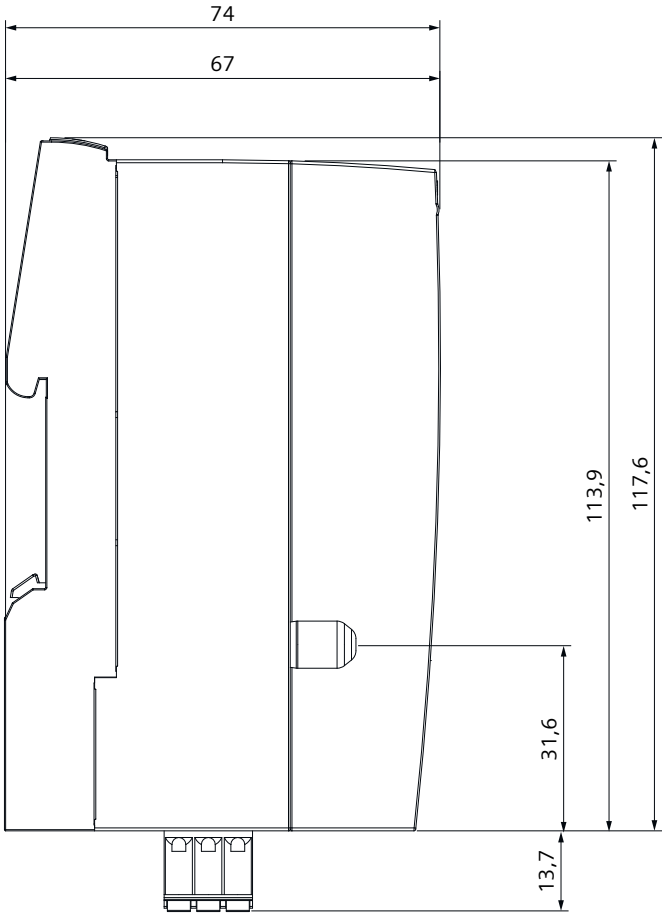
You can find the CAx data on the Internet at (https://www.automation.siemens.com/bilddb/index.aspx?lang=en)

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

The dimensions are specified in mm.





Approvals

11

Note

Issued approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

You will find the country-specific 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/ps/28575/man)

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.

11.1 General approvals

ATEX, IECEx, UKEX and CCC Ex certification

⚠ WARNING

Risk of explosion in hazardous areas

When using SIMATIC NET products in hazardous area zone 2, make absolutely sure that the associated conditions in the following document are adhered to:

"SIMATIC NET Product Information Use of subassemblies/modules in a Zone 2 Hazardous Area".

You will find this document

- on the Internet pages under Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/78381013).

The markings of the electrical devices are:



II 3G Ex ec IIC T4 Gc
DEKRA 18ATEX0026 X
IECEx DEK 18.0018X



II 3G Ex ec IIC T4 Gc
DEKRA 21UKEX0002 X

Importer UK:
Siemens plc,
Manchester, M20 2UR, UK



(Ex ec IIC T4 Gc, not on the nameplate)

The product meets the requirements of the standards:

- EN IEC/IEC 60079-0, GB/T 3836.1
- EN/IEC 60079-7, GB/T 3836.3

You will find the current versions of the standards in the currently valid certificates.

FM



The product meets the requirements of the standards:

- FM Class 3600, FM Class 3611, FM Class 3810
- ANSI/UL 121201, ANSI/UL 61010-1
- FM Hazardous (Classified) Location Electrical Equipment:
  Non Incendive / Class I / Division 2 / Groups A,B,C,D / T4 and
  Non Incendive / Class I / Zone 2 / Group IIC / T4

You can find the temperature class on the nameplate of the product. The permissible temperature range of the product is 0 °C to +55 °C.

cULus Approval for Information Technology Equipment



cULus Listed I. T. E.

Underwriters Laboratories Inc. complying with

- UL 62368-1
- CSA C22.2 No. 62368-1

Report no. E115352

cULus approval for industrial control equipment



cULus Listed PROG-CNTLR.

Underwriters Laboratories Inc. complying with

- UL 61010-1
- UL 61010-2-201
- CSA C22.2 NO 61010-1
- CSA C22.2 NO 61010-2-201

Report no. E85972

cULus Approval Hazardous Location



cULus Listed I. T. E. FOR HAZ. LOC.

Underwriters Laboratories Inc. complying with

- UL 121201
- CSA C22.2 No. 213

Approved for use in
Cl. 1, Div. 2, GP A, B, C, D T4
Cl. 1, Zone 2, GP IIC T4

Report no. E240480

Index

A

Accessories, 23
Antenna, 47
Antenna cables, 24
Antennas, 24
Article number, 5
    Structure, 21

B

Button, 30

C

CAx data, 57
Configuration manuals, 6, 54
Connecting
    Antenna, 47
    Ethernet, 45
    Grounding, 48
    Power supply, 44

D

Dimension drawing, 57
Documentation on the Internet, 6

E

Ethernet, 45

F

Factory defaults, 53
Factory setting, 53

G

Grounding, 40, 48

I

Installation
    DIN rail, 37
Interfaces, 55, 56

L

LED display, 27
Lightning protection, 39

M

Model, 5

P

Pin assignment, 46
Power supply, 44
Primary user (radar), 27

R

Reset button, 30
Reset device, 53

S

Safety notices
    for installation, 33
    general, 11
    Use in hazardous areas, 11, 33, 39
    when connecting up, 39
Scope of delivery, 22
Scope of validity, 5
System manual, 7

T

Technical specifications, 55, 56
Type designation, 21