SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE W760 / W720

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

10/2025
C79000-G8976-C322-15

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 persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the application described in the catalog and the associated usage information. 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-C322
Ⓟ 10/2025 Subject to change

Copyright © Siemens 2014 - 2025.
All rights reserved

Table of contents

1 Introduction 5

1.1 Purpose of the operating instructions 5

1.2 Scope of validity 5

1.3 Supplementary documentation 5

1.4 Service & Support 6

1.5 Cybersecurity information 7

1.6 Firmware 7

1.7 Open source license conditions 8

1.8 Error/fault 8

1.9 Decommissioning 8

1.10 Recycling and disposal 8

1.11 Marken 8

2 Safety notices 9

3 Security recommendations 11

3.1 Security recommendations 11

3.2 Available interfaces 17

3.3 Available services 18

4 Description of the device 21

4.1 Structure of the type designation 21

4.2 Device view 21

4.3 Components of the product 22

4.4 Accessories 22

4.4.1 Industrial Ethernet 22

4.4.2 Flexible connecting cables and antennas 23

4.4.2.1 Flexible connecting cables 23

4.4.2.2 Lightning protection 24

4.4.2.3 Terminating resistor 25

4.4.2.4 Cabinet feedthrough 25

4.4.2.5 Antennas 25

4.5 LED display 28

4.6 Reset button 31

5 Installation and removal 33

5.1 Safety notices for installation 33

5.2 Installing on a DIN rail / removing ... 36
6 Connection ... 39
6.1 Safety when connecting up ... 39
6.2 Power supply ... 43
6.3 Ethernet ... 44
6.4 Antenna connector ... 46
6.5 Grounding ... 47
7 Maintenance and cleaning ... 49
8 Troubleshooting ... 51
8.1 Downloading new firmware using TFTP without WBM and CLI ... 51
8.2 Restoring the factory settings ... 51
9 Technical data ... 53
10 Dimension drawings ... 55
11 Approvals ... 57
Index ... 59

Introduction

1

1.1 Purpose of the operating instructions

Based on the operating instructions, you will be able to install and connect the SCALANCE device correctly. The instructions are aimed primarily at planning, commissioning, maintenance and service personnel.

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

1.2 Scope of validity

These operating instructions cover the following products:

Product	Article numbers	Certification ID
Access point		
SCALANCE W761-1 RJ45	6GK5761-1FC00-0AA0 6GK5761-1FC00-0AB0 (US)	ELN-W1-RJ-E1
Ethernet client modules		
SCALANCE W722-1 RJ45 (iFeatures)	6GK5722-1FC00-0AA0 6GK5722-1FC00-0AB0 (US) 6GK5722-1FC00-0AC0 (ME)	ELN-W1-RJ-E1
SCALANCE W721-1 RJ45	6GK5721-1FC00-0AA0 6GK5721-1FC00-0AB0 (US)	ELN-W1-RJ-E1

These operating instructions apply to the following firmware version:

- SCALANCE W700 IEEE 802.11n Firmware as of version V6.6

Definition

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

1.3 Supplementary documentation

Documentation on the Internet

You can find the current version of the documents on the Internet at (https://sieportal.siemens.com/su/bjSDr).

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

Documentation on configuration

You will find detailed information on configuring the devices in the following configuration manuals:

- SCALANCE W700 nach IEEE 802.11n Web Based Management
- SCALANCE W700 nach IEEE 802.11n Command Line Interface

1.4 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)

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)

1.5 Cybersecurity information

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

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

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/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).

1.6 Firmware

You can find the firmware on the Internet under: (https://support.industry.siemens.com/cs/de/en/ps/15860/dl)

Firmware

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

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.

Update files

You will find a SHA256 hash value in the update file. With this, you can check whether the file was downloaded unchanged. To check this, you calculate the hash value of the downloaded file and compare it with the value specified on the download page.

1.7 Open source license conditions

Note

Open source software

Read the license conditions for open source software carefully before using the product.

The license terms and copyright information can be downloaded from the WBM or CLI as a zip file.

- WBM: System > Load&Save > HTTP / TFTP / SFTP > LicenseCondition
- CLI: `sftp save filetype LicenseConditions / tftp save filetype LicenseConditions`

1.8 Error/fault

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

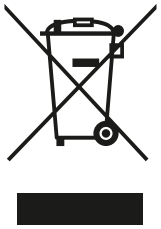
1.9 Decommissioning

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

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

Also restore the factory settings on the storage medium.

1.10 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.

1.11 Marken

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

SCALANCE, C-PLUG, 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.
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.
  Download (https://sieportal.siemens.com/su/blCGg)
  Check regularly for new features on the Siemens Internet pages.
  - You can find information on Industrial Security here:
    Link: (https://www.siemens.com/industrialsecurity)
  - You can find a selection of documents on the topic of network security here:
    Link: (https://support.industry.siemens.com/cs/ww/en/view/92651441)

  If Siemens detects and resolves security incidents in the products, this is published in Security Advisories. You will find the documents for the device on the Internet under: (https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications)

WLAN

- A WLAN interface can only be used within private networks by authorized users and devices.
- No authentication or data encryption is required in an open WLAN system ("Open System Authentication"). Therefore, it cannot be used in productive operation for security reasons. Use of the "Open System" authentication type is only permissible during initial setup and for test purposes.
- 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 and encryption of WLAN with WEP (Wired Equivalent Privacy) is not considered secure and is not recommended.

Authentication and users

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. Create a separate user account for each user that will receive access to the device.
- Define rules for the assignment of passwords. Follow current recommendations on defining strong passwords, e.g. by the German Federal Office for Information Security.
  Link (https://www.bsi.bund.de)
- 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. You can use password managers or encrypted files/drives for this purpose.
- A password must be changed if it is known or suspected to be known by unauthorized persons.

- When 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 in the WBM via "System > Load & Save".
- Use the certification authority including key revocation and management to sign the certificates.
- Use password-protected certificates in the format "PKCS #12".
- 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.
- Verify certificates based on the fingerprint on the server side 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, reset it to factory settings and replace the current certificates and keys with temporary throwaway certificates and keys that can be destroyed when the device is returned.
- The device does not perform a check for revoked certificates during certificate-based communication.
  Recommended measures:
  - Use certificates with a short lease time
    OR
  - Ensure prompt replacement of revoked certificates

  For OpenVPN communication, you can use automated certificate distribution in SINEMA RC.
- For the device to be able to correctly check digital certificates and establish secure connections, the system time always needs to be up to date. Follow the steps outlined below:
  Check and set time
  Check whether the time is set correctly on the device, especially after a reset to factory settings or a long power supply interruption.
  Enable time-of-day synchronization (recommended)
  Activate one of the supported synchronization methods.
  Make sure that there is a stable connection to the synchronization partner so that the device can regularly receive the current time.

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 8)".
- 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.
  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.
- Files (e.g. configuration files) can be downloaded from the device. Ensure that the files are adequately protected. The options for achieving this include storing the files in a secure location and transmitting them only through secure communication channels.
  In addition, you can create hash sums from the files after the download. This allows you to check that the file is unchanged before further use.
- Configuration files can be password-protected during download. You enter passwords on the WBM page "System > Load & Save > Passwords".
- 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 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, 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.

- The following protocols and services can only be used in physically separate networks:
  - Non-authenticated and unencrypted ports
  - DCP
  - DHCP
  - DNS client
  - HTTP
  - IEEE 802.1x (RADIUS)
  - iPRP
  - iPCF
  - iPCF-MC
  - LLDP
  - NTP client
  - ICMP
  - PROFINET
  - Remote Packet Capture
  - SIMATIC NET Time
  - SMTP client
  - SNMP v1/2c
  - SNMP traps
  - SNTP client
  - STP, RSTP and MSTP
  - Syslog client
  - TCP event
  - Telnet
  - TFTP

- 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
  - NTP → NTPsecure
  - TFTP → SFTP
  - 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.
- The LAN interface of the product must not be operated in unprotected or untrusted networks (e.g. the Internet) without additional upstream protective devices.
- Only operate Syslog, SNTP and other non-secure protocols over secure connections (e.g. SINEMA RC/OpenVPN).

3.2 Available interfaces

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

Interface	Default status	Change to the status	
		WBM / CLI (administrator)	Physical
LAN	Enabled	✓	-
WLAN	Disabled	✓	-
Digital input [1)]	Disabled	-	✓

Interface	Default status	Change to the status	
		WBM / CLI (administrator)	Physical
Digital output [1]	Disabled	✓	✓
PLUG slot [2]	Enabled	✓	✓

1) Only with SCALANCE W788/W748

2) Not with SCALANCE W760/W720

3.3 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
- **Default port status**
  This is the status of the port in the delivery state (factory setting).
- **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	Disabled Only outgoing	--	✓	--	--
DHCP Client IPv6	UDP/546	Disabled Only outgoing	--	✓	--	--
DHCP Server	UDP/67	Closed	--	✓	--	--
DNS Client	TCP/53 UDP/53	Active Only outgoing	--	✓	--	--
EthernetIP	TCP/44818 UDP/2222 UDP/44818	Closed	--	✓	--	--
HTTP	TCP/80	Disabled [4]	✓	✓	✓	--
HTTPS	TCP/443	Active	✓	✓	✓	✓

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [1]
			Port	Service		
NTP Client	UDP/123	Disabled Only outgoing	✓	✓	-	-
NTP Client (secure)	UDP/123	Disabled Only outgoing	✓	✓	✓	-
Packet Capture	TCP/2002 TCP/2003 [2]	Disabled	-	✓	-	-
Ping	ICMP	Active	-	-	-	-
PROFINET	UDP/34964 UDP/49154 UDP/49155	Disabled	-	✓	-	-
RADIUS Client	UDP/1812	Disabled Only outgoing	✓	✓	✓	-
SFTP Client	TCP/22	Active Only outgoing	✓	✓	✓	✓
SMTP Client	TCP/25	Disabled Only outgoing	✓	✓	-	-
SMTP Client (secure)	TCP/465	Disabled Only outgoing	✓	✓	Optional	✓
SNMPv1/v2c [3]	UDP/161	Disabled	✓	✓	-	-
SNMPv3	UDP/161	Disabled	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Disabled Only outgoing	-	✓	-	-
SNTP Client	UDP/123	Disabled Only outgoing	✓	✓	-	-
SSH	TCP/22	Active	✓	✓	✓	✓
Syslog Client	UDP/514	Disabled Only outgoing	✓	✓	-	-
Syslog Client TLS	TCP/6514	Disabled Only outgoing	✓	✓	-	✓
Telnet	TCP/23	Disabled	✓	✓	✓	-
TFTP Client	UDP/69	Disabled Only outgoing	✓	✓	-	-

[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

[4] The HTTP port is always open. If the service is disabled, automatic HTTP forwarding to the HTTPS port takes place.

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.

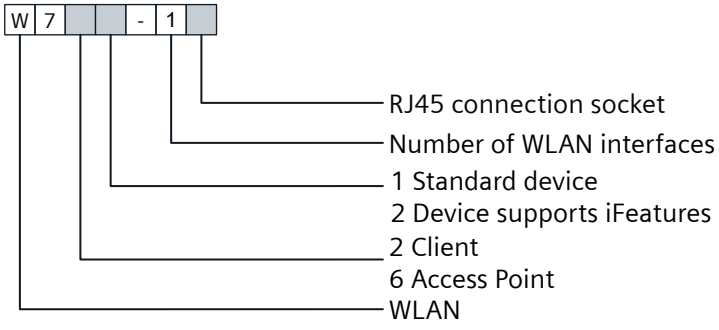
Layer 2 service	Default setting of service	Service configurable	Encryption
DCP	Active	✓	-
ICMP	Active	-	-
iPCF	Disabled	✓	-
iPCF-MC	Disabled	✓	-
iPRP	Disabled	✓	-
LLDP	Active	✓	-
MSTP	Disabled	✓	-
RSTP	Disabled	✓	-
SIMATIC NET TIME	Disabled	✓	-
802.1n	Disabled	✓	Optional

Description of the device

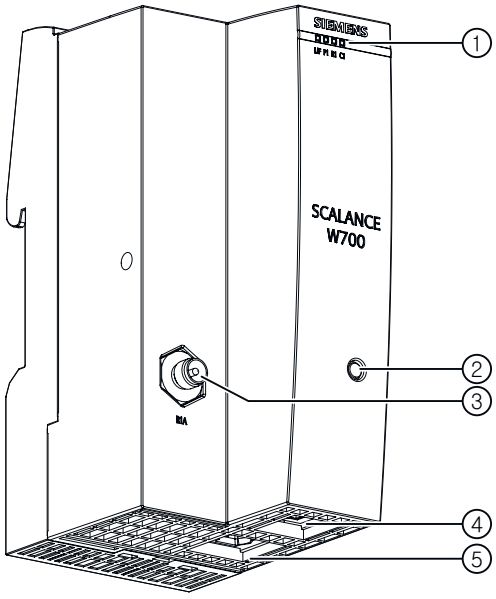
4

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 Device view



① LED display
② Reset button
③ Antenna connector, R-SMA type
④ Ethernet connector
⑤ Connector for power supply and grounding

4.3 Components of the product

The following components are supplied with the product:

- One SCALANCE device
- One protective cap for the antenna socket
- A 3-pin terminal block for the power supply
- One product DVD

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

4.4 Accessories

Note on 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.

4.4.1 Industrial Ethernet

Cables Industrial Ethernet

Component	Description	Article number
IE FC TP STANDARD CABLE GP2X2 (PROFINET type A)	Standard bus cable, TP installation cable for connection to FC OUTLET RJ-45, for universal use, 4-wire, shielded, CAT 5E Sold by the meter	6XV1840-2AH10
IE FC TP ROBUST STANDARD CABLE GP 2X2 (PROFINET type A)	Standard bus cable, ATPE outer jacket for connection to FC RJ-45 PLUG and FC OUTLET RJ-45, fixed installation, for universal use, 4-wire, shielded, CAT 5 Sold by the meter	6XV1841-2A
IE FC TP ROBUST FLEXIBLE CABLE GP 2X2 (PROFINET type B)	Flexible bus cable, TPE outer jacket for connection to FC RJ-45 PLUG and FC OUTLET RJ-45, flexible wires, 4-wire, shielded, CAT 5 Sold by the meter	6XV1841-2B
IE FC TP FLEXIBLE CABLE GP 2X2 (PROFINET type B)	Flexible bus cable, TP installation cable, flexible wires, shielded, CAT 5 Sold by the meter	6XV1870-2B

Component	Description	Article number
IE FC TP TRAILING CABLE 2X2 (PROFINET type C)	Highly flexible bus cable, TP installation cable for connection to FC OUTLET RJ-45, for use in drag chains, 4-wire, shielded, CAT 5 Sold by the meter	6XV1840-3AH10
IE TP TORSION CABLE 2X2 (PROFINET type C)	Highly flexible bus cable, TP installation cable for use in highly flexible applications (torsion), 4-wire Sold by the meter	6XV1870-2F
IE CONNECTING CABLE M12-180/IE RJ45	Flexible IE connecting cable, 4-wire, preassembled with a 4-pin M12 plug (D-coded) and an IE FC RJ-45 plug 145	6XV1871-5T*
IE CONNECTING CABLE M12-180/M12-180	Flexible IE connecting cable, 4-wire, preassembled with two 4-pin M12 plugs (D-coded)	6XV1870-8A*

* Available in different lengths

4.4.2 Flexible connecting cables and antennas

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).

4.4.2.1 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 an N-Connect male and an R-SMA male connector:

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 to the flexible connecting cables; preassembled with one QMA male and one N-Connect female connector; scope of delivery 3 units:

Length	Article number
1 m	6XV1875-5JH10

For railway applications, the following connecting cable is available, scope of delivery 1 unit:

Length	Article number
1 m	6XV1875-5VH10

4.4.2.2 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

4.4.2.3 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

4.4.2.4 Cabinet feedthrough

Component	Description	Article number
IE M12 Panel Feedthrough	Cabinet feedthrough for conversion from M12 connector technology (D-coded, IP65) to RJ-45 connector technology (IP20) pack of 5	6GK1901-0DM20-2AA5
IE M12 Panel Feedthrough PRO	Cabinet feedthrough for conversion from M12 connector technology (D-coded, IP65) to M12 connector technology (D-coded, IP65) pack of 5	6GK1901-0DM30-2AA5
IE M12 Panel Feedthrough 4X2	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-Connect female/ female Panel Feedthrough	Panel feedthrough for wall thicknesses up to a maximum of 5.5 mm, two N-Connect/SMA female connectors.	6GK5798-0PT00-2AA6

4.4.2.5 Antennas

Note

When you select an antenna, keep in mind the national approvals for your device.

You will find more detailed information in Link (http://www.siemens.com/wireless-approvals).

The SCALANCE W1788-2IA uses internal omni antennas (3/4 dBi at 2.4 GHz or 5 GHz).

Type	Properties	Article number
IWLAN RCoax ANT792-4DN	RCoax helical antenna with circular polarization for RCoax systems, 4 Bi, 2.4 GHz, IP65, N-Connector female.	6GK5792-4DN00-0AA6
ANT792-6MN	Omnidirectional antenna, mast/wall mounting, 6 dBi 2.4 GHz, IP67, N-Connect female	6GK5792-6MN00-0AA6

Type	Properties	Article number
ANT792-8DN	Directional antenna, mast/wall mounting, 14 dBi 2.4 GHz, IP32, N-Connect female	6GK5792-8DN00-0AA6
ANT793-6DG	Wide angle antenna, mast/wall mounting, 9 dBi 5 GHz, IP66/67, 2 x N-Connect female	6GK5793-6DG00-0AA0
ANT793-8DJ	Directional antenna, mast/wall mounting, 18 dBi 5 GHz, IP67, 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
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 This antenna is not available in Korea	6GK5793-8DP00-0AA0
IWLAN RCoax ANT793-4MN	RCoax λ4 antenna with vertical polarization for RCoax systems, 6 dBi, 5 GHz, IP65, N-Connector female	6GK5793-4MN00-0AA6
ANT795-4MA	Omnidirectional antenna, directly on the device, 3/5 dBi 2.4 GHz and 5 GHz, IP30, R-SMA connector male for direct installation on the device, angle connector adjustable 0° - 180°.	6GK5795-4MA00-0AA3
ANT795-4MB	Omnidirectional antenna, 2/3 dBi 2.4 GHz and 5 GHz, IP30, R-SMA connector female for direct mounting on the device, angle connector adjustable 0° to 90°	6GK5795-4MB00-0Ax0
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
ANT795-4MX	Omnidirectional antenna, 2/2.5 dBi, 2.4 GHz and 5 GHz, IP69K, N-Connector male	6GK5795-4MX00-0AA0
ANT795-6DC	Wide angle antenna, mast/wall mounting, 9 dBi 2.4 GHz and 5 GHz, N-Connect 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
ANT795-6MT	Omnidirectional antenna (MIMO), mounted on roof/vehicle/ceiling, 5/7 dBi 2.4 GHz and 5 GHz, 3 x QMA connector female	6GK5795-6MT00-0AA0
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"	Omnidirectional antenna, 0 Bi 2.400 -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

NOTICE
ANT795-4MA The ANT795-4MA antenna has degree of protection IP30 and is therefore only suitable for dry environments.

Note

ANT793-8DJ

The antenna ANT793-8DJ may only be used with the flexible connecting cable 6XV1875-5CH50 (5 m length) or 6XV1875-5CN10 (10 m length). Other flexible connecting cables are not permitted.

Notice for USA/Canada

Only one antenna per device can be used (connected to R1A1, R1A2 or R2A1, R2A2).

Note

ANT793-8DK

The antenna ANT793-8DK may only be used with the flexible connecting cable 6XV1875-5CN10 (10 m length). Other flexible connecting cables are not permitted.

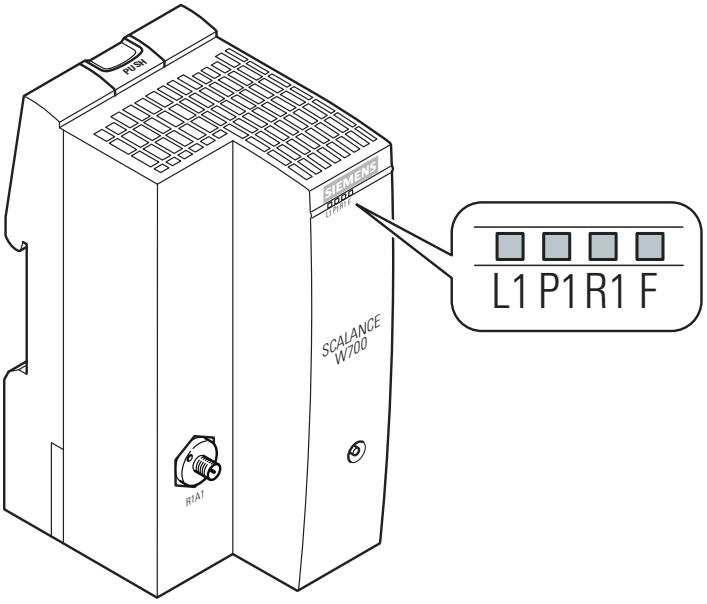
Notice for USA/Canada

Only one antenna per device can be used (connected to R1A1, R1A2 or R2A1, R2A2).

4.5 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.
P1	Off □	There is no connection over the Ethernet port P1.
	Green ■	There is a connection over the Ethernet port 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 via 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. *Client mode:* The client waits for the MAC address due to the setting "Automatic" for the "MAC Mode" parameter and is not connected to an access point.
	Flashing yellow and green  Interval: 3x (100 ms on / 100 ms off) 1x 1000 ms on	*Client mode:* The client waits for the MAC address due to the setting "Automatic" for the "MAC Mode" parameter and is connected to an access point.

LED	Color	Meaning
F	Off 	No fault/error.
	Red 	The device is starting up or an error has occurred.
	Flashing red  Interval: 500 ms on / 500 ms off	The bootloader waits in this state for a new firmware file that you can download by TFTP.
	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 yellow flashing 	A competing radar signal was found on all enabled channels.
P1 R1	Flashing yellow 	The port LEDs flash for detection of device location. The "LED flash" function is • 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)

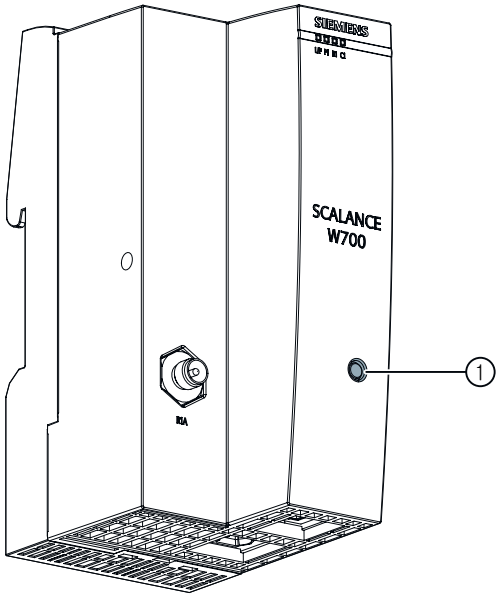
If the device detects competing radar signals on all enabled channels of the WLAN interface, the **F** LED is lit and **R1** flash. No data traffic is then possible for the next 30 minutes. After this time, the device runs the scan again and checks whether a primary user still exists. If no primary user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

4.6 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 51)".
- **Resetting the device to factory settings**
  If you reset, all the settings you have made will be overwritten by factory defaults. If a PLUG has been inserted in the device, the PLUG is also reset to default settings. You can find more detailed information in the section "Restoring the factory settings (Page 51)".

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 notices for installation

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.

⚠ 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.

⚠ WARNING

The device is intended for indoor use only.

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

⚠ WARNING

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

⚠ WARNING

EXPLOSION HAZARD

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

⚠ WARNING

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

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

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

⚠ WARNING

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

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:

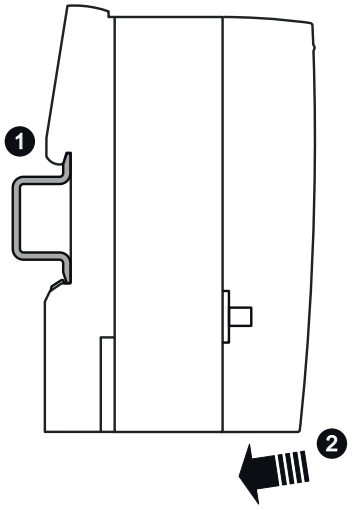
- Installation in a suitable cabinet.
- Installation in a suitable enclosure.
- Installation in a suitably equipped, enclosed control room.

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.

5.2 Installing on a DIN rail / removing

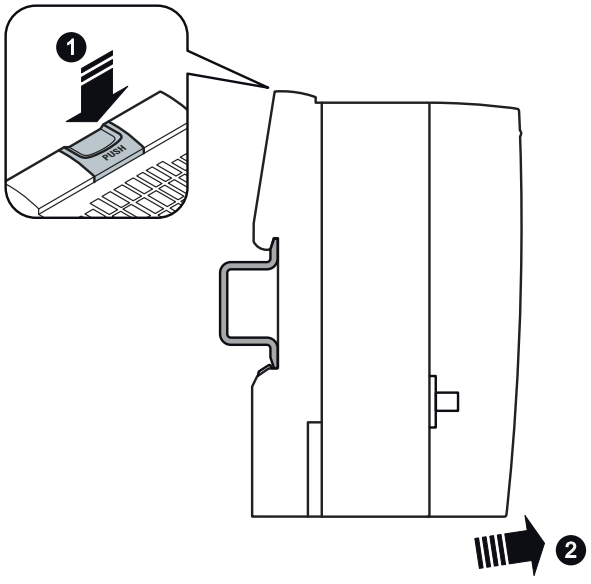
Procedure for installation



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 up

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 24) 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 62368-1 / EN 62368-1 / VDE 62368-1 may be connected to the power supply terminals.
- The power supply unit for the device must meet NEC Class 2 according to the National Electrical Code (r) (ANSI / NFPA 70).

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

Grounding



⚠ WARNING

Danger to life from overvoltage, fire hazard

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

NOTICE

Damage to the device due to potential differences

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

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

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

WARNING

EXPLOSION HAZARD

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

WARNING

EXPLOSION HAZARD

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

WARNING

Unsuitable cables or connectors

Risk of explosion in hazardous areas

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

⚠ WARNING

Lack of equipotential bonding

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

- Ensure that equipotential bonding is available for the device.

⚠ WARNING

Unprotected cable ends

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

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

⚠ WARNING

Improper installation of shielded cables

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

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

⚠ WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

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

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

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

⚠ WARNING

Transient overvoltages

Take measures to prevent transient 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.

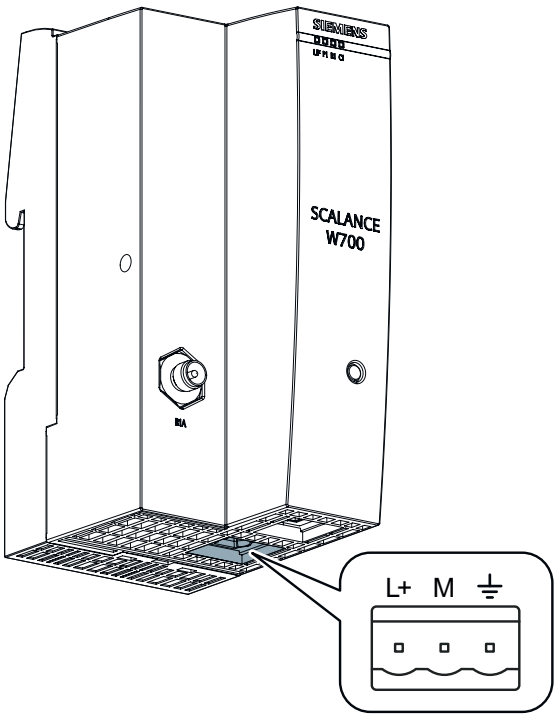
6.2 Power supply

⚠ 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 47)"

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

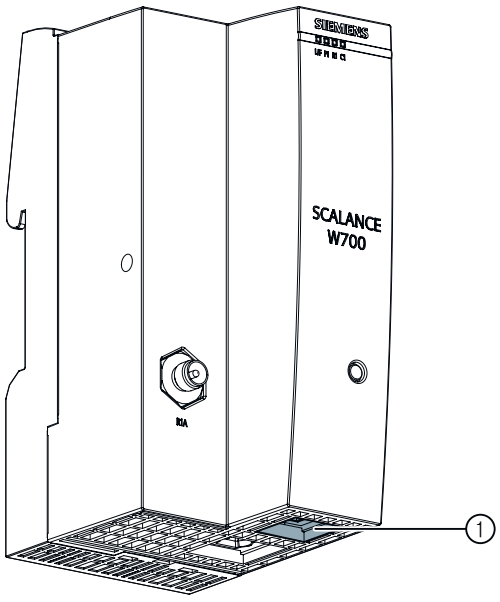
The "L/F" LED indicates whether a power supply is connected; see section "LED display (Page 28)".

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

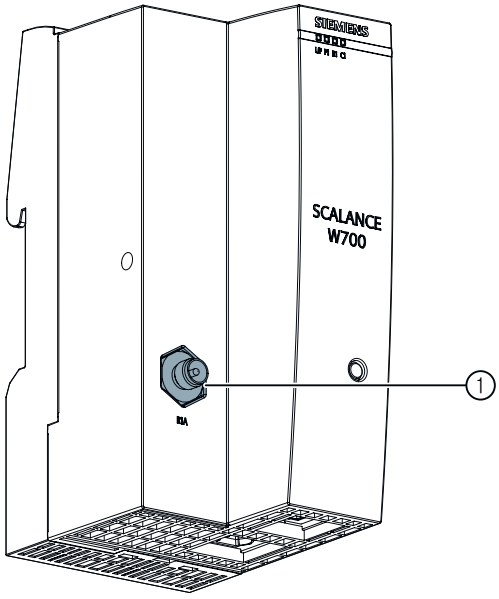
Pin assignment

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 connector

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.

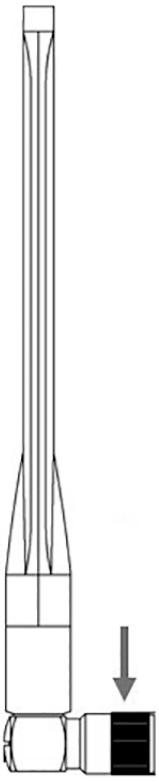


Figure 6-1 Figure of the ANT795-4MA; the arrow points to the screw cap.

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 and antennas (Page 23)".

6.5 Grounding

Functional grounding must be established from the 3-pin terminal block to the DIN rail; refer to section "Device view (Page 21)" or section "Power supply (Page 43)". 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 22) 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

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

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

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

1. Turn off the power to the device.
2. 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 31)".

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

1. Turn off the power to the device.
2. 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 W761-1 RJ-45
- SCALANCE W722-1 RJ-45
- SCALANCE W721-1 RJ-45

Note

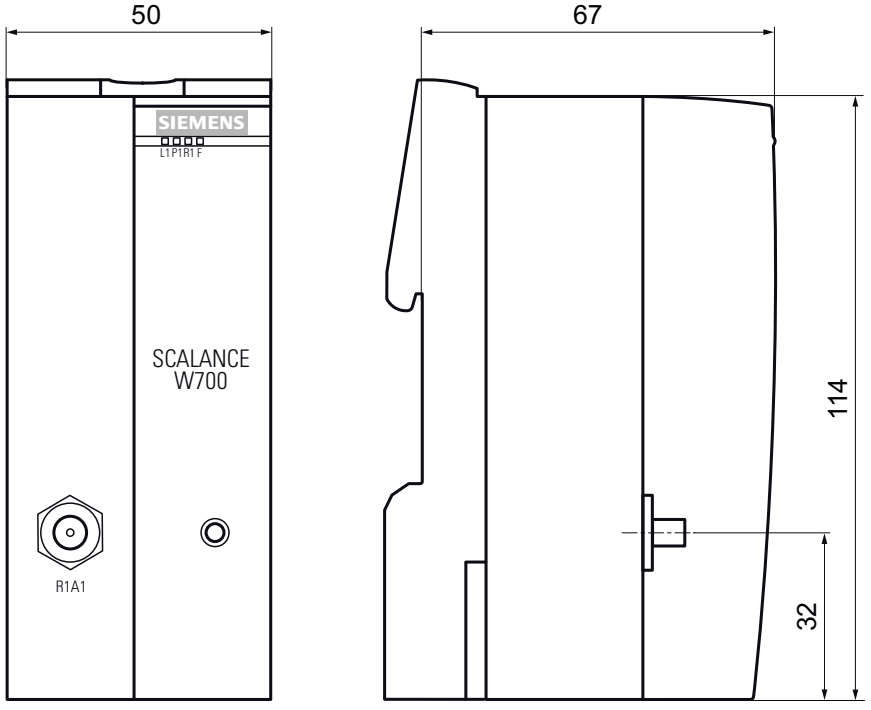
You will find detailed information on the transmit power and receiver sensitivity in the document "Performance data 802.11 abgn SCALANCE W760/W720" on the supplied data medium (REF_W760-RadioInterface.pdf).

SCALANCE W761/W722/W721		
Data transfer		
Ethernet transfer rate		10 / 100 Mbps
Wireless transmission rate		1 ... 150 Mbps
Wireless standards supported		IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11h IEEE 802.11n
Attachment to Industrial Ethernet		
	Quantity	1
	Design	RJ-45 jack
	Properties	Half duplex/full duplex, autocrossover, auto-negotiation, autosensing, floating
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 IE FC TP FRNC cable IE FC TP festoon cable IE FC TP food 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		

SCALANCE W761/W722/W721		
Antenna connector	Quantity	1
	Design	R-SMA female
	Impedance	50 Ω nominal
Frequency range		2412 ... 2480 MHz 4920 ... 5875 MHz
Electrical data		
Power supply	Supply voltage	24 V DC safety extra low voltage (SELV)
	Permitted range	19.2 to 28.8 VDC
	Design	Terminal block, 3 terminals
Fusing		2.5 A / 24 VDC
Current consumption	At 24 VDC / typical	150 mA
Power loss at 24 VDC	At 24 V DC / maximum	3.6 W
	At 24 VDC / typical	2.2 W
Permitted ambient conditions		
Ambient temperature	During operation with the rack installed horizontally / vertically	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 protection		
	IP code	IP20
Dimensions and weight		
Dimensions	W x H x D	50 x 114 x 74 mm
Weight		130 g
Installation options		
	Mounting on a DIN rail	
Mean time between failure (MTBF)		
	at 40 °C ambient temperature	106.51 years

10 Dimension drawings

The dimensions are specified in mm.



11 Approvals

You will find the approvals of the products in the reference work "Approvals SCALANCE W700 802.11n" on the Internet pages of 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

A

Accessories, 22
Antenna, 46
Antenna cables, 23
Antennas, 23
  Directional antenna, 26
  Dual directional antenna with linear polarization, 26
  Dual-band directional antenna with linear polarization, 26
  Helical antenna, 25
  MIMO antenna, 26
  Omnidirectional antenna, 25
Article numbers, 5

B

Button, 31

C

Certification ID, 5
Configuration manuals, 52
Connecting
  Antenna, 46
  Ethernet, 44
  Grounding, 47
  Power supply, 43

D

Dimension drawing, 55
Documentation on the Internet, 5

E

Ethernet, 44

F

Factory defaults, 51
Factory setting, 51

G

Grounding, 40, 47

I

Installation
  DIN rail, 36
Interfaces, 53, 54

L

LED display, 28
Lightning protection, 39

P

Pin assignment, 45
Power supply, 43
Primary user (radar), 28

R

Reset button, 31
Reset device, 51

S

Safety extra low voltage, 40
Safety notices
  for installation, 33
  general, 9
  Use in hazardous areas, 9, 33, 39
  when connecting up, 39
Scope of delivery, 22
Scope of validity, 5

T

Technical specifications, 53, 54
Type designation, 21