SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE W774-1 / W734-1

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

Upkeep and maintenance 8

Technical data 9

Dimension drawings 10

Approvals 11

SCALANCE W Mainstream (MSN)

03/2022

C79000-G8976-C325-15

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 personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C325-15
Ⓟ 03/2022 Subject to change

Table of contents

1 Introduction 5

2 Safety notices 9

3 Security recommendations 11

4 Description of the device 19

4.1 Structure of the type designation 19

4.2 Device view 20
4.2.1 SCALANCE W7x4-1 RJ45 20
4.2.2 SCALANCE W774-1 M12 21

4.3 Components of the product 21

4.4 Accessories 22
4.4.1 PLUG 22
4.4.2 Industrial Ethernet 22
4.4.3 Power supply 24
4.4.4 Flexible connecting cables, antennas and accessories 24
4.4.4.1 Flexible connecting cables 24
4.4.4.2 Lightning protection 26
4.4.4.3 Terminating resistor 26
4.4.4.4 Cabinet feedthrough 26
4.4.4.5 Antennas 27

4.5 LED display 29

4.6 Reset button 32

4.7 PLUG 34

5 Installation and removal 37

5.1 Safety notices for installation 37

5.2 Wall mounting 39

5.3 Installing on an S7-300 standard rail 41

5.4 Installing on an S7-1500 standard rail 42

5.5 Installing on a DIN rail / removing 43

6 Connection 45

6.1 Safety when connecting up 45

6.2 Power supply 50

6.3 Ethernet 52

6.4 Antenna connectors 54

6.5 Grounding 56

6.6 Replacing the PLUG 57

7 **Maintenance and cleaning** **59**

8 **Upkeep and maintenance** **61**

8.1 Device configuration with PRESET-PLUG 61

8.2 Restoring the factory settings 63

8.3 Firmware update via WBM or CLI not possible 65

9 **Technical data** **67**

9.1 SCALANCE W774/W734 RJ45 67

9.2 SCALANCE W774 M12 69

10 **Dimension drawings** **73**

11 **Approvals** **75**

Index **77**

Introduction 1

Validity of the Operating Instructions

These operating instructions cover the following products:

Product	Article number	Article number of the US version	Article number of the Israel version
Access points			
SCALANCE W774-1 RJ-45	6GK5774-1FX00-0AA0	6GK5774-1FX00-0AB0	6GK5774-1FX00-0AC0
SCALANCE W774-1 M12 EEC	6GK5774-1FY00-0TA0	6GK5774-1FY00-0TB0	-
Ethernet client module			
SCALANCE W734-1 RJ-45	6GK5734-1FX00-0AA0	6GK5734-1FX00-0AB0	-

These operating instructions apply to the following software version:

- SCALANCE W774/W734 with firmware as of version 6.5

Purpose of the Operating Instructions

Based on the operating instructions, you will be able to install and connect up the SCALANCE W774/W734 correctly. The configuration and the integration of the device in a WLAN are not described in these instructions.

Documentation on the accompanying DVD

You can find detailed information about configuration in the SCALANCE W700 configuration manuals on the accompanying DVD under the file name:

PH_SCALANCE-W770-W730-WBM_76.pdf and PH_SCALANCE-W770-W730-CLI_76.pdf

Note

Make sure that you read the explanations and instructions in the readme.htm file

Documentation on the Internet

You can find the current version of the document on the Internet at (https://support.industry.siemens.com/cs/de/en/ps/15859/man)

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

Documentation on configuration

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

- SCALANCE W770/W730 nach IEEE 802.11n Web Based Management
- SCALANCE W770/W730 nach IEEE 802.11n Command Line Interface

Note

Make sure that you read the explanations and instructions in the readme.htm file.

Training, Service & Support

You will find information on Training, Service & Support in the multi--language document "DC_support_99.pdf" on the data medium supplied with the documentation.

Security information

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

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions 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 security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity
(https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends 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 Security RSS Feed under
https://www.siemens.com/cert (https://www.siemens.com/cert).

Firmware

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

The firmware is available on the Internet pages of the Siemens Industry Online Support: (https://support.industry.siemens.com/cs/de/en/ps/15860/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.

Device defective

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

Decommissioning

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

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

Also restore the factory settings on the storage medium.

Recycling and disposal

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

Do not dispose of the products at public disposal sites.

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

Note the different national regulations.

Trademarks

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

SCALANCE, C-PLUG, RCoax

2 Safety notices

⚠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

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 2048 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 access the system without authorization.
- For communication via non-secure networks, use additional devices with VPN functionality to encrypt and authenticate communication.
- When you establish a secure connection to a server (for example for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTP, HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it. For more information, refer to "Decommissioning (Page 7)".
- We recommend formatting a PLUG that is not being used.

Hardware / Software

- Use VLANs whenever possible as protection against denial-of-service (DoS) attacks and unauthorized access.
- Restrict access to the device by setting firewall rules or rules in an access control list (ACL).
- Selected services are enabled by default in the firmware. It is recommended to enable only the services that are absolutely necessary for your installation.
  For more information on available services, see "List of available services (Page 15)".
- Use the latest web browser version compatible with the product to ensure you are using the most secure encryption methods available. Also, the latest web browser versions of Mozilla Firefox, Google Chrome, and Microsoft Edge have 1/n-1 record splitting enabled, which reduces the risk of attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (for example, BEAST).

- Ensure that the latest firmware version is installed, including all security-related patches.
  You can find the latest information on security patches for Siemens products at the Industrial Security (https://www.siemens.com/industrialsecurity) or ProductCERT Security Advisories (https://www.siemens.com/cert) website.
  For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.
- Enable only those services that are used on the device, including physical ports. Free physical ports can potentially be used to gain access to the network behind the device.
- For optimal security, use SNMPv3 authentication and encryption mechanisms whenever possible, and use strong passwords.
- Configuration files can be downloaded from the device. Ensure that configuration files are adequately protected. The options for achieving this include digitally signing and encrypting the files, storing them in a secure location, or transmitting configuration files only through secure communication channels.
  Configuration files can be password protected during download. You enter passwords on the WBM page "System > Load & Save > Passwords".
- When using SNMP (Simple Network Management Protocol):
  - Configure SNMP to generate a notification when authentication errors occur. For more information, see WBM "System > SNMP > Notifications".
  - Ensure that the default community strings are changed to unique values.
  - Use SNMPv3 whenever possible. SNMPv1 and SNMPv2c are considered non-secure and should only be used when absolutely necessary.
  - If possible, prevent write access above all.
- Use the security functions such as address translation with NAT (Network Address Translation) or NAPT (Network Address Port Translation) to protect receiving ports from access by third parties.
- Use WPA2/ WPA2-PSK with AES to protect the WLAN. You can find additional information in the configuration manual Web Based Management "Security menu".

Secure/ non-secure protocols

- Use secure protocols if access to the device is not prevented by physical protection measures.
- Disable or restrict the use of non-secure protocols. While some protocols are secure (e.g. HTTPS, SSH, 802.1X, etc.), others were not designed for the purpose of securing applications (e.g. SNMPv1/v2c, RSTP, etc.).

  Therefore, take appropriate security measures against non-secure protocols to prevent unauthorized access to the device/network. Use non-secure protocols on the device using a secure connection (e.g. SINEMA RC).

- If non-secure protocols and services are required, ensure that the device is operated in a protected network area.
- Check whether use of the following protocols and services is necessary:
  - Non-authenticated and unencrypted ports
  - LLDP
  - Syslog
  - DHCP options 66/67
  - TFTP
  - Telnet
  - HTTP
  - SNMP v1/2c
  - Syslog
  - SNTP
- The following protocols provide secure alternatives:
  - SNMPv1/v2c → SNMPv3

    Check whether use of SNMPv1/v2c is necessary. SNMPv1/v2c is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options.

    If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.

    Use SNMPv3 in conjunction with passwords.
  - HTTP → HTTPS
  - Telnet → SSH
  - TFTP → SFTP
  - Syslog Client → Syslog Client TLS
- Using a firewall, restrict the services and protocols available to the outside to a minimum.
- For the DCP function, enable the "Read Only" mode after commissioning.

List of available services

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

The table includes the following columns:

- **Service**

  The services that the device supports
- **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
			Port	Service		
DHCP Client IPv4	UDP/68	Outgoing only	--	✓	--	--
DHCP Client IPv6	UDP/546	Outgoing only	--	✓	--	--
DHCP Server	UDP/67	Closed	--	✓	--	--
DNS Client	TCP/53 UDP/53	Outgoing only	--	✓	--	--
EthernetIP	TCP/44818 UDP/2222 UDP/44818	Closed	--	✓	--	--
HTTP	TCP/80	Open	✓	✓	✓	--
HTTPS	TCP/443	Open	✓	✓	✓	✓
NTP Client	UDP/123	Outgoing only	✓	✓	--	--
PROFINET	UDP/34964 UDP/49154 UDP/49155	Open	--	✓	--	--
RADIUS Client	UDP/1812	Outgoing only	✓	✓	✓	--
Remote Capture	TCP/2002	Closed	--	✓	--	--
SFTP Client	TCP/22	Closed	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	--	--
SMTP Client (secure) [1]	TCP/465	Closed	✓	✓	✓	✓
SNMPv1/v2c	UDP/161	Open	✓	✓	--	--
SNMPv3	UDP/161	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outgoing only	--	✓	--	--
SNTP Client	UDP/123	Outgoing only	✓	✓	--	--
SSH	TCP/22	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Closed	✓	✓	--	--
Syslog (secure) Client	TCP/6514	Closed	✓	✓	--	✓
Telnet	TCP/23	Closed [1] / Open [2]	✓	✓	✓	--
TFTP Client	UDP/69	Outgoing only	✓	✓	--	--

1) Only for SCALANCE W1700ac

2) Only for SCALANCE W700n

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.

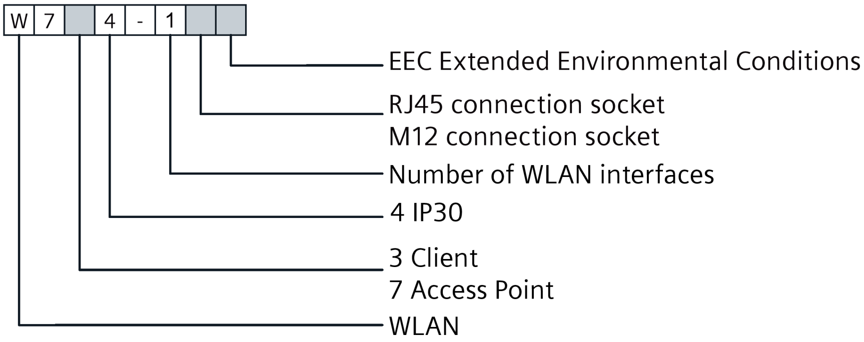
Layer 2 service	**Default status**	**Service configurable**
DCP	Open	✓
LLDP	Open	✓
RSTP	Open	✓
iPRP	Open	✓
MSTP	Closed	✓
SIMATIC NET TIME	Closed	✓

Description of the device

4

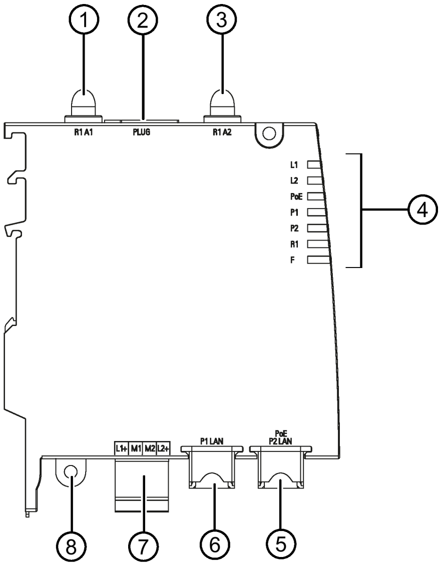
4.1 Structure of the type designation

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



4.2 Device view

4.2.1 SCALANCE W7x4-1 RJ45



① Antenna connector R1A1

② PLUG slot and Reset button

③ Antenna connector R1A2

④ LED display

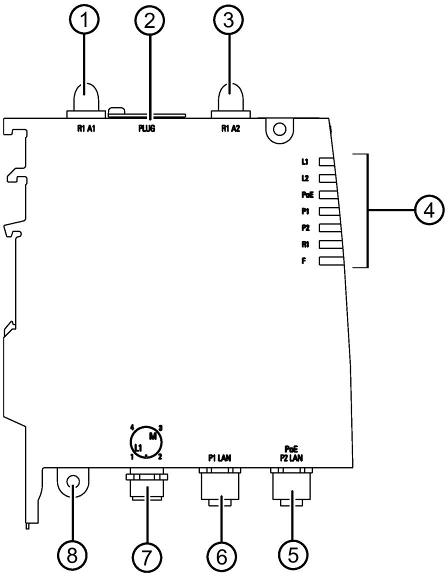
⑤ Ethernet connector P2 (PoE capability)

⑥ Ethernet connector P1

⑦ Connector for power supply

⑧ Eye for grounding (diameter 4.5 mm) and wall mounting

4.2.2 SCALANCE W774-1 M12



① Antenna connector R1A1
② PLUG slot and Reset button
③ Antenna connector R1A2
④ LED display
⑤ Ethernet connector P2 (PoE capability)
⑥ Ethernet connector P1
⑦ Connector for power supply
⑧ Eye for grounding (diameter 4.5 mm) and wall mounting

4.3 Components of the product

The following components are supplied with the product:

- One SCALANCE W device
- Two protective caps for the antenna sockets
- One screw for mounting on an S7-300 standard rail or S7-1500 standard rail
- One product DVD

In addition with the M12 device version

- Three protective caps for the M12 sockets

In addition with the RJ45 device version:

- One 4-pin 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.

4.4 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 PLUG

Component	Description	Article number
C-PLUG	Configuration PLUG Exchangeable storage medium for configuration data.	
	256 MB	6GK1900-0AB10
KEY-PLUG features	Enabling of iFeatures and exchangeable storage medium for storage of configuration data	
	KEY-PLUG W780 iFeatures AP	6GK5907-8PA00
	KEY-PLUG W740 iFeatures Client	6GK5907-4PA00
KEY-PLUG W700 Security	W700 Security Enabling of “Inter AP Blocking” and exchangeable storage medium for storage of configuration data	6GK5907-0PA00

4.4.2 Industrial Ethernet

M12 data plug-in connector

Component	Description		Article number
IE FC M12 PLUG PRO 2x2	M12 data plug-in connector for IE FC TP cables 2x2, IP65/67, D-coded, axial cable outlet	1 connector per package	6GK1901-0DB20-6AA0
		8 connectors per package	6GK1901-0DB20-6AA8

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
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

4.4.3 Power supply

Energy cable

Component	Description	Article number
Energy cable 2 x 0.75	Energy cable for connection of signaling contact and power supply 24 VDC, stranded wire 2 x 0.75 mm^2, trailing type, not assembled Sold by the meter	6XV1812-8A
Robust Energy Cable 4 x 0.75	Energy cable for connection of power supply 24 VDC, 4-wire stranded 4 x 0.75 mm^2, robust, flexible, not assembled Sold by the meter	6XV1801-2A
M12 PLUG-IN CABLE	Flexible plug-in power cable to connect the power supply 24 VDC, 4-wire, preassembled with a 4-pin M12 plug and an M12 socket (A-coded)	6XV1801-5D*

* Available in different lengths

Socket

Component	Description	Article number
IE POWER M12 CABLE CONNECTOR PRO	Socket for the 24 VDC power supply. 4-pin, A-coded pack of 3	6GK1907-0DC10-6AA3

4.4.4 Flexible connecting cables, antennas and accessories

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

4.4.4.1 Flexible connecting cables

Flexible connecting cable N-Connect/R-SMA

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

4.4.4.2 Lightning protection

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

4.4.4.3 Terminating resistor

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

4.4.4.4 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

4.4.4.5 Antennas

Note

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

You will find more detailed information in Wireless approvals (https://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
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 λ 4 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

Type	Properties	Article number
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.

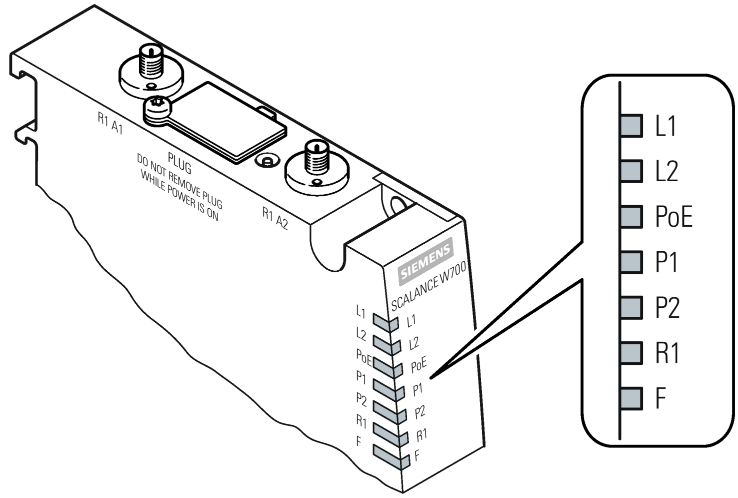
Notice for USA/Canada

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.
L2	Off □	Power supply L2 too low.
	Green 🟩	Power supply L2 is applied.
PoE	Off □	The device is not supplied using PoE.
	Green 🟩	The device is supplied using PoE.
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
P2	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.
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.
F	Off □	No fault/error.
	Red 🟥	The device is starting up or an error has occurred.

LED	Color	Meaning
	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: 2000 ms on / 200 ms off	Firmware on PLUG: The device is performing a firmware update or downgrade.
	Red 🟥 Simultaneous R1 yellow flashing 🟨	A competing radar signal was found on all enabled channels.
P1 P2 R1	Flashing yellow 🟨	The port LEDs flash for detection of device location. The "LED flash" function is • Either with SINEC PNI • Or via 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.

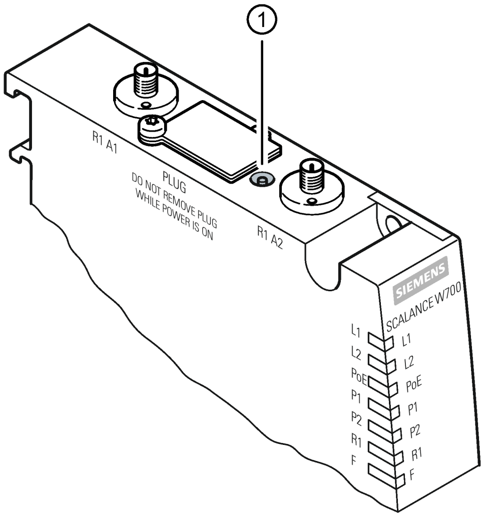
The wait time of 30 minutes is necessary due to legal requirements and cannot be shortened even by restarting the device.

4.6 Reset button

Position

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

The Reset button ① is on the top of the housing:



Functions of the reset button

The reset button has the following functions:

- **Restart of the device**

  To restart the device, press the Reset button briefly.

  Note

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

- **Loading new firmware**

  If the "Load & Save" menu command 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 will find further information in the configuration manual in Downloading new firmware using TFTP without WBM and CLI.

- **Resetting the device to the factory defaults**

  The device can be reset to the factory defaults during operation. You will find more detailed information in the configuration manual in Resetting the device to factory defaults.

NOTICE

Previous settings

If you reset, all the changes you have made will be overwritten by factory defaults.

NOTICE

Inadvertent reset

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

4.7 PLUG

The PLUG is available in the following variants:

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

You will find the article numbers under Accessories (Page 22).

NOTICE

Do not remove or insert a C-PLUG / KEY-PLUG during operation!

A PLUG may only be removed or inserted when the device is turned off.

The device checks whether or not a PLUG is inserted at one second intervals. If it is detected that the PLUG was removed, there is a restart.

If a KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE W, the available wireless interfaces are deactivated in this case.

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

NOTICE

Loss of the degree of protection

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

Position

The PLUG slot is on the top of the device housing under a cover, see Device description (Page 20).

Function

The device supports the following modes of operation:

- Without PLUG

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

- With PLUG

  If an unwritten PLUG (factory status or deleted with Clean function) is used, the local configuration already existing on the device is automatically stored on the inserted PLUG. If the PLUG contains a license, additional functions are also enabled.

  A device with a written and accepted PLUG ("ACCEPTED" status) uses the configuration data of the PLUG automatically when it starts up. Acceptance is possible only when the data was written by a compatible device type.

  One exception to this can be the IP configuration if it is set using DHCP and the DHCP server has not been reconfigured accordingly. Reconfiguration is necessary if you use functions based on MAC addresses.

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

  If changes are made to the configuration, the device stores the configuration directly on the PLUG, if this is in the "ACCEPTED" status. The internal memory is neither read nor written.

Response to errors

Inserting a PLUG that does not contain the configuration of a compatible device type, accidentally removing the PLUG/KEY-PLUG or general malfunctions of the PLUG are signaled by the diagnostics mechanisms of the device (LEDs, Web-Based Management (WBM), SNMP, Command Line Interface (CLI) and PROFINET diagnostics). The user then has the choice of either removing the PLUG again or selecting the option to reformat the PLUG.

Note

Incompatibility with previous versions with PLUG inserted

During the installation of a previous version of the firmware, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "NOT ACCEPTED" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data. If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using "System > PLUG".

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

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

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

⚠**WARNING**

To comply with EU Directive 2014/34 EU (ATEX 114), UK-Regulation SI 2016/1107 or the conditions of IECEx or CCC-Ex, the housing or cabinet must meet the requirements of at least IP54 (according to EN/IEC 60529, GB/T 4208) in compliance with EN IEC/IEC 60079-7, GB 3836.8.

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.

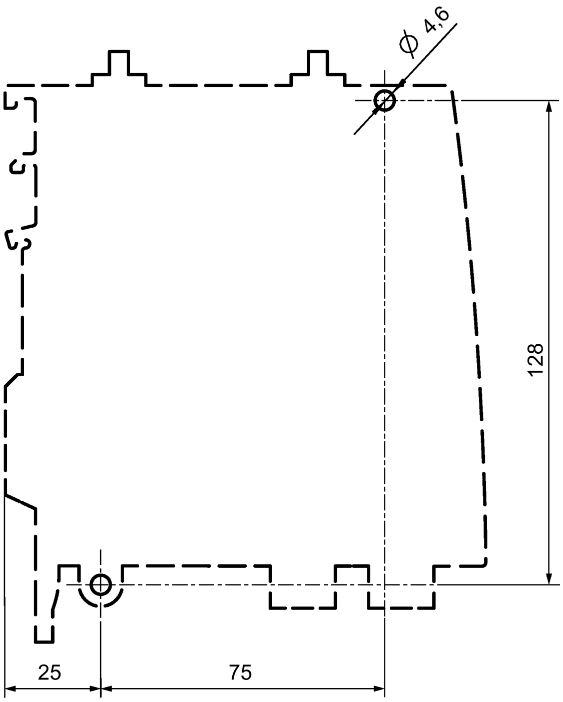
Note

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

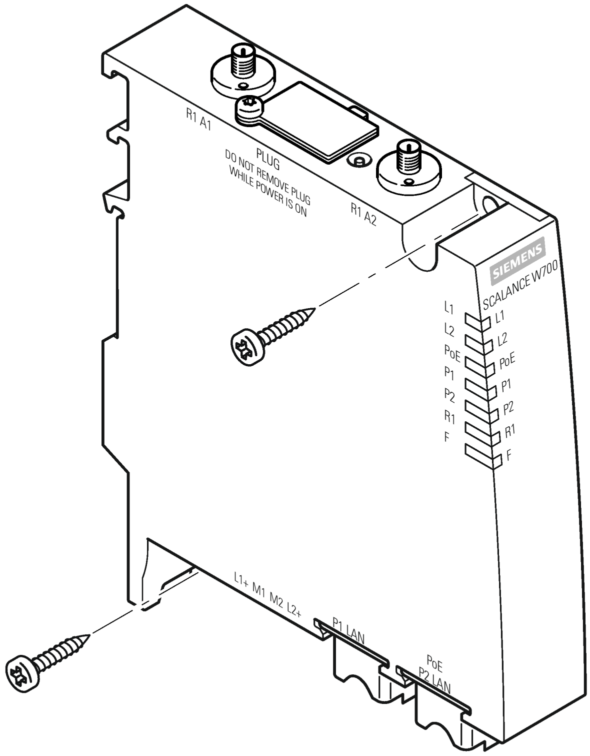
5.2 Wall mounting

Drilling template

The location of the holes for fitting the mounting plate of the device is shown in the following figure:


∅ 4,6
128
25
75

Procedure

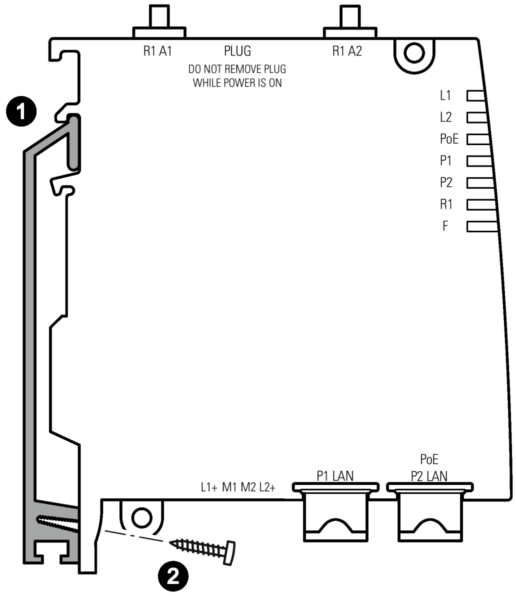

R1 A1
PLUG
DO NOT REMOVE PLUG
WHILE POWER IS ON
R1 A2
SIEMENS
SCALANCE W700
L1
L2
PoE
P1
P2
R1
F
L1+ M1 M2 L2+
P1 LAN
PoE
P2 LAN

1. Prepare the drill holes for wall mounting. For the precise dimensions, refer to the drilling template.
2. Secure the device to the wall with two screws. The screws are not supplied with the device.

   The type and length of the screws depend on the type of wall.
3. Mount the connecting cables and the antenna, see section "Connecting up (Page 45)".

5.3 Installing on an S7-300 standard rail

Procedure



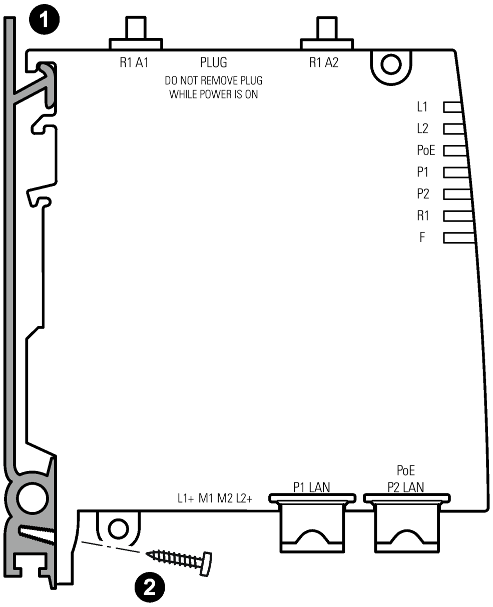
Follow the steps below to mount the device on an S7-300 standard rail:

1. Place the device on the upper edge of the S7-300 standard rail as shown in the figure.
2. Screw the housing to the S7-300 standard rail.

   The required screw ships with the device.
3. Mount the connecting cables and the antenna, see section "Connecting up (Page 45)".

5.4 Installing on an S7-1500 standard rail

Procedure

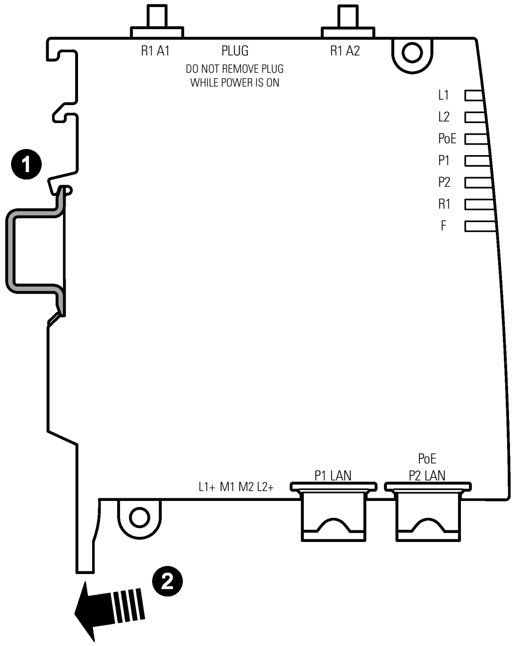


Follow the steps below to fit the SCALANCE W774/W734 to an S7-1500 standard rail:

1. Place the device on the upper edge of the S7-1500 standard rail as shown in the figure.
2. Screw the housing to the S7-1500 standard rail. The required screw ships with the device.
3. Mount the connecting cables and the antenna, see section "Connecting up (Page 45)".

5.5 Installing on a DIN rail / removing

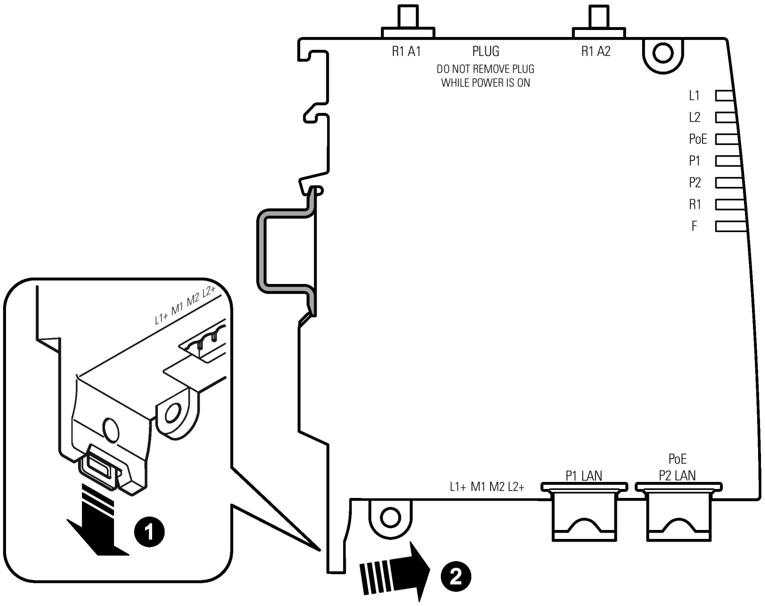
Procedure for installation



Follow the steps below to fit the SCALANCE W774/W734 to 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 45)".

Procedure when removing



Follow the steps below to remove the SCALANCE W774/W734 from a DIN rail:

1. Turn off the power to the device.
2. Disconnect all connected cables.
3. Pull the DIN rail slider down with a screwdriver.
4. Tilt the SCALANCE W774/W734 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.

Note

Close unused sockets

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

Lightning protection

⚠ WARNING

Danger due to lightning strikes

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

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

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

Note

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

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

⚠ **WARNING**

Danger due to lightning strikes

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

Note

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

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

Supply voltage

⚠ **WARNING**

Power supply

The device is designed for operation with a directly connectable safety extra low voltage (SELV) 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 overvoltages of more than 40% of the rated voltage (or more than 119 V). This is the case if you only operate devices with SELV (safety extra-low voltage).

⚠WARNING

Suitable cables at high ambient temperatures in hazardous area

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

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

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

⚠WARNING

WARNING - EXPLOSION HAZARD -

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

⚠WARNING

Restricted area of application

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

⚠WARNING

Restricted area of application

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

6.2 Power supply

Note

Galvanic isolation of the power supply unit

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

SCALANCE W774/W734 RJ45

With this device version, there are two options for the power supply:

- Direct infeed via the four-pin connection socket ①

  For the direct infeed of the power supply, use copper cables with the following properties:

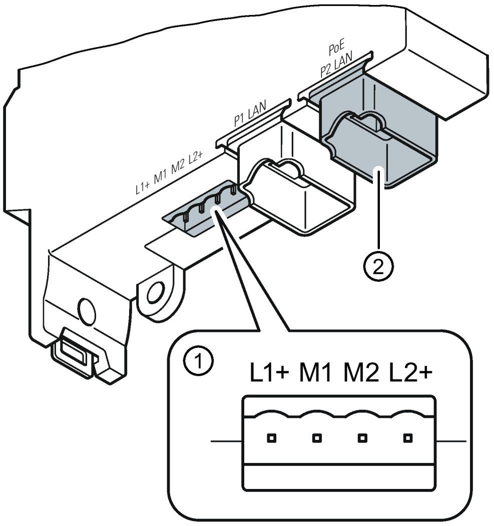
  – Round cable cross-section with 6 to 8 mm diameter.

  – Two-wire cable with 0.5 to 1.5 mm2 cross-section per wire.

  – Permitted tensile load at least 100 N. - UL

  – Listing of the cables according to the national installation regulations. In areas where NEC or CEC applies: Type PTLC or ITC

- Power over Ethernet via the RJ45 Ethernet interface P2 ②. The other Ethernet interface P1 is not capable of PoE.



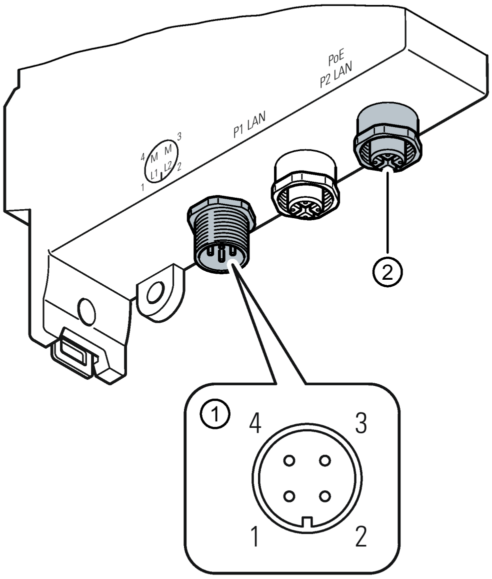
The 4-pin connection socket has the following pin assignment:

Pin	Assignment
L1+	24 VDC
M1	Ground
M2	Ground
L2+	24 VDC

SCALANCE W774 M12 EEC

With this device version, there are two options for the power supply:

- Direct infeed via the four-pin M12 connection socket ①
  - Round cable cross-section with 6 to 8 mm diameter.
  - Two-wire cable with 0.5 to 1.5 mm2 cross-section per wire.
  - Permitted tensile load at least 100 N. - UL
  - Listing of the cables according to the national installation regulations. In areas where NEC or CEC applies: Type PTLC or ITC
- Power over Ethernet via the M12 Ethernet interface P2 ②. The other Ethernet interface P1 is not capable of PoE.



The 4-pin M12 socket has the following pin assignment:

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

Power over Ethernet

The two following variants are available for power supply via an Ethernet cable:

- **IEEE 802.3at type 1 (IEEE 802.3af)**
  On an 8-wire Fast Ethernet cable, the power is supplied via the free data wires 4, 5, 7 and 8. This corresponds to alternative B according to IEEE 802.3af.
- **IEEE 802.3 at type 2**
  The power supply is known as phantom power via the wire pairs carrying signals (1/2 and 3/6).

The SCALANCE W774/W734 RJ45 devices support the standards IEEE 802.3at type 1 (IEEE 802.3af) and IEEE 802.3 at type 2.

Note

Disabling the PoE power supply

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

Note

"Phantom power" only with SCALANCE W774 M12 EEC

The SCALANCE W774 M12 EEC device only supports the standard IEEE 802.3 at type 2. With this device, the attachment to Ethernet is only possible using four-wire cables. For this reason, no PSE (Power Sourcing Equipment) can be used that only supplies the power via the free wire pairs.

Ethernet cables with M12 connectors for the SCALANCE W788-x M12 (Gigabit Ethernet, eight-wire) cannot be used for the SCALANCE W774 M12 EEC.

Note

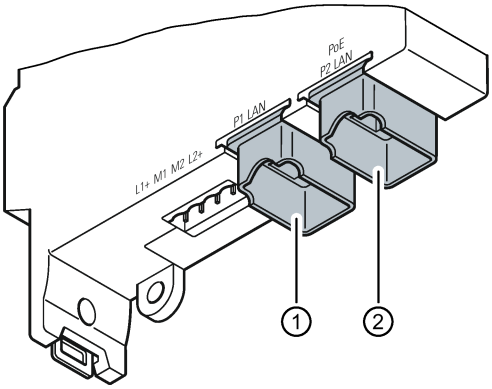
No power sourcing equipment (PSE)

The SCALANCE W774/W734 devices cannot be used as a PoE power supply for other devices.

6.3 Ethernet

The SCALANCE W774/W734 devices have two Ethernet interfaces located on the underside of the device. Depending on the version, either RJ-45 or M12 sockets are available.

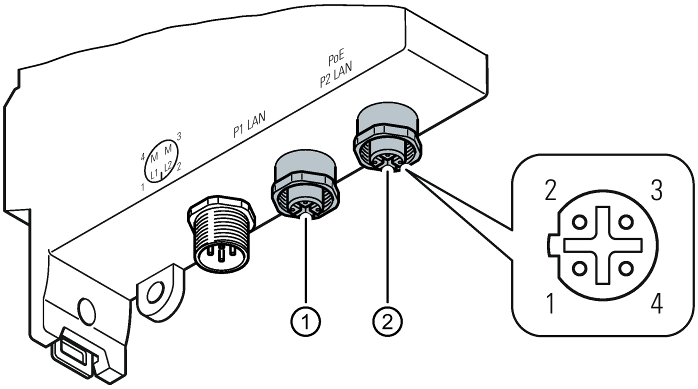
SCALANCE W774/W734 RJ-45



① Ethernet interface P1

② Ethernet interface P2
The power can also be supplied via this interface (Power over Ethernet).

SCALANCE W774/W734 M12 EEC



① Ethernet interface P1

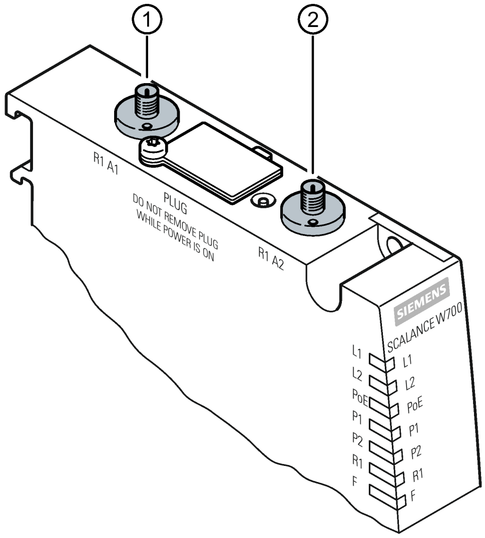
② Ethernet interface P2
The power can also be supplied via this interface (Power over Ethernet).

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

Pin	Assignment
1	TX
2	RX
3	TX
4	RX

6.4 Antenna connectors

The SCALANCE W774/W734 has two antenna connectors of the type R-SMA located on the top of the device.



① Antenna connector R1 A1

② Antenna connector R1 A2

Procedure

Follow the steps below to connect a cable for an external antenna to a SCALANCE W774/734:

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

NOTICE
R-SMA antenna connector
When securing antennas to the device, only the screw cap of the antenna can be rotated. Rotating the entire antenna could damage the R-SMA connector of the device.

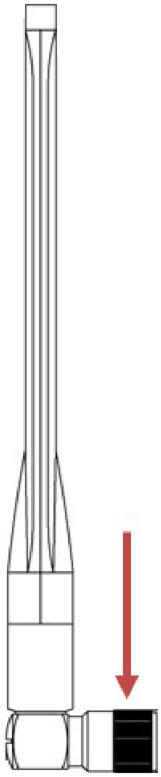


Figure 6-1 Figure of the ANT795-4MA; the arrow points to the screw cap.

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

NOTICE

UL approval only for use in buildings

Within the area of authority of the NEC and CEC, the SCALANCE W770/W730 devices and the antennas connected to them may only be used in a closed building. For this reason, do not lead antennas into the outdoor area if you need to meet UL requirements.

Note

Cabinet installation

When installing the SCALANCE W770/W730 in a cabinet, you need to use detached antennas. A suitable flexible connecting cable for a connection between SCALANCE 770/W730 and a detached antenna are available from SIMATIC NET. You will find detailed information in the section Accessories (Page 22).

6.5 Grounding

Grounding with wall mounting

The device is grounded by the securing screw in the unpainted hole (diameter 4.5 mm) see position ⑧ of the Device description (Page 20).

If the device is mounted on a non-conductive base, a grounding cable must be fitted. The grounding cable is not supplied with the device. Connect the paint-free surface of the device to the nearest grounding point using the grounding cable.

Grounding when installing on a DIN rail / S7 standard rail

The device is grounded via the rear of the device.

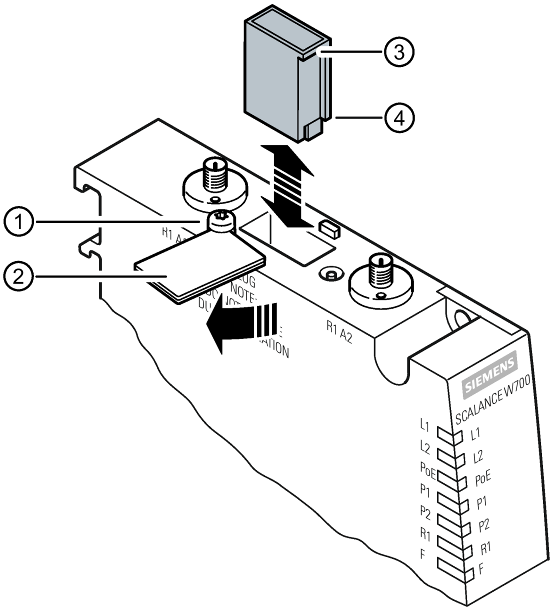
6.6 Replacing the PLUG

Position

The PLUG slot is at the top of the device under a cover, see Reset button (Page 32).

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

Removing the PLUG



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

1. Turn off the power to the device.
2. Loosen the screw for the slot cover ① and swivel the slot cover ② to the side.
3. Insert a screwdriver between the front edge of the PLUG ③ and the slot and release the PLUG.
4. Remove the PLUG from the slot.
5. Screw the cover back onto the device.

Note

Loss of the configuration

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

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

Inserting the PLUG

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

1. Turn off the power to the device.
2. Loosen the screw for the slot cover ① and swivel the slot cover ② to the side.
3. The housing of the PLUG has a protruding ridge on the long side ④. The slot has a groove at this position. Insert the PLUG correctly oriented into the slot. The PLUG is correctly inserted when it is completely inside the device and does not jut out of the slot.
4. Close the slot cover ②.
5. Tighten the screw ① (torque 0.8 Nm) to secure the slot cover.

Maintenance and cleaning 7

⚠WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

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

⚠WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

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

⚠CAUTION

Hot surfaces

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

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

NOTICE

Cleaning the housing

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

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

Do not use solvents.

Upkeep and maintenance 8

8.1 Device configuration with PRESET-PLUG

Note the additional information and security notes in the operating instructions of your device.

NOTICE
Do not remove or insert a PLUG during operation
A PLUG may only be removed or inserted when the device is turned off.

Note

Support as of V6.0

The PRESET-PLUG functionality is supported as of firmware version V6.0.

With the PRESET-PLUG, you can install the same device configuration (start configuration, user accounts, certificates) including the corresponding firmware on multiple devices.

The PRESET PLUG is write-protected.

You configure the PRESET PLUG using the Command Line Interface (CLI).

Creating a PRESET-PLUG

You create the PRESET PLUG using the Command Line Interface (CLI). You can create a PRESET-PLUG from any PLUG. To do this, follow the steps outlined below:

Note

Using configurations with DHCP

Create a PRESET-PLUG only from device configurations that use DHCP. Otherwise, disruptions will occur in network operation due to multiple identical IP addresses.

You assign fixed IP addresses extra following the basic installation.

Requirement

- A PLUG is inserted in the device on which you want to configure the PRESET-PLUG functionality.

Procedure

1. Start the remote configuration using Telnet (CLI) and log on with a user with the "admin" role.
2. Switch to the global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.
4. Create the PRESET-PLUG with the "presetplug" command.
   The firmware version of the device and the current device configuration incl. user accounts and certificates are stored on the PLUG and the PLUG is then write protected.
5. Turn off the power to the device.
6. Remove the PRESET-PLUG.
7. Start the device either with a new PLUG inserted or with the internal configuration.

Procedure for installation with the aid of the PRESET-PLUG

1. Turn off the power to the device.
2. If it exists, remove the PLUG from the slot. You will find further information on this in the operating instructions of your device.
3. Insert the PRESET-PLUG correctly oriented into the slot. The PRESET-PLUG is correctly inserted when it is completely inside the device and does not jut out of the slot.
4. Turn on the power to the device again.
   If there is a different firmware version on the device to be installed compared with that on the PRESET-PLUG, an upgrade/downgrade of the firmware is performed. You can recognize this by the red F-LED flashing (flashing interval: 2 sec on/0.2 sec. off). Afterwards the device is restarted and the device configuration incl. users and certificates on the PRESET-PLUG is transferred to the device.
5. Wait until the device has fully started up.

   The red F-LED is off.
6. Turn off the power to the device after the installation.
7. Remove the PRESET-PLUG.
8. Start the device either with a new PLUG inserted or with the internal configuration.

Note

KEY-PLUG

If you have created the PRESET-PLUG from a KEY-PLUG, for operation with this configuration, you require an inserted KEY-PLUG.

IN this case before recommissioning the device you need to insert the relevant KEY-PLUG.

Note

Restore factory defaults and restart with a PRESET PLUG inserted

If you reset the device to the factory defaults, when the device restarts an inserted PRESET PLUG is formatted and the PRESET PLUG functionality is lost. You then need to create a new PRESET PLUG. The keys stored on the KEY-PLUG for releasing functions are retained.

We recommend that you remove the PRESET PLUG before you reset the device to the factory settings.

Formatting a PRESET-PLUG (resetting the preset function)

You format the PRESET PLUG using the Command Line Interface (CLI) to reset the preset function. To do this, follow the steps outlined below:

1. Start the remote configuration using Telnet (CLI) and log on with a user with the "admin" role.
2. Switch to the global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.
4. Enter the command "factoryclean".
   The PRESET-PLUG is formatted and the preset function is reset.
5. Write the current configuration of the device with the "write" command.

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".

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

1. Turn off the power to the device.
2. Loosen the screws of the cover.
3. Remove the cover.
4. Press the reset button and reconnect the device to the power supply while holding down the button.
5. Hold down the button until the red error LED "F" stops flashing after approximately 10 seconds and is permanently lit.
6. Release the button and wait until the fault LED "F" goes off.

   The device starts automatically with the factory settings.
7. Close the cover (tightening torque 0.8 Nm), to ensure that the device is closed and water and dust proof.

With SINEC PNI

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

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

Via the configuration

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

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

8.3 Firmware update via WBM or CLI not possible

Cause

If there is a power failure during the firmware update, it is possible that the device is no longer accessible using Web Based Management or the CLI.

When pressing the button, make sure you adhere to the instructions in the section "Reset button (Page 32)".

Solution

You can then also assign firmware to a SCALANCE W using TFTP.
Follow the steps below to load new firmware using TFTP:

1. Turn off the power to the device.
2. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) starts to flash after approximately 2 seconds.
4. Now release the button. The bootloader waits in this state for a new firmware file that you can download by TFTP.
5. Connect a PC to the SCALANCE W over the Ethernet interface.
6. Assign an IP address to the SCALANCE W with the SINEC PNI.
7. Open a DOS box and change to the directory where the file with the new firmware is located and then execute the command "tftp -i <ip address> PUT <firmware>". As an alternative, you can use a different TFTP client.
8. Close the cover to ensure that the device is closed and water and dust proof.

Note

Use of CLI and TFTP in Windows 10

If you want to access the CLI or TFTP in Windows 10, make sure that the relevant functions are enabled in Windows 10.

Result

The firmware is transferred to the device.

Note

Please note that the transfer of the firmware can take several minutes. During the transmission, the red error LED (F) flashes.

Once the firmware has been transferred completely to the device, the device is restarted automatically.

Technical data 9

9.1 SCALANCE W774/W734 RJ45

The following technical specifications apply to the following devices:

- SCALANCE W774-1 RJ45
- SCALANCE W734-1 RJ45

Note

You will find detailed information on the transmit power and receiver sensitivity in the document "Performance data 802.11 abgn SCALANCE W770/W730" on the supplied data medium (REF_W770-RadioInterface.pdf).

Technical specifications		
Data transfer		
Ethernet transfer rate		10 / 100 Mbps
Wireless transmission rate		1 ... 300 Mbps
Wireless standards supported		IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n
Power supply standards supported	Standards	IEEE 802.3at type 1 (802.3af) 802.3at type 2 (Power over Ethernet)
	Class	Class 2 *)
	Mode	Mode A (phantom power)
Attachment to Industrial Ethernet		
	Quantity	2
	Design	RJ-45 jack
	Properties	Half duplex/full duplex, autocrossover, autonegotiation, autosensing, PoE, floating

Technical specifications		
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		
Antenna connector	Quantity	2
	Design	R-SMA female
	Impedance	50 Ω nominal
Frequency range		2412 ... 2480 MHz 4920 ... 5875 MHz
Electrical data		
Direct 24 VDC supply	Supply voltage from terminal block	24 V DC safety extra low voltage (SELV)
	Permitted range	19.2 to 28.8 VDC
	Design	Terminal block, 4 terminals
	Properties	Electrically isolated, redundant design PoE to 24 VDC non-redundant design
Supply voltage from PoE	Supply voltage	48 VDC
	Permitted range	36 to 57 VDC
Fusing		2 A / 24 VDC
		1 A / 48 V DC PoE
Current consumption	At 24 VDC / typical	250 mA
	With PoE / typical	125 mA
Power loss at 24 VDC	At 24 VDC / typical	6 W
	With PoE / typical	6 W
Permitted ambient conditions		
Ambient temperature	During operation with the rack installed horizontally / vertically	-20 °C to +60 °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. 60 ° C ambient temperature
Contaminant concentration		According to IEC 60721
Degree of protection		
	IP code	IP30

Technical specifications		
Dimensions and weight		
Dimensions	W x H x D	26 x 156 x 127 mm (height without antenna connector 147 mm)
Weight		520 g
Installation options		
Direct	Wall mounting	
With additional holding plate	Mast mounting Mounting on a DIN rail Mounting on an S7-300 standard rail Mounting on an S7-1500 standard rail	
Mean time between failure (MTBF)		
	at 40 ° C ambient temperature	61.85 years

*) The PoE class depends on the hardware version of the device. Devices with a hardware version ≥ 3 have PoE class 2. Devices with a lower hardware version have PoE class 3.

9.2 SCALANCE W774 M12

The following technical specifications apply to the following devices:

- SCALANCE W774-1 M12 EEC

Note

You will find detailed information on the transmit power and receiver sensitivity in the document "Performance data 802.11 abgn SCALANCE W770/W730" on the supplied data medium (REF_W770-RadioInterface.pdf).

Technical specifications		
Data transfer		
Ethernet transfer rate		10 / 100 Mbps
Wireless transmission rate		1 ... 300 Mbps
Wireless standards supported		IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n
Power supply standards supported	Standards	IEEE 802.3at type 1 (802.3af) 802.3at type 2 (Power over Ethernet)
	Class	Class 2 *)
	Mode	Mode A (phantom power)

Technical specifications			
Attachment to Industrial Ethernet			
	Quantity		2
	Design		M12 socket
	Properties		Half duplex/full duplex, autocrossover, autonegotiation, autosensing, PoE, 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			
Antenna connector	Quantity		2
	Design		R-SMA female
	Impedance		50 Ω nominal
Frequency range			2412 … 2480 MHz 4920 … 5875 MHz
Electrical data			
Direct 24 VDC supply	Supply voltage from socket		24 V DC safety extra low voltage (SELV)
	Permitted range	+/- 20 %	19.2 to 28.8 VDC (meets UL requirements)
		+/- 30 %	16.8 to 31.2 VDC
	Design		M12 socket
	Properties		Electrically isolated, redundant design PoE to 24 VDC non-redundant design
Supply voltage from PoE	Supply voltage		48 VDC
	Permitted range		36 to 57 VDC
Fusing			2 A / 24 VDC
			1 A / 48 V DC PoE
Current consumption	At 24 VDC / typical		250 mA
	With PoE / typical		125 mA
Power loss at 24 VDC	At 24 VDC / typical		6 W
	With PoE / typical		6 W
Permitted ambient conditions			
Ambient temperature	During operation with the rack installed horizontally / vertically		-30 °C to +65 °C
	During storage		-40 °C to +85 °C

Technical specifications		
	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. 60 ° C ambient temperature
Contaminant concentration		According to IEC 60721
Degree of protection		
	IP code	IP30
Dimensions and weight		
Dimensions	W x H x D	26 x 156 x 127 mm (height without antenna connector 147 mm)
Weight		520 g
Installation options		
Direct	Wall mounting	
With additional holding plate	Mast mounting Mounting on a DIN rail Mounting on an S7-300 standard rail Mounting on an S7-1500 standard rail	
Mean time between failure (MTBF)		
	at 40 ° C ambient temperature	61.85 years

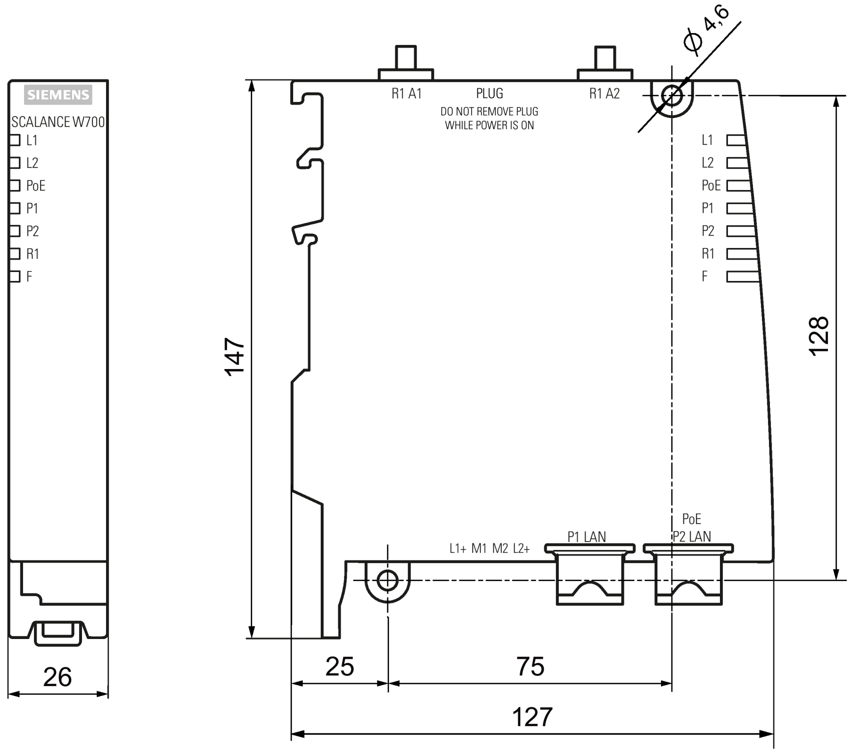
*) The PoE class depends on the hardware version of the device. Devices with a hardware version ≥ 2 have PoE class 2. Devices with a lower hardware version have PoE class 3.

Dimension drawings

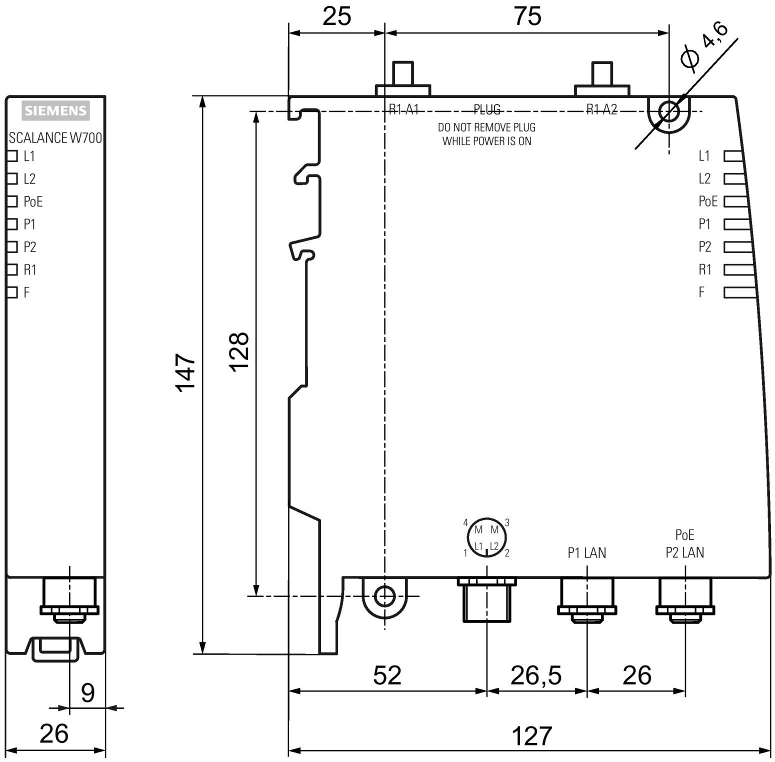
10

The following dimensions are specified in mm.

SCALANCE W774/734 RJ45



SCALANCE W774 M12 EEC



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/gb/en/)
- Using the search function at Industrial communication (https://support.industry.siemens.com/cs/gb/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 cables, 24
Antennas, 24
    Connectors, 54
    Directional antenna, 27
    Dual directional antenna with linear polarization, 27
    Dual-band directional antenna with linear polarization, 28
    Helical antenna, 27
    MIMO antenna, 28
    Omnidirectional antenna, 27
Article numbers, 5
Assembly
    DIN rail, 43
    S7-1500 standard rail, 42
    S7-300 standard rail, 41
    Wall mounting, 39

C

Cables
    Permitted lengths, 67, 69
Configuration manuals, 64

D

Dimension drawings, 73
Documentation on the CD, 5
Documentation on the Internet, 5

E

Ethernet
    Connectors, 52
    PoE, 50

F

Factory defaults, 33, 63
Factory setting, 63

G

Grounding, 46

I

Interfaces, 67, 69

L

LED display, 29
Lightning protection, 45
Loading firmware, 32

P

Power over Ethernet, 50
Power supply, 50
Primary user (radar), 29

R

Reset button, 32
Reset device, 63
Resetting the device, 32
Restart of the device, 32

S

Safety extra low voltage, 46
Safety notices
    for installation, 37
    general, 9
    Use in hazardous areas, 9, 37, 45
    when connecting up, 45
Scope of delivery, 21
Service & Support, 6

T

Technical specifications, 67, 69
Training, 6
Type designations, 19