SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE W1788-x / W1748-1

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

Troubleshooting 8

Technical specifications 9

Dimension drawings 10

Approvals 11

03/2023
C79000-G8976-C484-08

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-C484-08
Ⓟ 03/2023 Subject to change

Copyright © Siemens AG 2018 - 2023.
All rights reserved

Table of contents

1 Introduction 5

1.1 Purpose of the operating instructions 5

1.2 Supplementary documentation 5

1.3 Further documentation 6

1.4 Security information 6

1.5 Firmware 7

1.6 Error/fault 7

1.7 Decommissioning 7

1.8 Recycling and disposal 8

1.9 Marken 8

2 Safety notices 9

3 Security recommendations 11

3.1 Security recommendations 11

3.2 Available services 15

4 Description of the device 19

4.1 Structure of the type designation 19

4.2 Device views 20
4.2.1 SCALANCE W1788-1 / W1748-1 20
4.2.2 SCALANCE W1788-2 21
4.2.3 SCALANCE W1788-2IA 22

4.3 Components of the product 22

4.4 Accessories 23
4.4.1 Installation 23
4.4.2 CLP 24
4.4.3 Industrial Internet 24
4.4.4 Power supply 26
4.4.5 Flexible connecting cables, antennas and accessories 26
4.4.5.1 Flexible connecting cables 26
4.4.5.2 Lightning protection 27
4.4.5.3 Terminating resistor 28
4.4.5.4 Cabinet feedthrough 28
4.4.5.5 Antennas 28

4.5 LED display 30
4.5.1 SCALANCE W1788-1 / W1748-1 30
4.5.2 SCALANCE W1788-2 / W1788-2IA 34

4.6 Reset button 38

4.7 Configuration License PLUG ... 39
5 Installation and removal ... 41
5.1 Safety during mounting ... 41
5.2 Types of installation ... 44
5.3 Wall mounting ... 45
5.4 Installing on a DIN rail ... 50
5.5 Installing on a standard rail ... 52
6 Connection ... 57
6.1 Safety when connecting up ... 57
6.2 Power supply ... 62
6.3 Ethernet ... 65
6.4 Antenna ... 67
6.5 Grounding ... 70
6.6 Replacing a CLP ... 72
7 Maintenance and cleaning ... 75
8 Troubleshooting ... 77
8.1 Downloading new firmware using TFTP without WBM and CLI ... 77
8.2 Restoring the factory settings ... 78
9 Technical specifications ... 81
9.1 SCALANCE W1788-1 / W1748-1 ... 81
9.2 SCALANCE W1788-2 / W1788-2IA ... 83
10 Dimension drawings ... 87
10.1 SCALANCE W1788-x / W1748-1 ... 87
10.2 Mounting plate ... 88
11 Approvals ... 89
Index ... 91

Introduction 1

1.1 Purpose of the operating instructions

These operating instructions contain information with which you can install and connect the SCALANCE device correctly. The configuration and the integration of the device in a network are not described in these instructions.

Validity of the Operating Instructions

These operating instructions cover the following products:

	Article number	Certification ID
Access points		**Access points**
SCALANCE W1788-1 M12	6GK5788-1GY01-0AA0	RAPAC-W1-M12-E4
SCALANCE W1788-2 M12	6GK5788-2GY01-0AA0	RAPAC-W2-M12-E4
SCALANCE W1788-2 M12 EEC	6GK5788-2GY01-0TA0	RAPAC-W2-M12-E4
SCALANCE W1788-2IA M12	6GK5788-2HY01-0AA0	RAPAC-W2-M12-I4
Client		**Client**
SCALANCE W1748-1 M12	6GK5748-1GY01-0AA0	RAPAC-W1-M12-E4

These operating instructions apply to the following firmware version:

- SCALANCE W1700 as of Version 3.0

Definition

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

1.2 Supplementary documentation

Documentation on the Internet

You can find the current version of the document on the Internet at (https://support.industry.siemens.com/cs/de/en/ps/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 W1780/W1740 nach IEEE 802.11ac Web Based Management
- SCALANCE W1780/W1740 nach IEEE 802.11ac Command Line Interface

Note

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

1.3 Further documentation

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

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

You will find the system manuals here:

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

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

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

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

1.4 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).

1.5 Firmware

The firmware is available on the Internet pages of the Siemens Industry Online Support: (https://support.industry.siemens.com/cs/ww/en/ps/25169/dl)

Note on firmware/software support

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

1.6 Error/fault

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

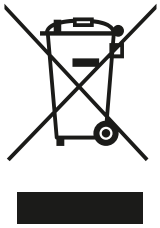
1.7 Decommissioning

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.

1.8 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.

1.9 Marken

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

SCALANCE, RCoax

Safety notices

2

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

Read the safety notices

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

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



⚠ WARNING
Hot surfaces
Electric devices have hot surfaces. Do not touch these surfaces. They could cause severe burns. • Allow the device to cool down before starting any work on it.

⚠ WARNING
EXPLOSION HAZARD
Do not open the device when the supply voltage is turned on.

Security recommendations

3

3.1 Security recommendations

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

General

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

WLAN

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

Authentication

Note

Accessibility risk - Risk of data loss

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

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

Certificates and keys

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

Physical/remote access

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

Hardware / Software

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

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

Secure/ non-secure protocols

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

- Check whether use of the following protocols and services is necessary:
  - Non-authenticated and unencrypted ports
  - LLDP
  - Syslog
  - DHCP options 66/67
  - TFTP
  - Telnet
  - HTTP
  - SNMP v1/2c
  - 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.

3.2 Available services

List of available services

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

The table includes the following columns:

- **Service**
  The services that the device supports
- **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	✓

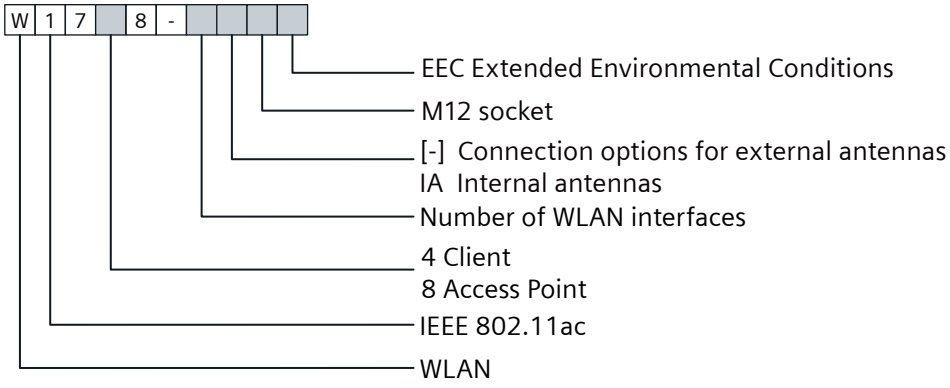
Description of the device

4

4.1 Structure of the type designation

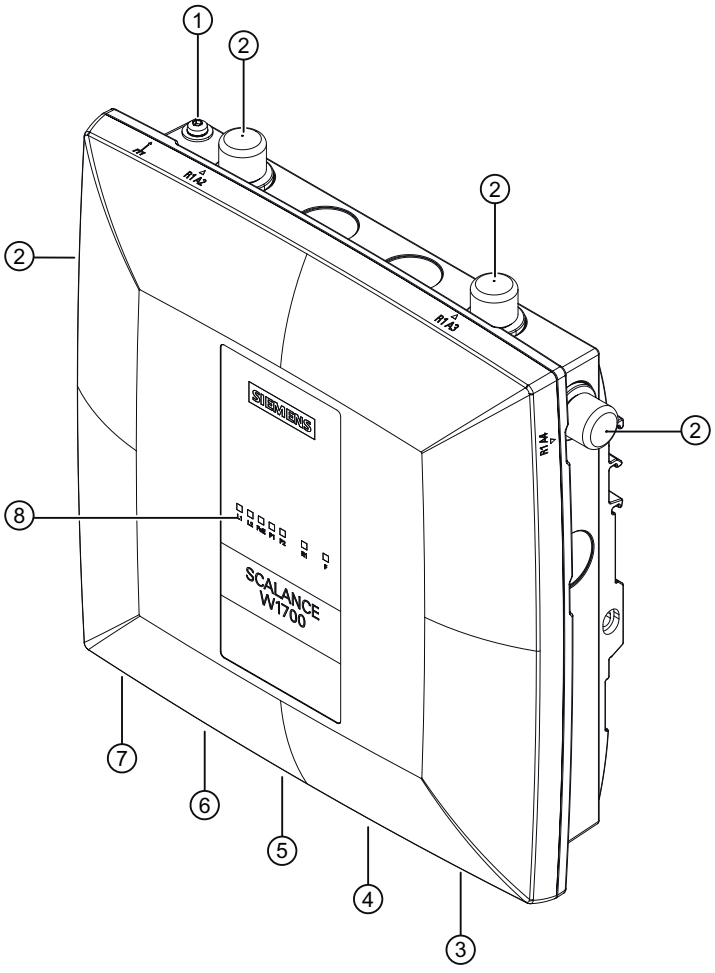
Structure of the type designation

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



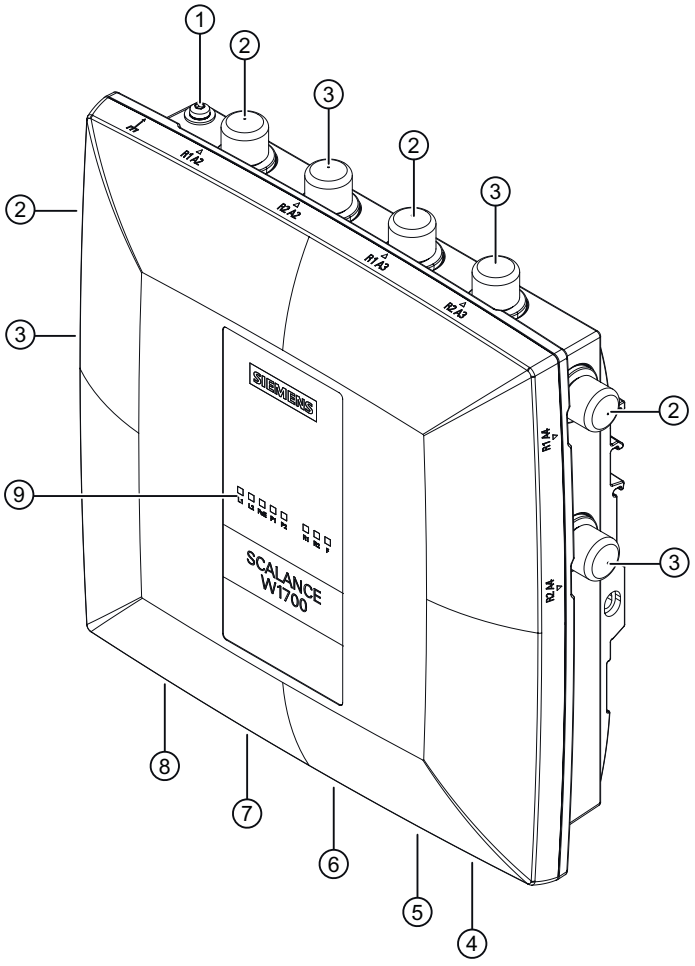
4.2 Device views

4.2.1 SCALANCE W1788-1 / W1748-1



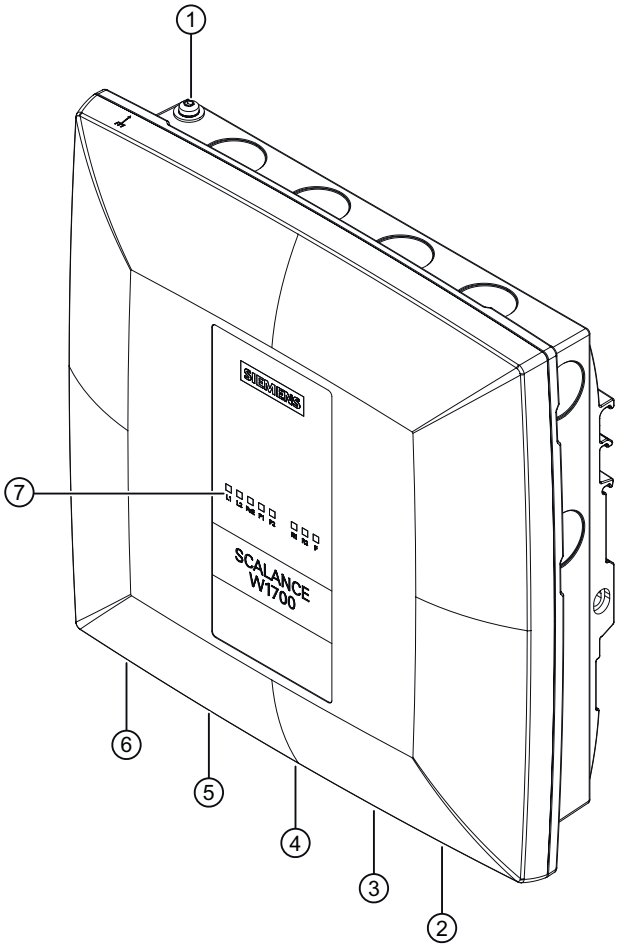
① Ground connector (thread M4) on the top
② R1 antenna port, female N-Connect type
Two connectors on the top and one each on the right and left side
③ Ground connector (thread M4) on the bottom, covered
④ Connector for power supply (L1, L2), covered
⑤ Ethernet connector P2 (PoE capability), covered
⑥ Ethernet connector P1, covered
⑦ Screw-down cover, covered
- for the reset button and
- for the PLUG slot (CLP)
⑧ LED display

4.2.2 SCALANCE W1788-2



① Ground connector (thread M4) on the top
② R1 antenna port, female N-Connect type
Two connectors on the top and one each on the right and left side
③ R2 antenna port, female N-Connect type
Two connectors on the top and one each on the right and left side
④ Ground connector (thread M4) on the bottom, covered
⑤ Connector for power supply (L1, L2), covered
⑥ Ethernet connector P2 (PoE capability), covered
⑦ Ethernet connector P1, covered
⑧ Screw-down cover, covered
- for the reset button and
- for the PLUG slot (CLP)
⑨ LED display

4.2.3 SCALANCE W1788-2IA



① Ground connector (thread M4) on the top
② Ground connector (thread M4) on the bottom, covered
③ Connector for power supply (L1, L2), covered
④ Ethernet connector P2 (PoE capability), covered
⑤ Ethernet connector P1, covered
⑥ Screw-down cover, covered
- for the reset button and
- for the PLUG slot (CLP)

⑦ LED display

4.3 Components of the product

The following components are supplied with the product:

- A SCALANCE device with pre-installed bracket for securing to a DIN rail
- Two grounding screws

- One cover for PLUG slot
- Three protective caps for the M12 sockets
  - 2 x Ethernet
  - 1 x power supply
- Protective caps for the antenna sockets:
  - 4 x for SCALANCE W1788-1 / W1748-1
  - 8 x for SCALANCE W1788-2

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

Note

Not included with the product

The following components do not ship with the product:

- Removable data storage medium CLP
- Antennas
- Wall mounting set
- Bracket set for securing the device on a standard rail

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

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/mall/en/WW/Catalog/Products/10021486)

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

4.4.1 Installation

Component	Description	Article number
Installation kit for installation on a mounting rail	Bracket set for securing the device on a standard rail • S7-300 standard rail • S7-1500 standard rail Mounting adapter with fixing screws	6GK5798-8MS00-0AA0
Wall mounting set	Installation kit for mounting the device to the wall or ceiling; mounting plate, fixing and locking screws	6GK5798-8MW00-0AA0

4.4.2 CLP

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

4.4.3 Industrial Internet

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

Cables Industrial Ethernet (pre-assembled)

Component	Description	Article number
IE TP Cord M12-180/M12-180	IE Flexible Cable with two M12 plugs (X-coded)	
	Length 0.3m	6XV1878-5HE30
	Length 0.5m	6XV1878-5HE50
	Length 1m	6XV1878-5HH10
	Length 1.5m	6XV1878-5HH15
	Length 2m	6XV1878-5HH20
	Length 3m	6XV1878-5HH30
	Length 5m	6XV1878-5HH50

Cables Industrial Ethernet (sold by the meter)

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

M12 plug-in connector Industrial Ethernet

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

4.4.4 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 mm², 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 mm², 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

4.4.5 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).

4.4.5.1 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

4.4.5.2 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

4.4.5.3 Terminating resistor

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

4.4.5.4 Cabinet feedthrough

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

4.4.5.5 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 (7 dBi at 2.4 GHz and 5 dBi at 5 GHz).

Antennas

Type	Properties	Article number
ANT792-4DN	RCoax helical antenna, circular polarization, 4 dBi, 2.4 GHz, N-Connect female.	6GK5792-4DN00-0AA6
ANT792-6MN	Omni antenna, mast/wall mounting, 6 dBi 2.4 GHz, N-Connect female	6GK5792-6MN00-0AA6
ANT792-8DN	Directional antenna, mast/wall mounting, 14 dBi 2.4 GHz, N-Connect female	6GK5792-8DN00-0AA6
ANT793-6DG	Wide angle antenna, mast/wall mounting, 9 dBi 5 GHz, 2 x N-Connect female	6GK5793-6DG00-0AA0
ANT793-8DJ	Directional antenna, mast/wall mounting, 18 dBi 5 GHz, 2 x N-Connect female	6GK5793-8DJ00-0AA0

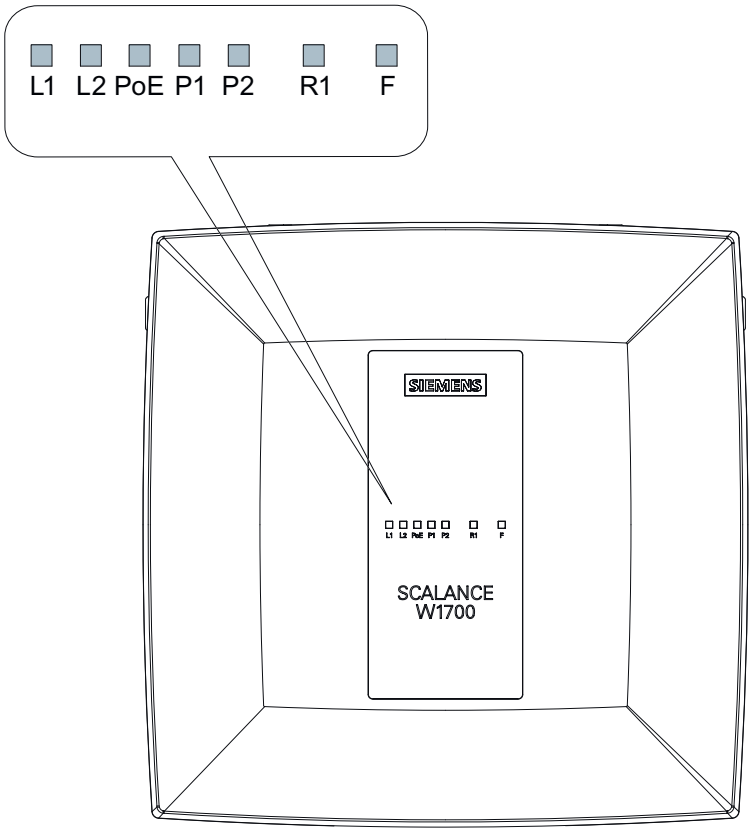
Type	Properties	Article number
ANT793-8DK	Directional antenna, mast/wall mounting, 23 dBi 5 GHz, 2 x N-Connect female	6GK5793-8DK00-0AA0
IWLAN RCoax ANT793-4MN	RCoax λ4 antenna with vertical polarization for RCoax systems, 6 dBi, 5 GHz, IP65, N-Connector female	6GK5793-4MN00-0AA6
ANT795-4MC	Omnidirectional antenna, 3/5 dBi, 2.4 GHz and 5 GHz, IP65, N-Connect male for direct installation on the device, straight connector.	6GK5795-4MC00-0AA3
ANT795-4MD	Omnidirectional antenna, 3/5 dBi, 2.4 GHz and 5 GHz, IP65, N-Connect male for direct installation on the device, 90° connector.	6GK5795-4MD00-0AA3
ANT795-6DC	Wide angle antenna, mast/wall mounting, 9 dBi 2.4 GHz and 5 GHz, N-Connect female	6GK5795-6DC00-0AA0
ANT795-6MN	Omni antenna, mounted on roof/vehicle, 6/8 dBi 2.4 GHz and 5 GHz, N-Connect female	6GK5795-6MN10-0AA6
ANT793-8DL	Directional antenna vertical-horizontal polarized, 5 GHz, 14dBi, IP66, 2 x N-Connector female	6GK5793-8DL00-0AA0
ANT793-8DP	Directional antenna, mast/wall mounting, 13 / 13.5 dBi 4.9 GHz and 5 GHz, N-Connect female	6GK5793-8DP00-0AA0
ANT795-4MX	Omnidirectional antenna, 2/2.5 dBi, 2.4 GHz and 5 GHz, IP69K, N-Connector male	6GK5795-4MX00-0AA0
ANT795-6MP	Omnidirectional antenna, 5/7 dBi, 2.4 GHz and 5 GHz, IP65/67, N-Connector female	6GK5795-6MP00-0AA0
ANT897-4ME	Omnidirectional antenna for public 3/4/5G mobile wireless networks and private 5G networks worldwide; 2 ... 6 dBi, 0.6 ... 6 GHz, IP65, N-Connector female	6GK5897-4ME00-0AA0
IWLAN RCoax Cable 2,4 GHz PE 1/2"	Omni antenna, 0 dBi 2.400 - 2.485 GHz, N-Connect female	6XV1875-2A
IWLAN RCoax Cable 5 GHz PE 1/2"	Omni antenna, 0 dBi 5.150 – 5.875 GHz, N-Connect female	6XV1875-2D

4.5 LED display

4.5.1 SCALANCE W1788-1 / W1748-1

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.

LED	Color	Meaning
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.
	Flashing green  Interval: 170 ms on / 170 ms off	The port has the status "Discarding" in the spanning tree. The port is part of a spanning tree, however it is located on a redundant path and is blocked for data traffic.
P2	Off 	There is no connection over the Ethernet port P2.
	Green 	There is a connection over the Ethernet port P2 (link).
	Flashing green and yellow 	Data transfer over the Ethernet interface P2.
	Flashing green  Interval: 170 ms on / 170 ms off	The port has the status "Discarding" in the spanning tree. The port is part of a spanning tree, however it is located on a redundant path and is blocked for data traffic.

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 	*Client mode:* The client is searching for a connection to an access point.
	Flashing green and yellow 	Data transfer via the WLAN interface 1.
	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.

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: 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 green 	The port LEDs flash for detection of device location. The "LED flash" function is activated • Either with SINEC PNI • Or via the WBM page "Discovery and Set via DCP"

Note

Primary user (radar) on all enabled channels

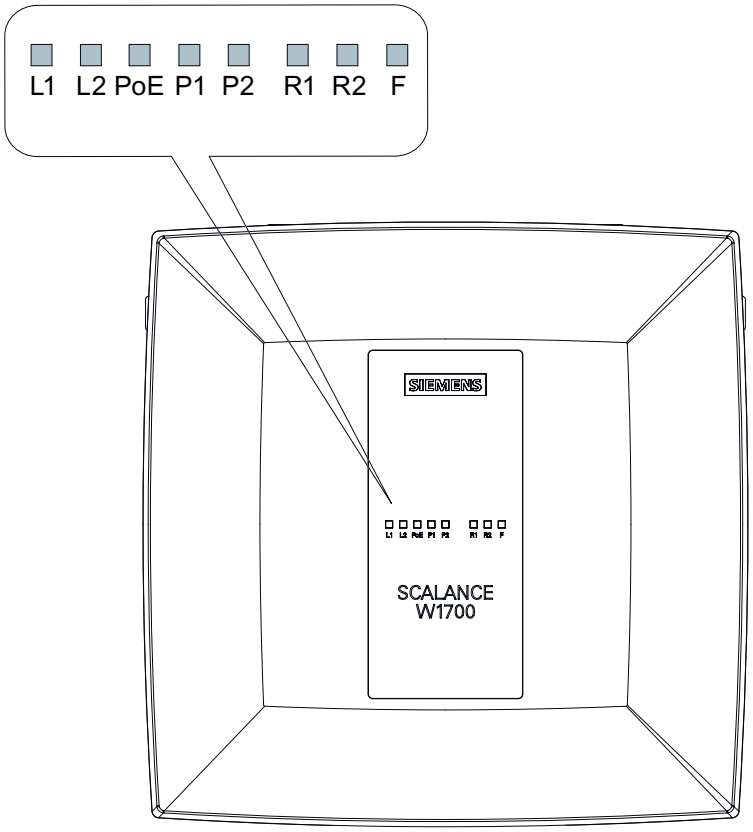
If the device detects competing radar signals on all enabled channels of the WLAN interface, the **F** LED is lit and **R1** flash. No data traffic is then possible for the next 30 minutes. After this time, the device runs the scan again and checks whether a primary user still exists. If no primary user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

4.5.2 SCALANCE W1788-2 / W1788-2IA

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.

LED	Color	Meaning
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.
	Flashing green  Interval: 170 ms on / 170 ms off	The port has the status "Discarding" in the spanning tree. The port is part of a spanning tree, however it is located on a redundant path and is blocked for data traffic.
P2	Off 	There is no connection over the Ethernet port P2.
	Green 	There is a connection over the Ethernet port P2 (link).
	Flashing green and yellow 	Data transfer over the Ethernet interface P2.
	Flashing green  Interval: 170 ms on / 170 ms off	The port has the status "Discarding" in the spanning tree. The port is part of a spanning tree, however it is located on a redundant path and is blocked for data traffic.

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 	*Client mode:* The client is searching for a connection to an access point.
	Flashing green and yellow 	Data transfer via the WLAN interface 1.
	Flashing yellow  Interval: 100 ms on / 100 ms off	*Access point mode:* With DFS (802.11h), the channel is scanned for one minute for competing radar signals before the channel can be used for data traffic.
R2	Off 	The WLAN interface 2 is deactivated. *Client mode:* The LED is always off because WLAN interface 2 is not available in client mode.
	Green 	*Access point mode:* The WLAN interface 2 is initialized and ready for operation.
	Flashing green and yellow 	*Access point mode:* Data transfer via the WLAN interface 2.
	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.

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: 2000 ms on / 200 ms off	Firmware on PLUG: The device is performing a firmware update or downgrade.
	Red  Simultaneous R1/R2 yellow flashing 	A competing radar signal was found on all enabled channels.
P1 P2 R1 R2	Flashing green 	The port LEDs flash for detection of device location. The "LED flash" function is activated • Either with SINEC PNI • Or via the WBM page "Discovery and Set via DCP"

Note

Primary user (radar) on all enabled channels

If the device detects a competing radar signal on all enabled channels of the WLAN interfaces, the **F** LED is lit and **R1**/**R2** 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.

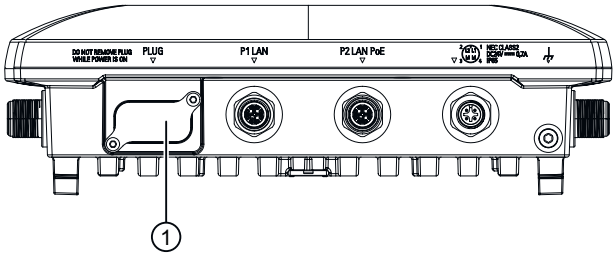
The wait time of 30 minutes is necessary due to legal requirements and cannot be shortened even by restarting the device.

4.6 Reset button

Position

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

The Reset button ① is located behind the screw-down cover on the underside of the housing.



① PLUG slot with the reset button (covered)

Functions

The reset button has the following functions:

- **Restart of the device**
  To restart the device, press the Reset button briefly.

  Note

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

- **Loading new firmware**
  If the normal procedure with the "Load & Save" menu of Web Based Management is unsuccessful, the reset button can be used to load new firmware. This situation can occur if there is a power outage during the normal firmware update. For more detailed information, refer to section "Upkeep and maintenance (Page 77)".
- **Restoring the default parameters (factory defaults)**
  For more detailed information, refer to section "Upkeep and maintenance (Page 77)".

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 a configured network with further consequences.

4.7 Configuration License PLUG

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

The PLUG is available in the following variants:

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

NOTICE
Loss of the degree of protection When the cover is not mounted correctly, the device loses its degree of protection IP65 and is not water and dust proof.

Position

The CLP slot is at the bottom of the device enclosure under a cover, see Reset button (Page 38).

Function

Devices with a CLP slot support the following operating modes:

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

    Note

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

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

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

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

The procedure for inserting and removing the CLP can be found in the section "Replacing a CLP (Page 72)".

Installation and removal

5

5.1 Safety during mounting

Safety notices

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

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

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

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

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

⚠ WARNING
The device is intended for indoor use only.

WARNING

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

WARNING

EXPLOSION HAZARD

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

WARNING

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

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

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

WARNING

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

Safety notices when using according to FM

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

WARNING

EXPLOSION HAZARD

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

WARNING

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

WARNING

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

WARNING

The IP65 marking is not associated with FM approval.

Note

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

WARNING

Substitution of components may impair suitability for Division 2.

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

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

WARNING

Open equipment

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

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

WARNING

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

WARNING

Improper disassembly

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

For proper disassembly, observe the following:

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

5.2 Types of installation

Note

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

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

For the device the following types of installation are permitted:

- Wall mounting
- Ceiling mounting
- Mounting on a DIN rail
- Mounting on an S7-300 or S7-1500 mounting rail

CAUTION

Danger of injury by falling objects

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

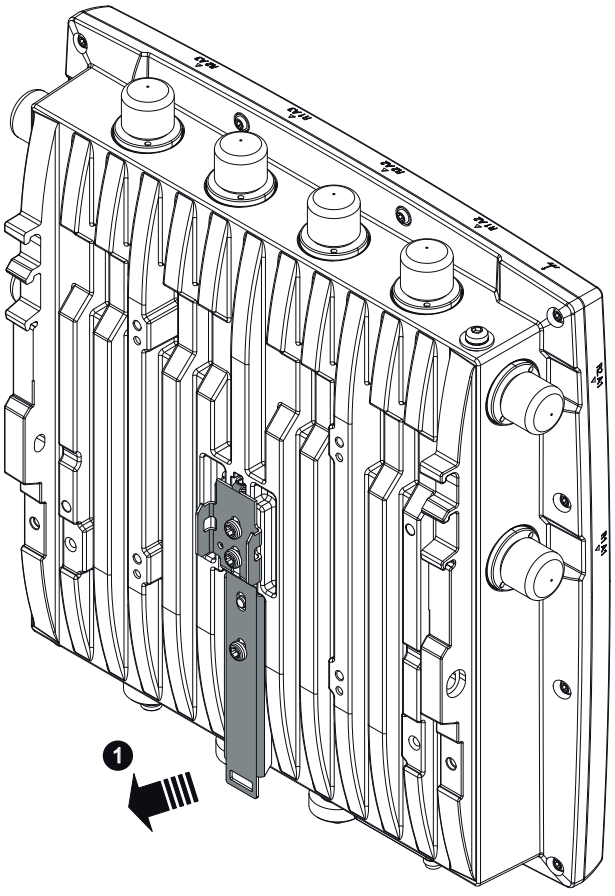
In this case, install the device on a wall.

5.3 Wall mounting

The wall mounting kit for wall mounting is not included with the product, see accessories. (Page 23)

Installation

1. Unscrew the bracket pre-installed at the factory for securing to a DIN rail from the device and remove it ❶.



2. Prepare the four drill holes for wall mounting. For the precise dimensions, refer to the section "Dimension drawings (Page 87)".
   Secure the mounting plate to the wall with four screws ❷. Note the direction of the holding plate ("TOP").

Note

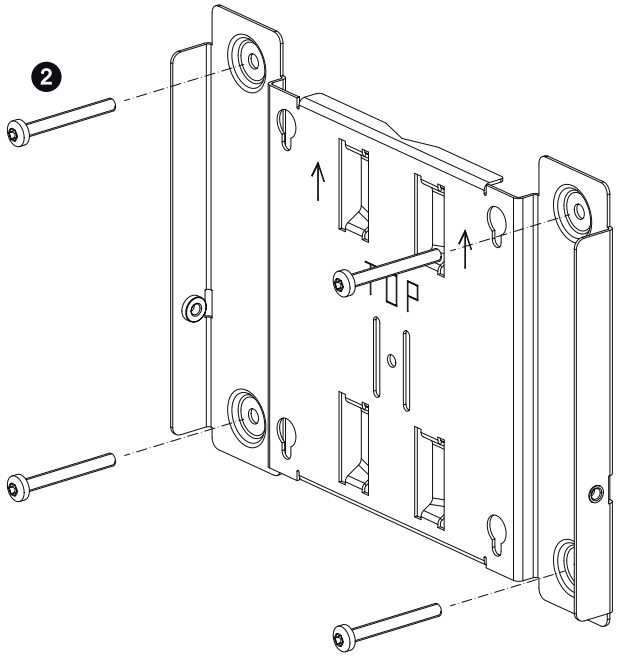
Depending on the mounting surface, use suitable fittings.

Note

The holding plate must be securely fastened

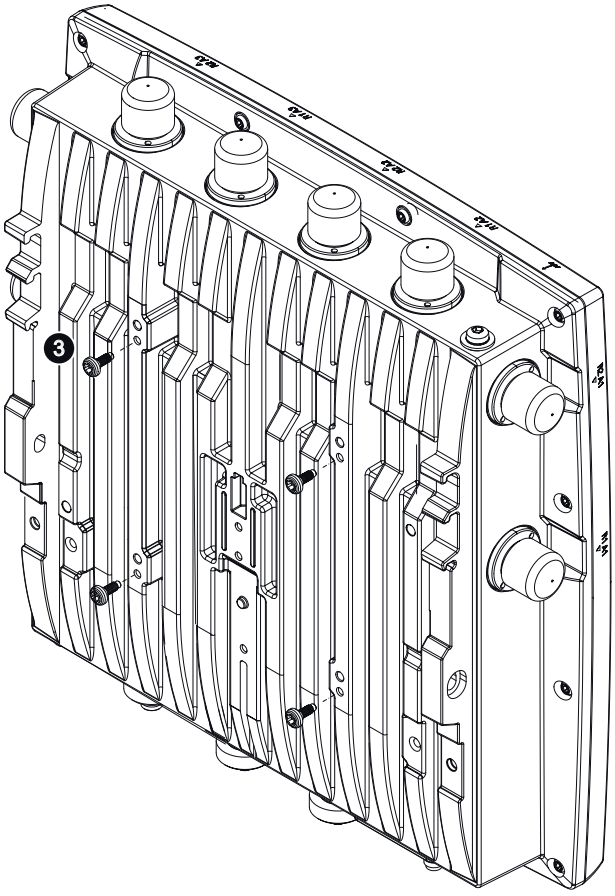
If the holding plate is not securely fastened, the holding plate may fall with the device.

The mounting material must be capable of supporting at least four times the weight of the device and the holding plate.

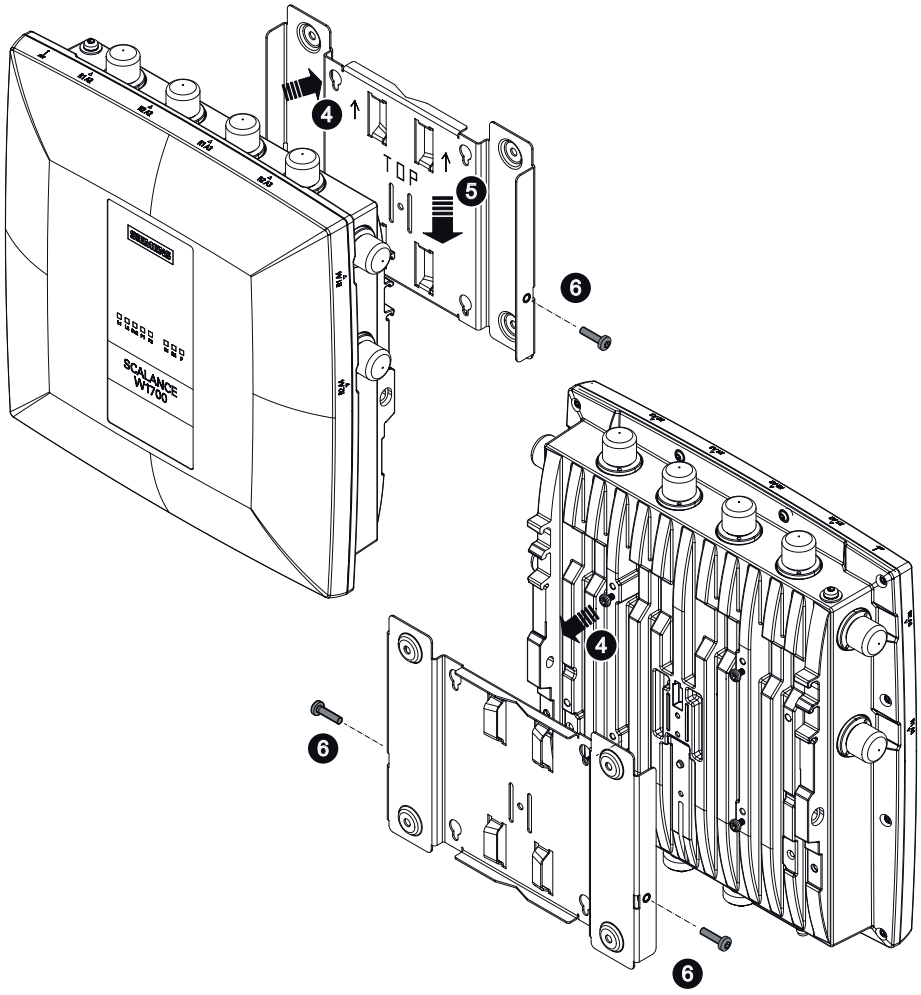


The mounting plate has four key-hole brackets for hanging up the device. The mounting material for securing to the base is not supplied with the product; see Accessories. (Page 23)

3. Screw the self-tapping M3 head screws into the device ❸ as far as they will go. The tightening torque is 1.2 Nm.



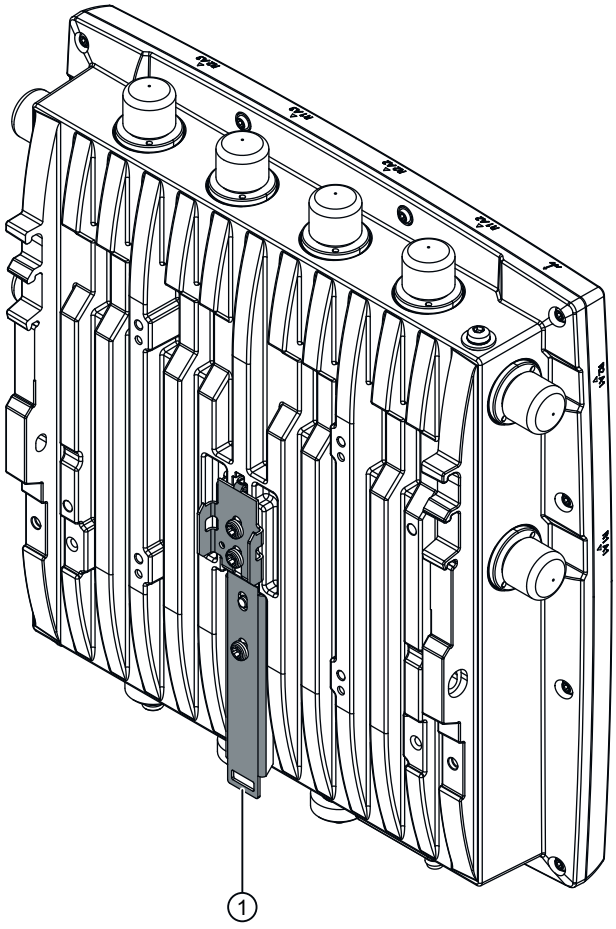
4. Insert the device with the screwed-in head screws into the four key-hole brackets of the mounting plate ❹. Make sure that the head screws are correctly positioned in the key-hole brackets.



5. Pull the inserted device down ❺ until it sits firmly in the key-hole brackets.
6. Secure the device to the holding plate on the side with two screws ❻. The tightening torque is 1.8 Nm.
7. Connect the power supply, refer to the section "Power supply (Page 62)".
8. Fit the antennas, refer to the section "Antennas (Page 67)".

5.4 Installing on a DIN rail

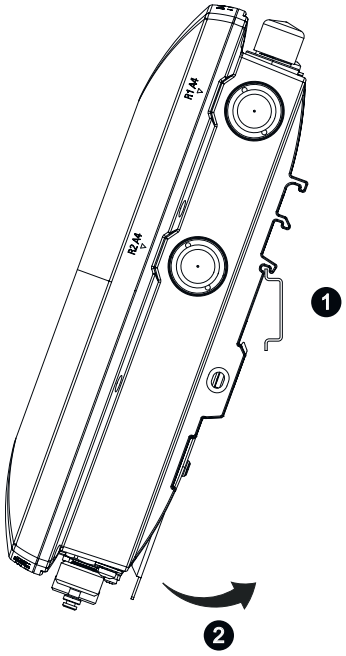
The bracket for securing to a DIN rail is pre-installed on the device in the factory settings.



① Bracket for securing to a DIN rail

Installation

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

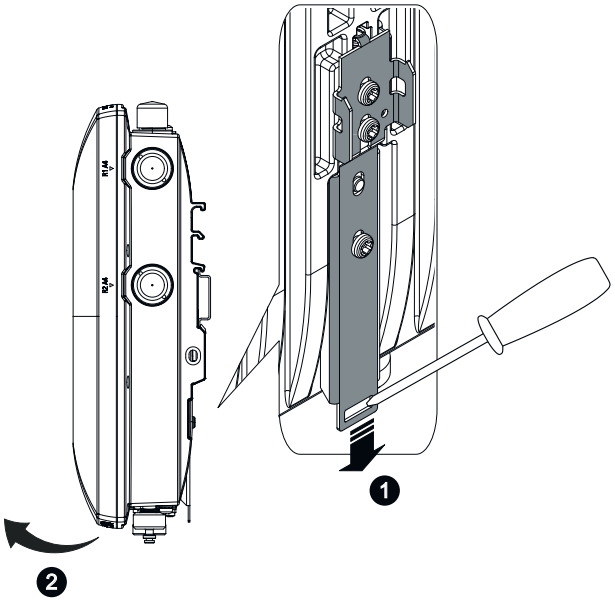


3. Connect the power supply, refer to the section "Power supply (Page 62)".
4. Fit the antennas, refer to the section "Antennas (Page 67)".

Uninstalling

1. Turn off the power to the device.
2. Disconnect all connected cables.

3. Pull the bracket down with a screwdriver ❶.



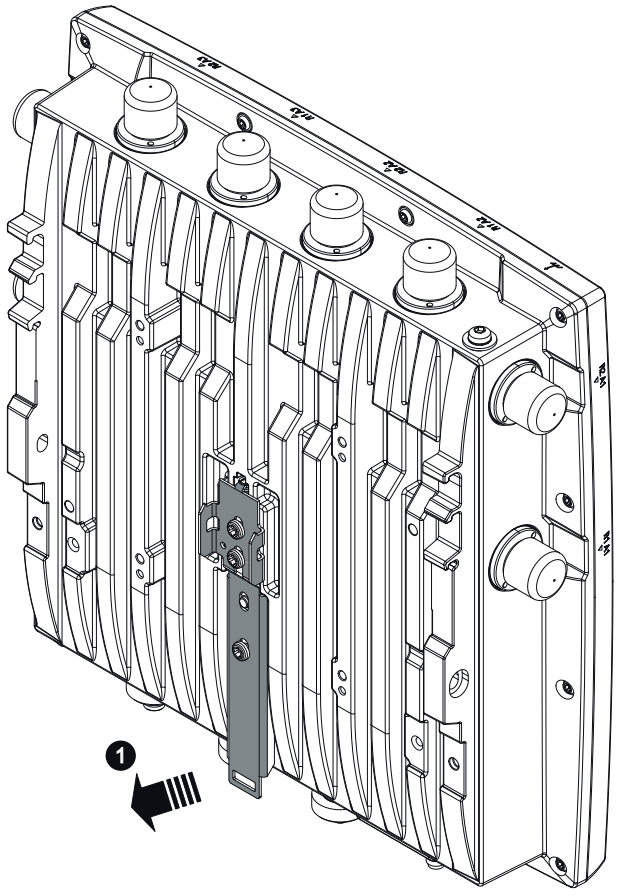
4. Swivel the device away from the DIN rail ❷and remove it from the DIN rail.

5.5 Installing on a standard rail

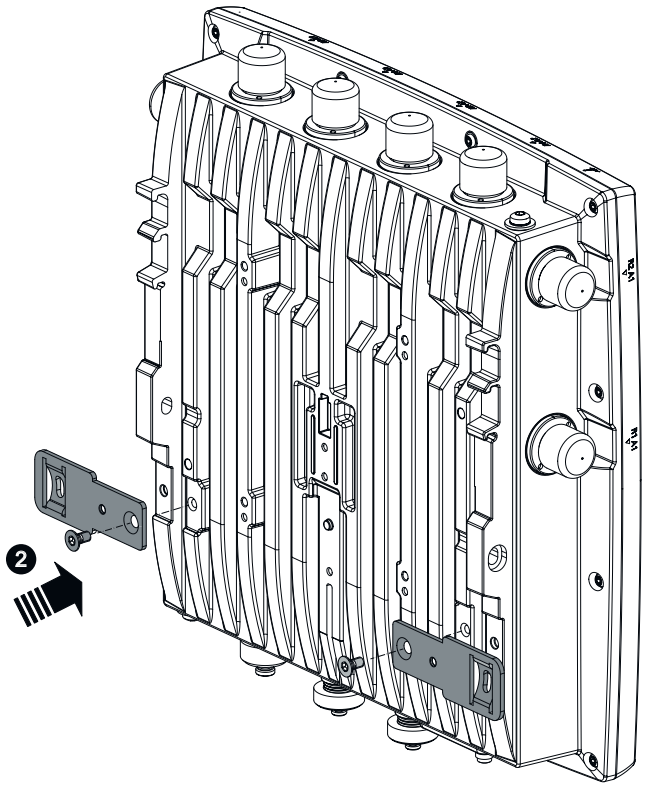
The mounting adapters and the corresponding screws are not supplied with the product; see "Accessories" (Page 23).

Installation

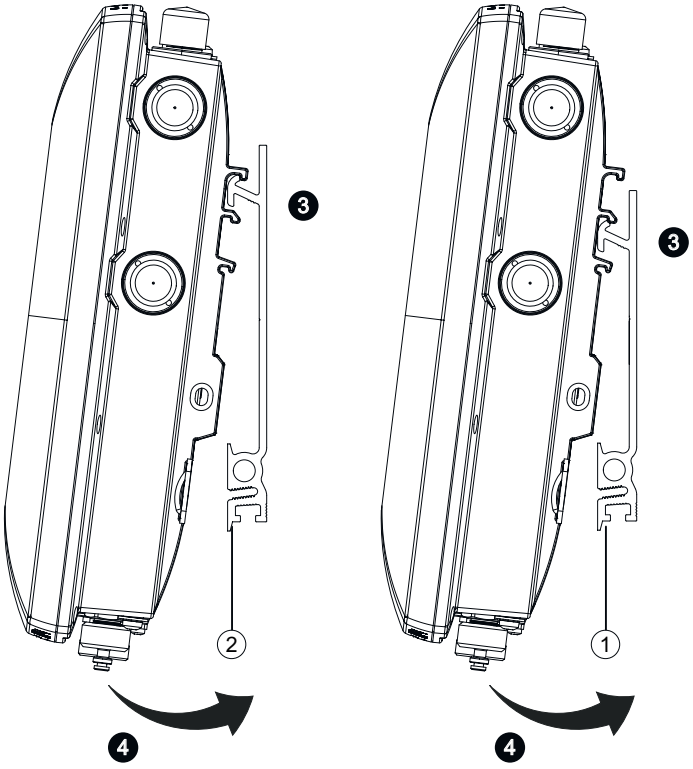
1. Unscrew the bracket pre-installed at the factory for securing to a DIN rail from the device and remove it ❶.



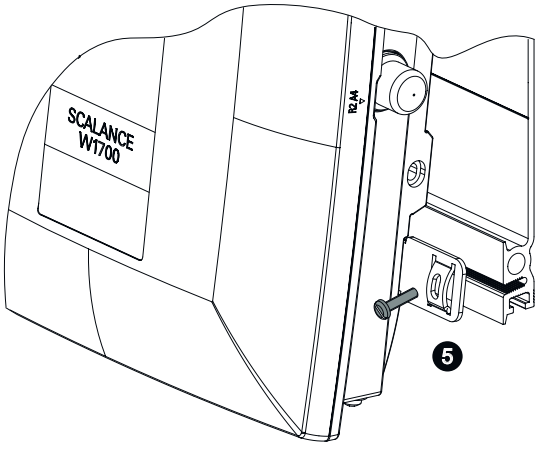
2. Secure the two mounting adapters with one M4 countersunk screw each to the device ❷. The tightening torque is 1.8 Nm.


2

3. Place the device on the upper edge of the corresponding mounting rail ❸:
   - ① S7-300 standard rail
   - ② S7-1500 standard rail



4. Swing the device to the standard rail ❹.
5. Screw the mounting adapters to the standard rail ❺ on both sides. The screws needed for this are supplied with the bracket set; see "Installation (Page 23)".



6. Connect the power supply, refer to the section "Power supply (Page 62)".
7. Fit the antennas, refer to the section "Antennas (Page 67)".

Uninstalling

1. Turn off the power to the device.
2. Disconnect all connected cables.
3. Loosen the screws of the mounting adapters completely from the standard rail.
4. Remove the device from the standard rail.
5. Loosen the screws of the mounting adapters completely from the device.

Connection

6

6.1 Safety when connecting up

Safety notices

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

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.

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 27) of SIMATIC NET Industrial WLAN.

Note

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

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



⚠ WARNING

Danger due to lightning strikes

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

Note

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

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

Supply voltage

⚠ WARNING

Power supply

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

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

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

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

Grounding



⚠ WARNING

Danger to life from overvoltage, fire hazard

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

NOTICE

Damage to the device due to potential differences

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

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

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

WARNING

EXPLOSION HAZARD

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

WARNING

EXPLOSION HAZARD

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

WARNING

Unsuitable cables or connectors

Risk of explosion in hazardous areas

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

WARNING

Lack of equipotential bonding

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

- Ensure that equipotential bonding is available for the device.

WARNING

Unprotected cable ends

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

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

WARNING

Improper installation of shielded cables

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

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

WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

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

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

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

WARNING

Transient overvoltages

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

WARNING

Suitable cables at high ambient temperatures in hazardous area

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

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

Do not remove or replace while circuit is live when a flammable or combustible atmosphere is present.

WARNING

Impermissible accessories

For connection to the SCALANCE W device, use only the cables and connectors listed in the "Accessories (Page 23)" section.

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

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

WARNING

WARNING - EXPLOSION HAZARD -

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

WARNING

Restricted area of application

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

WARNING

Restricted area of application

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

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

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

NOTICE
Suitable fusing for the power supply cable The current at the connecting terminals must not exceed 3 A. Use a fuse for the power supply that protects against currents > 3 A. • In areas where NEC or CEC are used, the following requirements must be met: – Suitable for DC (min. 60 V / max. 3 A) – Breaking current min. 10 kA – UL/CSA listet (UL 248-14 / CSA 22.2 No. 248.14) – Classes R, J, L, T or CC • In other areas, the following requirements must be met: – Suitable for DC (min. 60 V / max. 3 A) – Breaking current min. 10 kA – Permitted for electric circuits according to IEC / EN 60947-1/2/3 – Breaking characteristics: B or C for circuit-breakers or fuses You do not need a fuse for the power supply cable if you use a voltage source according LPS or NEC Class 2.

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

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

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.

Note

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

Information on the power supply

There are two options for the power supply:

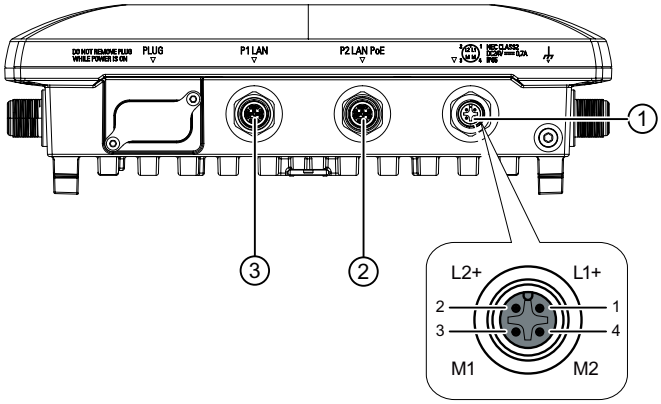
- Direct infeed via the 4-pin M12 socket ①
  The power supply can be connected redundantly. The inputs L1/L2 are decoupled There is no distribution of load. The power supply unit with the higher output voltage supplies the device alone.
- Power over Ethernet via the 8-pin M12 Ethernet interface P2 ②
  The power supply cannot be connected redundantly.

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

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

To connect the functional ground, use a copper cable of category 20 AWG or a cable with a cross-section ≥ 0.75 mm^2.

Position and pin assignment



① M12 interface, direct feed in, A-coded, 4-pin

② M12 Ethernet port P2 LAN PoE, X-coded, 8-pin
The power can also be supplied via this interface (Power over Ethernet).
Pin assignment, see Ethernet (Page 65)

③ M12 Ethernet port P1 LAN, X-coded, 8-pin

The four-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

Connecting/disconnecting the power supply

⚠ WARNING

Danger from electric shock

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

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

Power over Ethernet (PoE)

With PoE, the power for networked devices is carried via Ethernet.

- Mode A (Gigabit Ethernet)
  Power is transferred on the data wires 1, 2, 3 and 6 of the Ethernet cable.
- Mode B (Fast Ethernet)
  Power is transferred on the free wires 4, 5, 7 and 8 of the Ethernet cable.

Note

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

Note

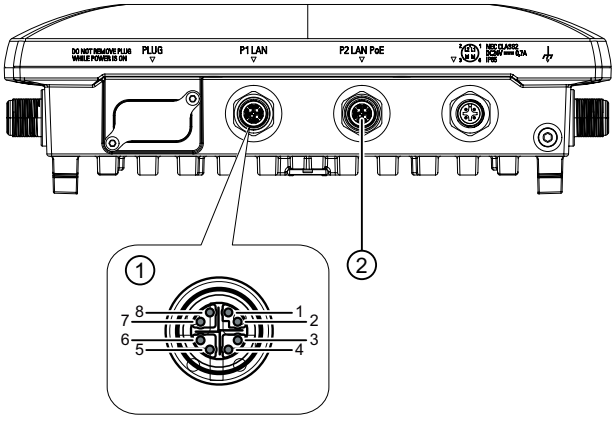
No power sourcing equipment (PSE)

The device cannot be used as a PoE power supply for other devices.

6.3 Ethernet

For connection to Industrial Ethernet at 10/100/1000 Mbps, the devices have the following two M12 interfaces: X-coded, 8-pin.

Position and pin assignment



① M12 interface P1 LAN

② M12 interface P2 LAN PoE
The power can also be supplied via this interface (Power over Ethernet).

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

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

Pin	Assignment
7	D2-
8	D2+

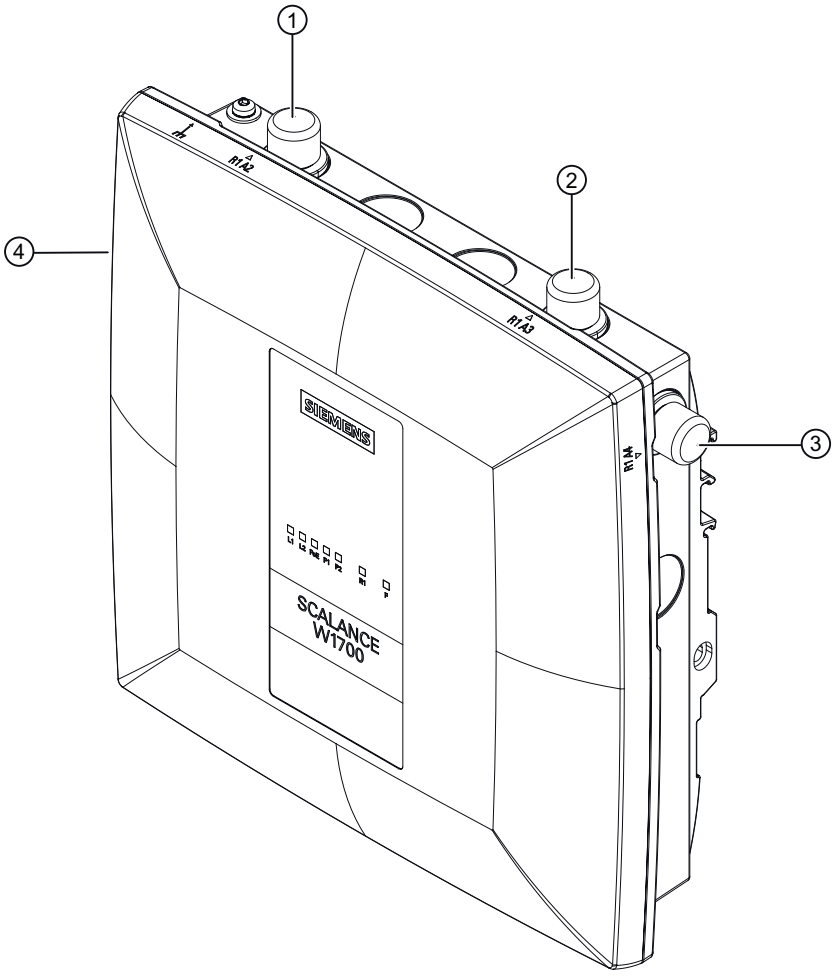
Connecting Ethernet ports

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

6.4 Antenna

SCALANCE W1788-1/W1748-1

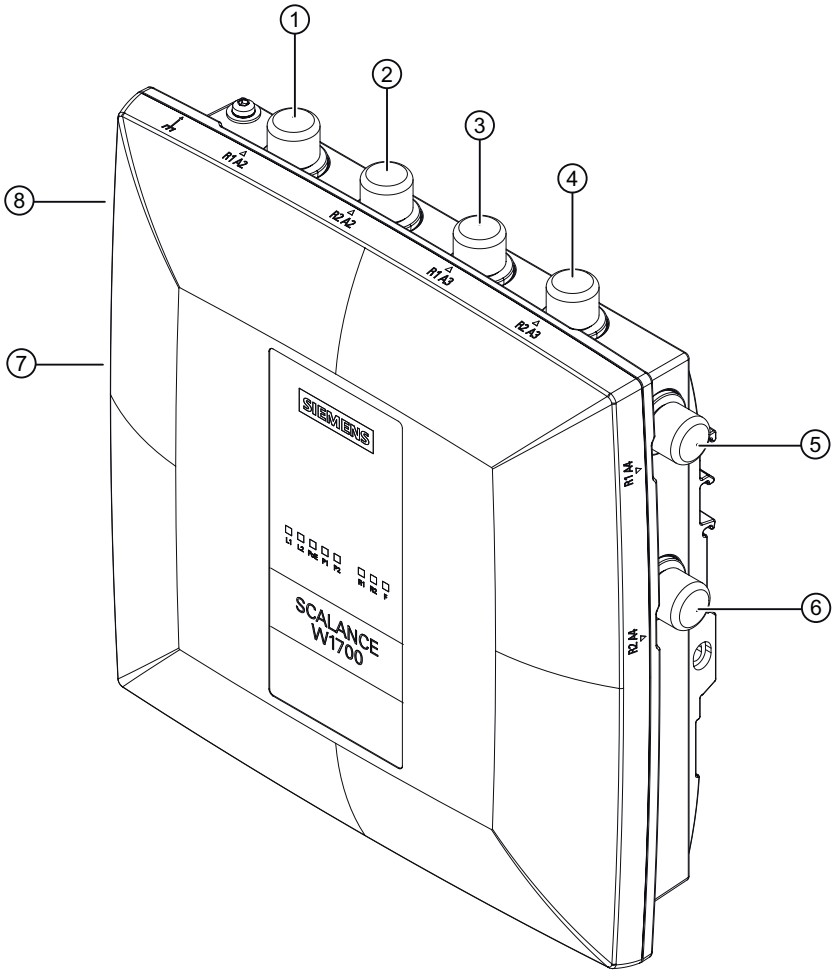
The SCALANCE W1788-1/ W1748-1 has four antenna connectors of the type N-Connector female.



① R1 A2
② R1 A3
③ R1 A4
④ R1 A1 (covered)

SCALANCE W1788-2

The SCALANCE W71788-2 has 8 antenna connectors of the type N-Connect female.



① R1 A2
② R2 A2
③ R1 A3
④ R2 A3
⑤ R1 A4
⑥ R2 A4
⑦ R1 A1 (covered)
⑧ R2 A1 (covered)

Procedure

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

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

   Note

   Keep the protective caps

   Keep the protective caps removed for later use.

2. You can connect an external antenna directly to the device or connect it with a flexible connecting cable.
   Place the antenna plug or the flexible connecting cable on the antenna connection and tighten the sleeve nut of the plug on the antenna connection (wrench SW19, torque 1.7 Nm).
3. An antenna must always be connected to the antenna connections R1 A1 ⑦ and R2 A1⑧. You can find additional information on configuration of antennas in the WBM / CLI.
4. Screw a terminating resistor onto the unused antenna connections.

Note

Terminating resistor

Each WLAN interface has four antenna connectors. Any connections that are not in use must be fitted with a terminating resistor, see Accessories (Page 28).
An antenna must always be connected to the antenna connectors R1 A1 and R2 A1 as soon as the WLAN interface is switched on. Otherwise, there may be transmission disruptions.

Note

Access points with two WLAN interfaces

If both interfaces are operated in the same frequency range for access points with two WLAN interfaces:

- The distance between the antennas connected to R1A1, R1A2, R1A3, R1A4 and those connected to R2A1, R2A2, R2A3, R2A4 must be at least 1 m.
- There may be wireless interference on one or both WLAN interfaces if the transmit power is higher than 15 dB.

Note

Cabinet installation

When installing the device in a cabinet, use detached antennas. Use a suitable flexible connecting cable for a connection between the device and the detached antenna. You will find detailed information in the section Flexible connecting cables (Page 26).

NOTICE

UL approval only for use in buildings

Within the area of authority of the NEC and CEC, the SCALANCE W1788/W1748 devices and the antennas connected to them may only be used in a closed building. For this reason, do not lead antennas into the outdoor area if you need to meet UL or CSA requirements.

6.5 Grounding

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

The grounding screws are identified by the following symbol for the functional ground ⏚.

Protective earth/functional ground

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

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

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

Position

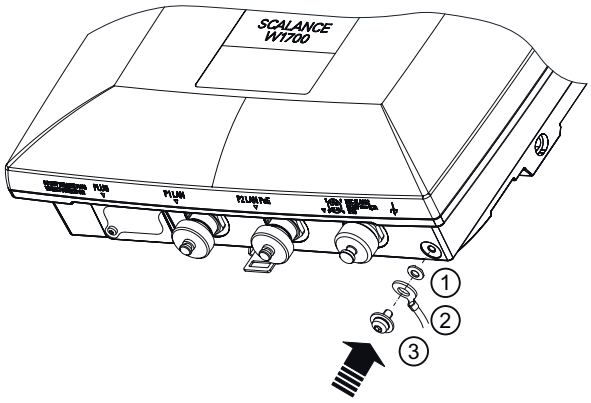
Functional ground is established via a grounding screw on the bottom of the device.

On the top, the device has an additional, optional connector to the functional ground, see Device views (Page 20).

Connecting up functional ground

Follow the steps below to connect the functional ground:

1. Put the toothed washer ①, the grounding terminal ② and the screw ③ together as shown in the drawing.



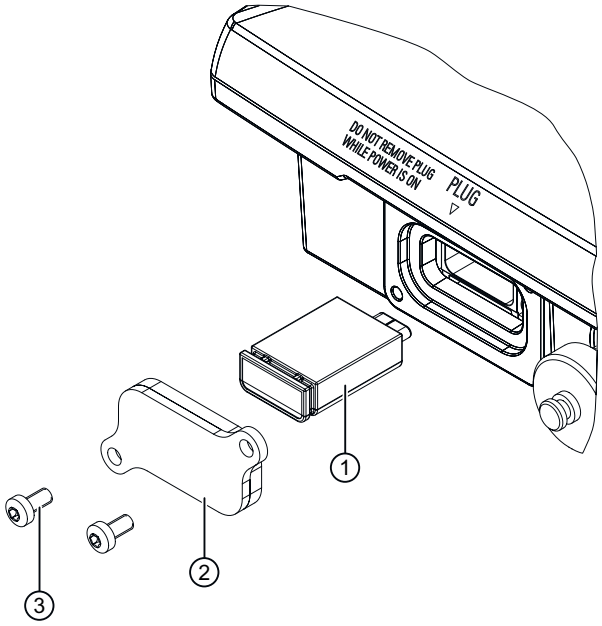
① Toothed washer
② Grounding terminal with cable
③ Screw (M4 thread) with washer

2. Tighten the screw ③ with a maximum tightening torque of 1.5 Nm.

6.6 Replacing a CLP

Position

The PLUG slot is on the bottom of the device housing under a cover, see Reset button (Page 19).



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

Removing a CLP

Note

Loss of the configuration

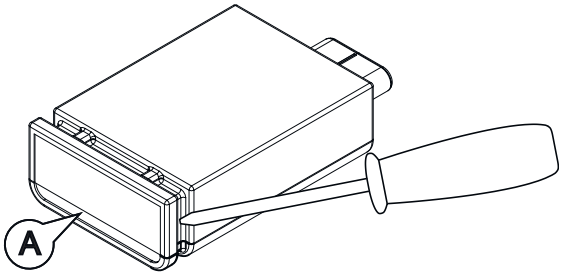
The reset button is located directly beside the slot for the CLP. The reset button cannot be used to remove the CLP.

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

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

1. Turn off the power to the device.
2. Loosen the screws M3 ③ with a Torx screwdriver T10 and remove the slot cover ②.
   As an alternative, you can loosen only one of the screws ③ and swivel the slot cover ② to the side.

3. To release the CLP ①, insert a screwdriver between the front edge of the CLP (A) and the slot.

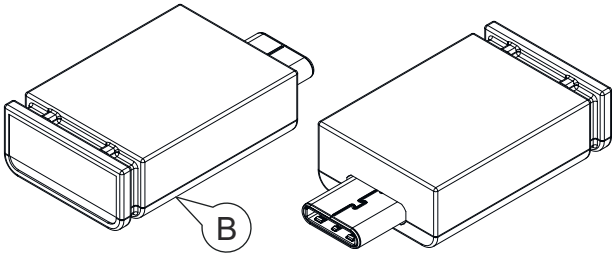


4. Remove the CLP from the slot.
5. Close the slot cover (torque 0.8 Nm) to ensure that the device maintains the degree of protection IP65.

Inserting the CLP

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

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



4. Close the slot cover (torque 0.8 Nm) to ensure that the device maintains the degree of protection IP65.

Maintenance and cleaning

7

⚠ WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

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

⚠ WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

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



⚠ CAUTION

Hot surfaces

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

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

NOTICE

Cleaning the housing

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

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

Do not use solvents.

Troubleshooting

8

8.1 Downloading new firmware using TFTP without WBM and CLI

Firmware

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

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

When pressing the button, make sure you adhere to the instructions in the section "Reset button (Page 38)".

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

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

8.2 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 38)".

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

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

With SINEC PNI

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

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

Via the configuration

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

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

Technical specifications

9

9.1 SCALANCE W1788-1 / W1748-1

Note

You will find detailed information on the transmit power and receiver sensitivity in the document "Performance data 802.11ac SCALANCE W1700" on the Internet at (https://support.industry.siemens.com/cs/de/en/view/109759606).

- SCALANCE W1788-1 M12
- SCALANCE W1748-1 M12

Technical specifications		
Data transfer		
Ethernet transfer rate		10/100/1000 Mbps
Wireless transmission rate		1 ... 1733 Mbps
Wireless standards supported		IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac
Power supply for PoE standards supported	Standards	IEEE 802.3at Type 2
	Class	Class 4 (12.95 – 25.50 W)
	Mode	Mode A, Mode B
Attachment to Industrial Ethernet		
	Quantity	2
	Design	M12 socket
	Properties	Half duplex/full duplex, autocrossover, autonegotiation, autosensing, floating, PoE at port 2
Permitted cable lengths (Ethernet)	**(Alternative combinations per length range)**	
	IE TP torsion cable	0 ... 55 m 0 ... 45 m + 10 m TP cord
	IE FC TP marine cable IE FC TP trailing cable IE FC TP flexible cable	0 ... 85 m 0 ... 75 m + 10 m TP cord
	IE FC TP standard cable	0 ... 100 m 0 ... 90 m + 10 m TP cord
Radio		

Technical specifications		
Antenna connector	Quantity	4
	Design	N-Connect socket
	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 Safe Extra Low Voltage (SELV)
	Type of current	⎓
	Permitted range ±30%	16.8 to 31.2 VDC
	Design	M12 socket
	Properties	Not galvanically isolated
		PoE to 24 V DC non-redundant design
Supply voltage from PoE	Supply voltage	48 VDC
	Type of current	⎓
	Permitted range	36 to 57 VDC
	Properties	Galvanically isolated
Fusing		2 A / 24 VDC
		1 A / 48 V DC PoE
Current consumption	At 24 VDC / typical	700 mA; max. 500 mA at PoE 36 V
	For PoE 48 V / typical	385 mA; max. 500 mA at PoE 36 V
Effective power loss	At 24 VDC / typical	16.8 W; max. 17.4 W at 31.2 V DC
	For PoE 48 V / typical	18.5 W; max. 18.5 W at PoE 36 V
Permitted ambient conditions		
Ambient temperature	During operation	-20 °C to +70 °C
	During storage	-40 °C to +85 °C
	During transportation	-40 °C to +85 °C
Relative humidity	During operation	≤ 90% at 25 °C, no condensation
Operating altitude	During operation	≤ 2000 m above sea level at max. 70 °C ambient temperature
Contaminant concentration		According to ISA-S71.04.-2013 Class G3
Degree of pollution		2
Degree of protection		IP65 (according to DIN EN 60529)
Dimensions and weight		
Dimensions	W x H x D	258 x 258 x 80 mm
Weight		2.7 kg
Installation options		
Direct	Wall mounting with mounting plate	
Rail	Mounting on a DIN rail with pre-installed DIN rail mounting adapter	
	Mounting on the standard rail S7-1200 / S7-1500 with rail mounting adapter	
Mean time between failure (MTBF)		
	at 40 °C ambient temperature	18 years

9.2 SCALANCE W1788-2 / W1788-2IA

Note

You will find detailed information on the transmit power and receiver sensitivity in the document "Performance data 802.11ac SCALANCE W1700" on the Internet at (https://support.industry.siemens.com/cs/de/en/view/109759606).

- SCALANCE W1788-2 M12
- SCALANCE W1788-2 M12 EEC
- SCALANCE W1788-2IA M12

Technical specifications		
Data transfer		
Ethernet transfer rate		10 / 100 / 1000 Mbps
Wireless transmission rate		1 ... 1733 Mbps
Wireless standards supported		IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac
Power supply for PoE standards supported	Standards	IEEE 802.3at Type 2
	Class	Class 4 (12.95 – 25.50 W)
	Mode	Mode A, Mode B
Attachment to Industrial Ethernet		
	Quantity	2
	Design	M12 socket
	Properties	Half duplex/full duplex, autocrossover, autonegotiation, autosensing, floating, PoE at port 2
Permitted cable lengths (Ethernet)	**(Alternative combinations per length range)**	
	IE TP torsion cable	0 ... 55 m 0 ... 45 m + 10 m TP cord
	IE FC TP marine cable IE FC TP trailing cable IE FC TP flexible cable	0 ... 85 m 0 ... 75 m + 10 m TP cord
	IE FC TP standard cable	0 ... 100 m 0 ... 90 m + 10 m TP cord
Radio		
Antenna connections for the device variants: • SCALANCE W1788-2 M12 • SCALANCE W1788-2 M12 EEC	Quantity	8
	Design	N-Connect socket
	Impedance	50 Ω nominal

Technical specifications			
Internal antennas for the device variant: • SCALANCE W1788-2IA M12	Quantity		8
	Antenna gain		7 dBi at 2.4 GHz 5 dBi at 5 GHz
Frequency range (all device variants)			2412 ... 2480 MHz 4920 ... 5875 MHz
Electrical data			
Direct 24 VDC supply	Supply voltage from socket		24 V DC Safe Extra Low Voltage (SELV)
	Type of current		⎓
	Permitted range	±30%	16.8 to 31.2 VDC
	Design		M12 socket
	Properties		Not galvanically isolated PoE to 24 V DC non-redundant design
Supply voltage from PoE	Supply voltage		48 VDC
	Type of current		⎓
	Permitted range		36 to 57 VDC
	Properties		Galvanically isolated
Fusing			2 A / 24 VDC 1 A / 48 V DC PoE
Current consumption	At 24 VDC / typical		700 mA; max. 500 mA at PoE 36 V
	For PoE 48 V / typical		385 mA; max. 500 mA at PoE 36 V
Effective power loss	At 24 VDC / typical		16.8 W; max. 17.4 W at 31.2 V DC
	For PoE 48 V / typical		18.5 W; max. 18.5 W at PoE 36 V
Permitted ambient conditions			
Ambient temperature	During operation	Non EEC variant	-20 ℃ to +70 ℃
		EEC variant	-40 °C ...+75 °C
	During storage		-40 ℃ to +85 ℃
	During transportation		-40 ℃ to +85 ℃
Relative humidity	During operation		≤ 90% at 25 °C, no condensation
Operating altitude	During operation		≤ 2,000 m above sea level at max. 70 °C / 75 °C (EEC) ambient temperature
Contaminant concentration			According to ISA-S71.04.-2013 Class G3
Degree of pollution			2
Degree of protection			IP65 (according to DIN EN 60529)
Dimensions and weight			
Dimensions	W x H x D		258 x 258 x 80 mm
Weight			2.7 kg
Installation options			
Direct	Wall mounting with mounting plate		
With additional holding plate	Mounting on a DIN rail with pre-installed DIN rail mounting adapter Mounting on the standard rail S7-1200 / S7-1500 with rail mounting adapter		

Technical specifications		
Mean time between failure (MTBF)		
	at 40 °C ambient temperature	18 years

Dimension drawings

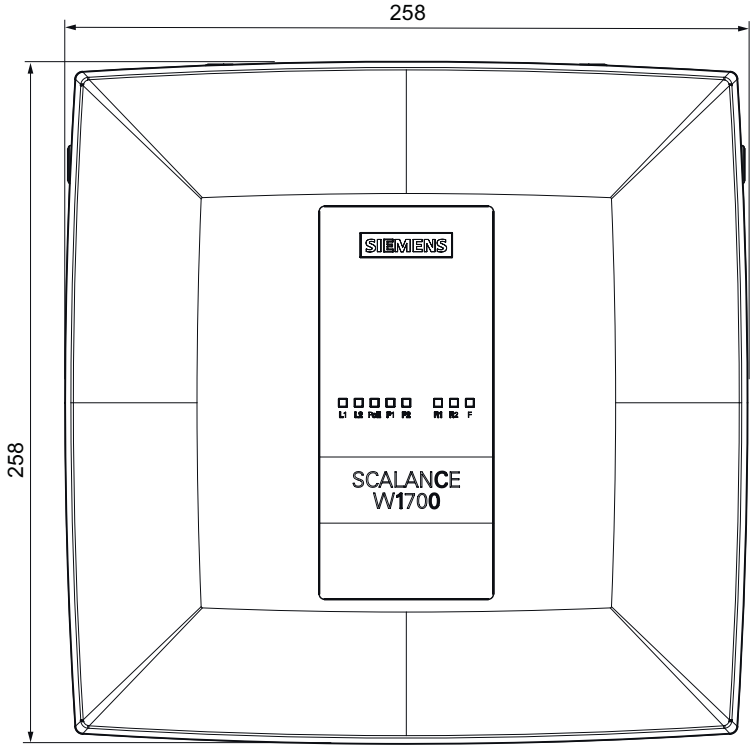
10

10.1 SCALANCE W1788-x / W1748-1

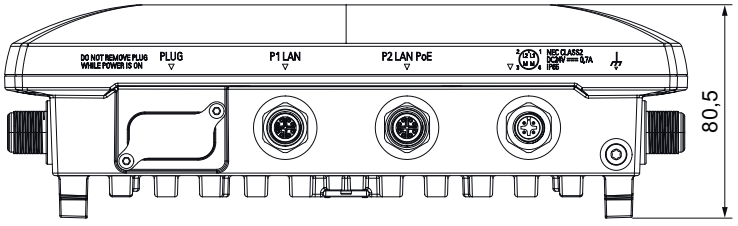
Note

Dimensions are specified in mm.

Front view

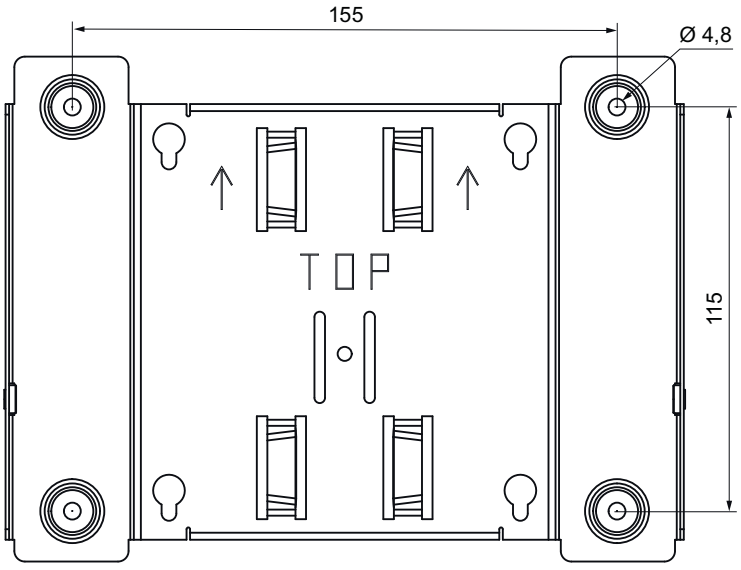


Side view



10.2 Mounting plate

Drill holes for wall mounting



Approvals

11

You will find the approvals of the products in the reference document "Approvals SCALANCE W1700 802.11ac" on the Internet pages of Siemens Industry Online Support:

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

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:

- SIMATIC NET Manual Collection
- SCALANCE W Manual Collection

Index

A

Accessories, 23
A-coded, 63
Antenna cables, 26
Antennas, 26, 67

C

Cables
  Permitted lengths, 81, 82, 83, 84, 85
CLP, 39
  Function, 40
  Replacing, 72
Components of the product, 22
Configuration manuals, 79
Connecting
  Antennas, 67
  Ethernet, 65
  Grounding, 70
  Power supply, 63

D

Documentation on the Internet, 5

E

Ethernet, 65

F

Factory defaults, 38, 78
Factory setting, 78
Functional ground, 70

G

Grounding, 58, 70

I

Installation
  DIN rail, 50
  S7-1500 standard rail, 53
  S7-300 standard rail, 53
  Wall mounting, 46
Interfaces, 81, 82, 83, 84, 85

L

LED display, 30, 34
Lightning protection, 57
Loading firmware, 38

P

PLUG, 39
  Function, 40
  Replacing, 72
Power supply, 63
Primary user (radar), 30, 34

R

Reset button, 38
Reset device, 38, 78
Resetting the device, 38
Restart of the device, 38

S

Safety extra low voltage, 58
Safety notices
  for installation, 41
  general, 9
  Use in hazardous areas, 9, 41, 57
  when connecting up, 57
System manual, 6

T

Technical specifications, 81, 82, 83, 84, 85
Type designations, 19