SIEMENS

SIMATIC NET

Industrial Ethernet switches SCALANCE XC-400

Operating Instructions

Introduction 1

Safety notices 2

Security recommendations 3

Description of the device 4

Installing and removing 5

Connecting up 6

Maintenance and cleaning 7

Troubleshooting 8

Technical specifications 9

Dimension drawings 10

Certifications and approvals 11

10/2025
C79000-G8976-C694-03

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C694-03
Ⓟ 10/2025 Subject to change

Copyright © Siemens 2023 - 2025.
All rights reserved

Table of contents

1 Introduction 7

1.1 Scope of validity 7

1.2 Designations used 7

1.3 Additional documentation 8

1.4 Service & Support 9

1.5 SIMATIC NET glossary 10

1.6 Cybersecurity information 10

1.7 Error/fault 11

1.8 Decommissioning 11

1.9 Recycling and disposal 11

1.10 Trademarks 11

1.11 Electrostatic discharge 12

2 Safety notices 13

3 Security recommendations 15

3.1 Security recommendations 15

3.2 Available interfaces 21

3.3 Available services 21

4 Description of the device 25

4.1 Article numbers 25

4.2 Factory settings 25

4.3 Device views 27
4.3.1 SCALANCE XC416-8 27
4.3.2 SCALANCE XC424-4 28
4.3.3 SCALANCE XC432 29

4.4 Type designation 30

4.5 Components of the product 30

4.6 Spare parts 31
4.6.1 Terminal blocks (2-pin) 31
4.6.2 Configuration and License PLUG 31

4.7 Accessories 31
4.7.1 Energy cable 31
4.7.2 Serial USB cable 32
4.7.3 SFP transceivers 32
4.7.4 Terminal blocks (4-pin) 34

4.8 LED display ... 35
4.8.1 Position and arrangement ... 35
4.8.2 "F" LED ... 35
4.8.3 "RM" LED ... 36
4.8.4 "SB" LED ... 36
4.8.5 LEDs "DM1" and "DM2" ... 36
4.8.6 LEDs "L1" and "L2" ... 37
4.8.7 "P" LEDs ... 38
4.9 SELECT/SET button ... 40
4.9.1 Position ... 40
4.9.2 Function ... 40
4.9.3 Setting the display mode ... 41
4.10 Configuration License PLUG ... 41
4.10.1 Position ... 41
4.10.2 Function ... 42
5 Installing and removing ... 43
5.1 Safety during mounting ... 43
5.2 Types of installation ... 46
5.3 Installation clearance ... 47
5.4 Installation position ... 47
5.5 Mounting on DIN rails ... 48
5.6 Installation on a standard S7-300 rail ... 50
5.7 Installation on a standard S7-1500 rail ... 51
5.8 Wall mounting ... 52
5.9 Changing the position of the securing bar ... 53
5.10 Disassembly ... 54
6 Connecting up ... 55
6.1 Safety when connecting up ... 55
6.2 Wiring rules ... 60
6.3 Power supply ... 61
6.4 Functional ground ... 62
6.5 Industrial Ethernet ... 63
6.5.1 Electrical ... 63
6.5.2 Optical ... 66
6.5.3 Dependency between ports and ambient temperature (derating) ... 66
6.5.3.1 Devices with 4 SFP/SFP+ slots ... 68
6.5.3.2 Devices with 8 SFP/SFP+ slots ... 69
6.5.4 Inserting and removing pluggable transceivers ... 70
6.5.4.1 General notes for SFP transceivers ... 70
6.5.4.2 Inserting a plug-in transceiver (SFP/SFP+) ... 70
6.5.4.3 Removing a pluggable transceiver (SFP/SFP+) ... 71
6.6 Signaling contact ... 71

6.7 USB console interface ... 73
6.8 Replacing a CLP ... 74
7 Maintenance and cleaning ... 75
8 Troubleshooting ... 77
8.1 Resetting the device to default settings with the button (in the startup phase) ... 77
8.2 Resetting the device to default settings with the button (during operation) ... 78
8.3 Loading a firmware file via TFTP ... 79
9 Technical specifications ... 81
9.1 Technical specifications of SCALANCE XC416-8 ... 81
9.2 Technical specifications of SCALANCE XC424-4 ... 83
9.3 Technical specifications of SCALANCE XC432 ... 85
9.4 Mechanical stability (in operation) ... 87
9.5 Resistance to harmful gases according to ISA-71.04 ... 87
9.6 Cable lengths ... 87
9.7 Switching properties ... 88
9.8 RF radiation according to NAMUR NE21 ... 88
10 Dimension drawings ... 89
11 Certifications and approvals ... 93
Index ... 99

Introduction

1

These operating instructions will help you to install and connect devices of the SCALANCE XC-400 product group.

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

1.1 Scope of validity

These operating instructions apply to the following devices:

- SCALANCE XC416-8
- SCALANCE XC424-4
- SCALANCE XC432

Unless mentioned otherwise, the descriptions in these operating instructions refer to all devices of the SCALANCE XC-400 product group specified in the scope of validity.

1.2 Designations used

This section describes the conventions used in this document to clearly and efficiently portray information.

Classification	Description	Terms used
Product line	The product line includes all devices and variants of all product groups. If information applies to all product groups within the product line, the term SCALANCE X-400 is used.	SCALANCE X-400
Product group	If information applies to all devices and variants of a product group, the term SCALANCE XC-400 is used.	SCALANCE XC-400
Device	If information relates to a specific device, the device name is used.	e.g. SCALANCE XC424-4

1.3 Additional documentation

The following additional documents may be of interest. Unless specified otherwise, the documents are available in the Siemens Industry Online Support (SIOS) (https://support.industry.siemens.com/cs/ww/en/ps/29061).

Note

The listed documents are the documents that were available at the time of the publication. Newer versions of these documents or the associated products may be available. Additional information is available in the SIOS or contact your Siemens customer service.

Product notes

Product notes are available online in the SIOS (https://support.industry.siemens.com/cs/ww/en/ps/15247).

Manuals

Document title	Link
Configuration manual "SIMATIC NET: SCALANCE Layer 2 Switches Command Line Interface (CLI) VX.X"	Visit (https://support.industry.siemens.com/cs/ww/en/view/109799819)
Configuration manual "SIMATIC NET: SCALANCE Layer 2 Switches Web Based Management (WBM) VX.X"	
"Transceiver SFP/SFP+/SCP/STP" Operating Instructions	Visit (https://support.industry.siemens.com/cs/ww/en/ps/25547/man)
"Industrial Ethernet/PROFINET Industrial Ethernet" System Manual	Visit (https://support.industry.siemens.com/cs/ww/en/view/27069465)
"Industrial Ethernet/PROFINET Passive Network Components" System Manual	Visit (https://support.industry.siemens.com/cs/ww/en/view/84922825)

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 communication partners that you require for the design.

Catalogs

You will find the article numbers for the Siemens products of relevance here in the following catalogs:

- SIMATIC NET Industrial Communication / Industrial Identification, catalog IK PI
- SIMATIC Products for Totally Integrated Automation and Micro Automation, catalog ST 70
- Industry Mall - catalog and ordering system for automation and drive technology, Online catalog (https://mall.industry.siemens.com/goos/WelcomePage.aspx?regionUrl=/de&language=en)

You can request the catalogs and additional information from your Siemens representative.

See also

WBM (https://support.industry.siemens.com/cs/ww/en/view/109799818)

1.4 Service & Support

Industry Online Support

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

Apart from news, there you will also find:

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

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

SITRAIN - Training for Industry

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

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

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

Industrial Networks Education

Training and certification for Industrial Networks

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

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

1.5 SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD
  The DVD ships with certain SIMATIC NET products.
- On the Internet under the following address:
  50305045 (https://support.industry.siemens.com/cs/ww/en/view/50305045)

1.6 Cybersecurity information

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

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

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

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

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

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

1.7 Error/fault

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

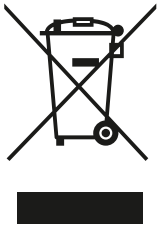
1.8 Decommissioning

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.

1.9 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.

1.10 Trademarks

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

- SCALANCE
- SINEC

1.11 Electrostatic discharge



NOTICE
Electrostatic sensitive devices (ESD) Electronic modules contain electrostatic sensitive components These components can easily be destroyed if handled incorrectly. Note the following instructions to avoid damage. • Touch electronic modules only when you absolutely need to work on them. • If electronic modules need to be touched, the body of the person involved must first be electrostatically discharged and grounded. • Do not bring electronic modules in contact with electrically isolating materials such as plastic film, isolating table top pads or clothing made of synthetic fibers. • Place the modules only on conductive surfaces. • Pack, store and transport electronic modules and components only in conductive packaging such as metalized plastic or metal containers, conductive foam or household aluminum foil.

Safety notices

2

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".

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

NOTICE
Information security
Connect to the device and change the standard password for the user set in the factory "admin" and "" before you operate the device.

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

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

Safety instructions for use in hazardous locations according to UL/FM HazLoc

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

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

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

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.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx).
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- No product liability will be accepted for operation in a non-secure infrastructure.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (IPsec, OpenVPN).
- Separate connections correctly (WBM, SSH etc.).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central logging server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.
  Download (https://sieportal.siemens.com/su/blCGg)
  Check regularly for new features on the Siemens Internet pages.
  - You can find information on Industrial Security here:
    Link: (https://www.siemens.com/industrialsecurity)
  - You can find a selection of documents on the topic of network security here:
    Link: (https://support.industry.siemens.com/cs/ww/en/view/92651441)

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

Authentication and users

Note

Accessibility risk - Risk of data loss

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

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

Certificates and keys

- There is a preset SSL certificate on the device with a key length of 256 bits for the elliptic-curve cryptography (ECDSA). Replace this certificate with a self-made certificate with key. You can install the certificate via the WBM ("System > Load and Save"). We recommend that you use a certificate signed by a reliable external or internal certification authority.
  Use ECDSA certificates in PEM format that were generated with one of the following curves:
  - secp256r1 (NIST P-256)
  - secp384r1 (NIST P-384)
  - secp521r1 (NIST P-521)

  RSA certificates with a recommended key length of 4096 bits can also be used. However, this is not recommended for performance reasons.
- 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.
- For the device to be able to correctly check digital certificates and establish secure connections, the system time always needs to be up to date. Follow the steps outlined below:
  Check and set time
  Check whether the time is set correctly on the device, especially after a reset to factory settings or a long power supply interruption.
  Enable time-of-day synchronization (recommended)
  Activate one of the supported synchronization methods.
  Make sure that there is a stable connection to the synchronization partner so that the device can regularly receive the current time.

Physical/remote access

- Operate the devices only within a protected network area. Attackers cannot access internal data from the outside when the internal and the external network are separate from each other.
- Limit physical access to the device exclusively to trusted personnel.
  The memory card or the PLUG (C-PLUG, KEY-PLUG, CLP) contains sensitive data such as certificates and keys that can be read out and modified. An attacker with control of the device's removable media could extract critical information such as certificates, keys, etc. or reprogram the media.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.

- We highly recommend that you keep the protection from brute force attacks (BFA) activated to prevent third parties from gaining access to the device. For more information, see the configuration manuals, section "Brute Force Prevention".
- For communication via non-secure networks, use additional devices with VPN functionality to encrypt and authenticate communication.
- When you establish a secure connection to a server (e.g. for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTP, HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it. For more information, refer to "Decommissioning".
- We recommend formatting a PLUG that is not being used.

Software (security functions)

- Keep the firmware up to date. Check regularly for security updates for the device. You can find information on this at the Industrial Security (https://www.siemens.com/industrialsecurity) website.
- Inform yourself regularly about security recommendations published by Siemens ProductCERT (https://www.siemens.com/cert).
- Only activate protocols that you require to use the device.
- Restrict access to the management of the device with rules in an access control list (ACL).
- The option of VLAN structuring provides protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.
- Use a central logging server to log changes and accesses. Operate your logging server within the protected network area and check the logging information regularly.
- Files (e.g. configuration files) can be downloaded from the device. Ensure that the files are adequately protected. The options for achieving this include storing the files in a secure location and transmitting them only through secure communication channels.
  In addition, you can create hash sums from the files after the download. This allows you to check that the file is unchanged before further use.
- Configuration files can be password-protected during download. You enter passwords on the WBM page "System > Load & Save > Passwords".
- The names of the configuration files can be changed. To improve security, do not use spaces in the TFTP file name.
- Only use VXLAN in trustworthy networks.

Secure/non-secure protocols and services

- Avoid or disable non-secure protocols and services, for example HTTP, Telnet and TFTP. For historical reasons, these protocols are available, however not intended for secure applications. Use non-secure protocols on the device with caution.
- Check whether use of the following protocols and services is necessary:
  - Non authenticated and unencrypted ports
  - DCP
  - DHCP
  - DNS client
  - HTTP
  - IEEE 802.1x (RADIUS)
  - ICMP
  - IGMP Snooping
  - LLDP
  - MRP, HRP, STP, RSTP and MSTP
  - NTP client
  - PROFINET
  - SIMATIC NET Time
  - SMTP client
  - SNMP v1/2c
  - SNMP Traps
  - SNTP-Client
  - Syslog client
  - Telnet
  - TFTP
  - GMRP and GVRP

- The following protocols provide secure alternatives:
  - SNMPv1/v2c → SNMPv3
    Check whether use of SNMPv1/v2c. is necessary. SNMPv1/v2c is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options.
    If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
    Use SNMPv3 in conjunction with passwords.
  - HTTP → HTTPS
  - Telnet → SSH
  - NTP → NTPsecure
  - TFTP → SFTP
  - Syslog Client → Syslog Client TLS
- Use secure protocols when access to the device is not prevented by physical protection measures.
- If you require non-secure protocols and services, operate the device only within a protected network area.
- Select a trusted DNS provider.
- Restrict the services and protocols available to the outside to a minimum.
- With authentication on the RADIUS server and RADIUS client, use the Message Authenticator attribute to check packets.
- If you use RADIUS for management access to the device, activate secure protocols and services.
- The LAN interface of the product must not be operated in unprotected or untrusted networks (e.g. the Internet) without additional upstream protective devices.
- Only operate Syslog, SNTP and other non-secure protocols over secure connections (e.g. SINEMA RC/OpenVPN).

Interfaces security

- Disable unused interfaces.
- Use IEEE 802.1X for interface authentication.
- Use the function "Locked Ports" to block interfaces for unknown nodes.
- Use the configuration options of the interfaces, e.g. the "Edge Type".
- Configure the receive ports so that they discard all untagged frames ("Tagged Frames Only").

3.2 Available interfaces

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

Interface	Default status	Change to the status	
		WBM / CLI (administrator)	Physical
LAN 1 to 32 *)	Enabled	✓	-
WAN	Disabled	✓	-
Signaling contact	Enabled	-	✓
USB console interface	Enabled	-	✓
PLUG slot	Enabled	✓	✓

*) Depending on the device variant

3.3 Available services

List of available services

Note

Packet filtering

Packets are processed according to their importance for the operation of the network. Some packets directed to the CPUs of the switch may be discarded due to various security-relevant packet filters. Therefore, it can occur that not all ICMP packets are delivered to the CPUs, for example, and are thus not responded to.

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 setting of service	Default port status	Configurable		Authentication	Encryption [7]
				Port	Service		
DHCPv4 Server	UDP/67	Active	Closed	✓	✓	-	-
DHCPv4 Client (IPv4)	UDP/68	Disabled	Open	-	✓	-	-
DNS Client	TCP/53 UDP/53	Disabled	Outbound only	-	✓	-	-
EtherNet/IP [2]	TCP/44818 UDP/2222 UDP/44818	Disabled	Closed	-	✓	-	-
HTTP Server [4] [5]	TCP/80	Disabled	Closed	✓	✓	✓	-
HTTPS WBM Server	TCP/443	Active	Open	✓	✓	✓	✓
NTP Client	UDP/123	Disabled	Closed	✓	✓	-	-
NTP (secure)	UDP/123	Disabled	Closed	✓	✓	✓	-
Ping	ICMP	Active	Open	-	-	-	-
PROFINET	UDP/34964 UDP/ 49151 ... 49159 [1]	Disabled	Open	-	✓	-	-
RADIUS Client	UDP/1812 [6] UDP/1813 [6]	Disabled	Outbound only	✓	✓	-	-
	UDP/3799	Disabled	Open	✓	✓	-	-
SFTP Client	TCP/22	Active	Outbound only	✓	✓	✓	✓
SMTP Client	TCP/25	Disabled	Closed	✓	✓	-	-
SMTP Client (secure)	TCP/465	Disabled	Closed	✓	✓	✓	✓
SNMPv1/v2c [3] [4]	UDP/161	Disabled	Open	✓	✓	-	-
SNMPv3	UDP/161	Disabled	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Disabled	Outbound only	-	✓	-	-
SNTP Client	UDP/123	Disabled	Closed	✓	✓	-	-
SSH CLI Server	TCP/22	Active	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Disabled	Closed	✓	✓	-	-
Syslog (secure) Client	TCP/6514	Disabled	Closed	✓	✓	-	✓
Telnet [4]	TCP/23	Disabled	Closed	✓	✓	✓	-
TFTP Client	UDP/69	Disabled	Outbound only	✓	✓	-	-
VRRP	TCP/50000	Disabled	Open, filtered	-	✓	-	-

1) Port number can be configured via the WBM.

2) Service disabled by default.

3) Read-only access only.

4) Protocol according to Security by Default.

5) The HTTP port is always open. If the service is disabled, automatic HTTP forwarding to the HTTPS port takes place.

6) The port is closed by default and is displayed when a RADIUS server is configured.

7) You can find additional information on the encryption methods used in the WBM appendix "Ciphers used".

The following is a list of all available Layer 2 services through which the device can be accessed.

The table includes the following columns:

- **Layer 2 service**
  The Layer 2 services that the device supports**.**
- **Default status**
  The default status of the service (open or closed).
- **Service configurable**
  Indicates whether the service can be configured via WBM / CLI.

Layer 2 service	Default setting of service	Default port status	Service configurable	Encryption
DCP	Active	Setup mode [1)]	✓	-
ICMP	Active	Open	-	-
LLDP	Active	Open	✓	-
RSTP	Disabled	Closed	✓	-
MSTP	Disabled	Open	✓	-
SIMATIC NET TIME	Disabled	Closed	✓	-
VLAN	Disabled	Open (when configured)	✓	-
VXLAN [2)]	Disabled	Closed	✓	-

1) Setting according to Security by Default

2) Not with SCALANCE XR-500WG

4 Description of the device

4.1 Article numbers

Device	Description	Article number
SCALANCE XC416-8	• 16 x 10 / 100 / 1000 Mbps RJ45 ports • 8 x SFP / SFP+ plug-in transceiver slots with 1G / 10 Gbps • 2 x 2-pin terminal block 24 V DC, power supply connection • 1 x CLP slot • 1 x USB Type B, serial interface connection • 1 x 2-pin terminal block 24 V DC, signaling contact connection	6GK5 424-8TR00-2AC2
SCALANCE XC424-4	• 24 x 10 / 100 / 1000 Mbps RJ45 ports • 4 x SFP / SFP+ plug-in transceiver slots with 1G / 10 Gbps • 2 x 2-pin terminal block 24 V DC, power supply connection • 1 x CLP slot • 1 x USB Type B, serial interface connection • 1 x 2-pin terminal block 24 V DC, signaling contact connection	6GK5 428-4TR00-2AC2
SCALANCE XC432	• 32 x 10 / 100 / 1000 Mbps RJ45 ports • 2 x 2-pin terminal block 24 V DC, power supply connection • 1 x CLP slot • 1 x USB Type B, serial interface connection • 1 x 2-pin terminal block 24 V DC, signaling contact connection	6GK5 432-0GR00-2AC2

4.2 Factory settings

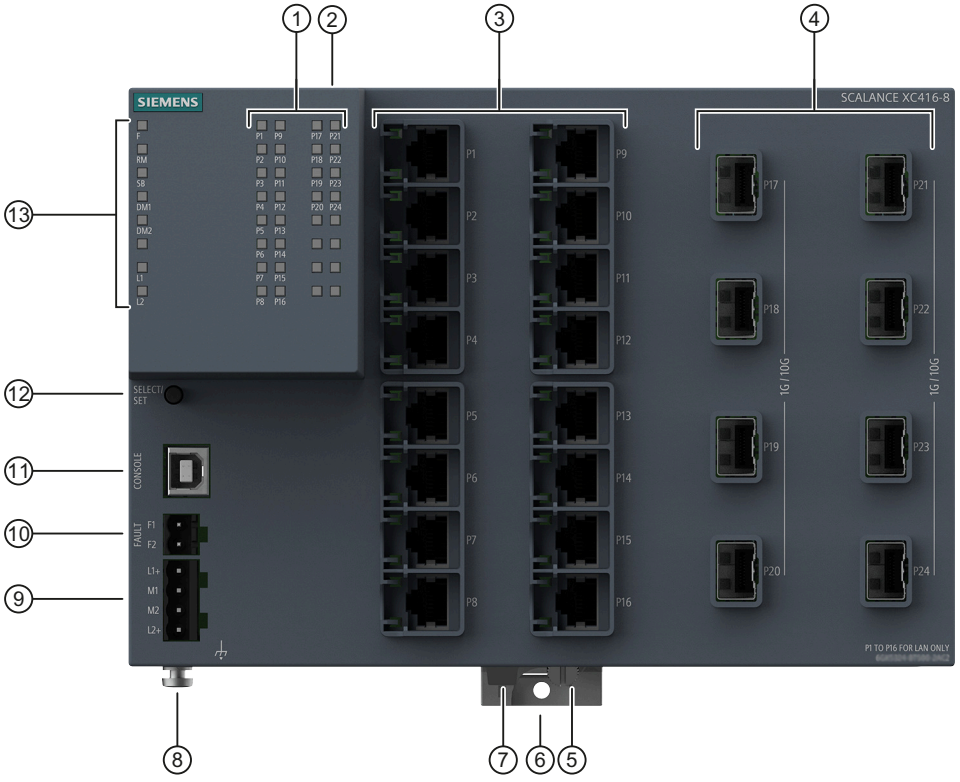
- Ring Redundancy: Off
- Ring Redundancy Mode: Off
- Spanning Tree Protocol (STP): On
- Protocol Compatibility: MSTP
- Passive Listening: Off
- VLAN Awareness: On
- Operating mode: VLAN-capable (IEEE 802.1Q)
- PROFINET Device Diagnostics: On
- DCP Server: Read/Setup
- IGMP Snooping: Off
- IGMP Querier: Off

- IPv4 Address conflict detection defense method: Never give up
- EtherNet/IP Device Diagnostics: Off
- QoS Trust Mode: Trust CoS-DSCP

4.3 Device views

4.3.1 SCALANCE XC416-8

The following figure shows an overview of the components of the SCALANCE XC416-8:

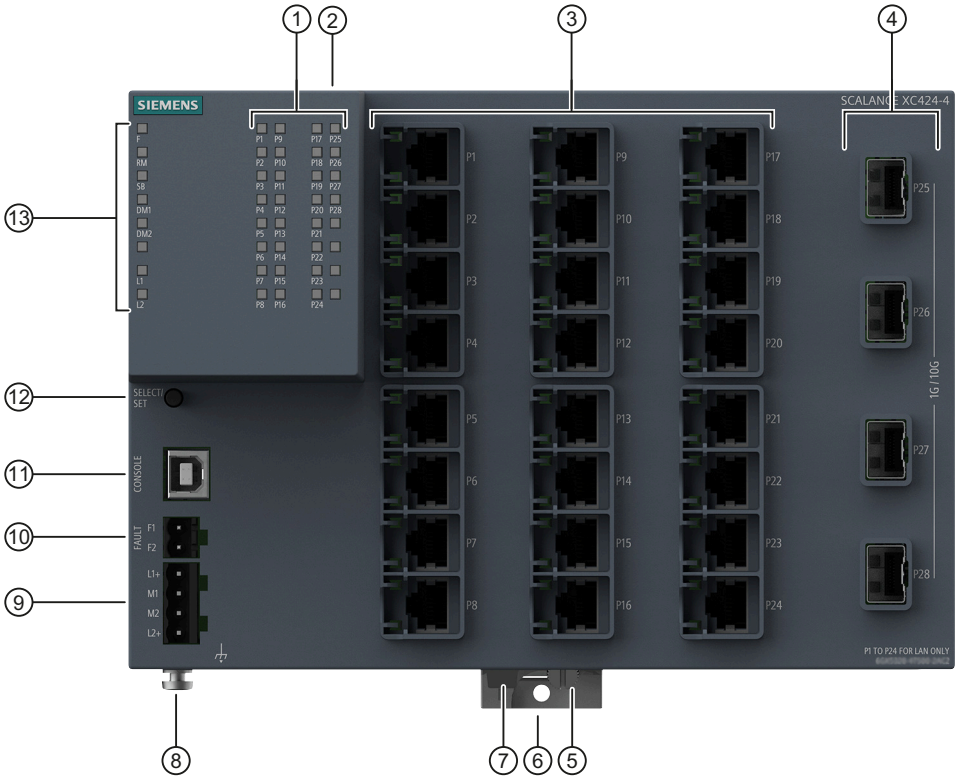


① Port LEDs
② CLP slot
③ Electrical ports with 10/100/1000 Mbps
④ Slots for SFP/SFP+ plug-in transceiver with 1/10 Gbps
⑤ Knurled screw
⑥ Securing bar
⑦ Levering aid on securing bar
⑧ Grounding screw
⑨ Power supply
⑩ Signaling contact
⑪ USB console interface
⑫ "SELECT/SET" button
⑬ LED display
- "F" LED for faults
- "RM" LED for the redundancy manager function
- "SB" LED for the status of the standby function
- "DM1/DM2" LED for the display mode
- "L1/L2" LED for the power supply

Figure 4-1 SCALANCE XC416-8

4.3.2 SCALANCE XC424-4

The following figure shows an overview of the components of the SCALANCE XC424-4.

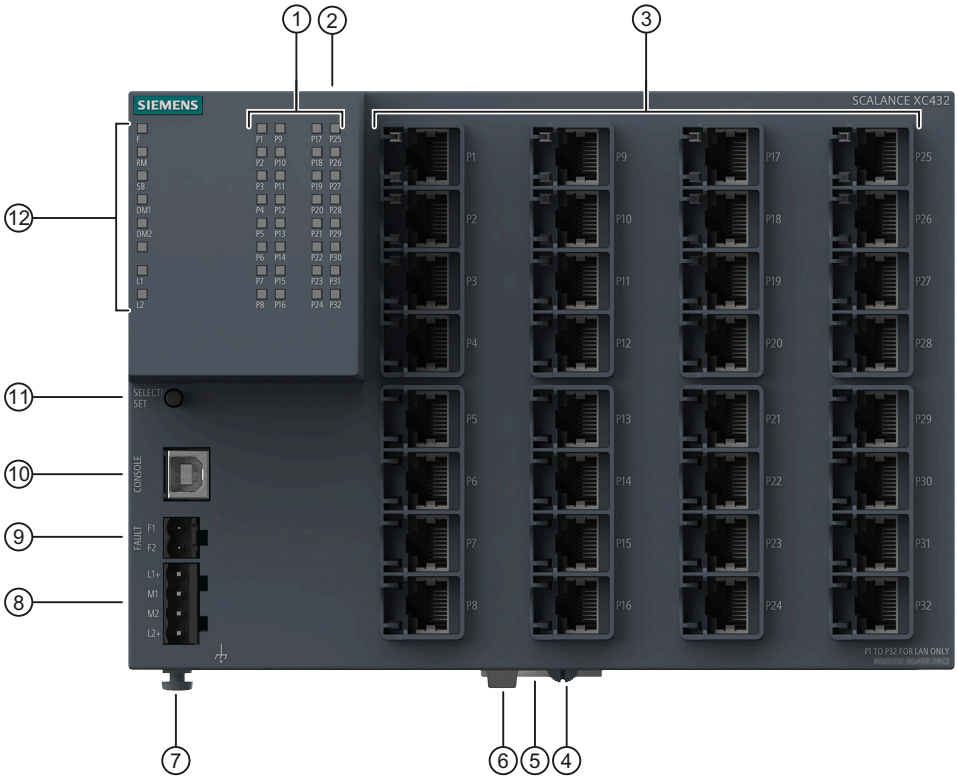


1. Port LEDs
2. CLP slot
3. Electrical ports with 10/100/1000 Mbps
4. Slots for SFP/SFP+ plug-in transceiver with 1/10 Gbps
5. Knurled screw
6. Securing bar
7. Levering aid on securing bar
8. Grounding screw
9. Power supply
10. Signaling contact
11. USB console interface
12. "SELECT/SET" button
13. LED display
    - "F" LED for faults
    - "RM" LED for the redundancy manager function
    - "SB" LED for the status of the standby function
    - "DM1/DM2" LED for the display mode
    - "L1/L2" LED for the power supply

Figure 4-2 SCALANCE XC424-4

4.3.3 SCALANCE XC432

The following figure shows an overview of the components of the SCALANCE XC432:



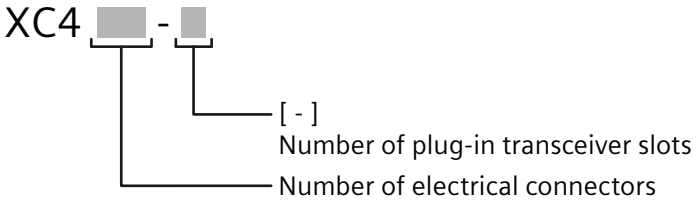
① Port LEDs
② CLP slot
③ Electrical ports with 10/100/1000 Mbps
④ Knurled screw
⑤ Securing bar
⑥ Levering aid on securing bar
⑦ Grounding screw
⑧ Power supply
⑨ Signaling contact
⑩ USB console interface
⑪ "SELECT/SET" button
⑫ LED display

- "F" LED for faults
- "RM" LED for the redundancy manager function
- "SB" LED for the status of the standby function
- "DM1/DM2" LED for the display mode
- "L1/L2" LED for the power supply

Figure 4-3 SCALANCE XC432

4.4 Type designation

The type designation of a SCALANCE XC-400 is made up of several parts that have the following meaning:



4.5 Components of the product

The following components are supplied with a SCALANCE XC-400:

- One device
- One CLP removable data storage medium 2 GB (article number 6GK1900-0UB00-0AA0)
- Two 2-pin spring-loaded terminal blocks 24 V DC for the power supply
- One 2-pin spring-loaded terminal block 24 V DC for the signaling contact
- One product DVD with documentation and software

The following additional components are supplied with a SCALANCE XC-400 with plug-in transceiver slots:

- One cover for each plug-in transceiver slot

Unpacking and checking

WARNING

Do not use any parts that show evidence of damage

If you use damaged parts, there is no guarantee that the device will function according to the specification.

If you use damaged parts, this can lead to the following problems:

- Injury to persons
- Loss of the approvals
- Violation of the EMC regulations
- Damage to the device and other components

Use only undamaged parts.

1. Make sure that the package is complete.
2. Check all the parts for transport damage.

4.6 Spare parts

The following spare parts are available for the devices mentioned in the scope of validity:

4.6.1 Terminal blocks (2-pin)

Component	Description	Article number
2-pin spring-loaded terminal block	2-pin spring-loaded terminal block for connecting the 24 V DC power supply and the 24 V DC signaling contact pack of 5	6GK5980-0BB10-0AA5

4.6.2 Configuration and License PLUG

Component	Description	Article number
SCALANCE CLP 2 GB	Configuration and License PLUG, removable data storage medium for configuration data, 2 GB	6GK1900-0UB00-0AA0

4.7 Accessories

The following accessories are available for the devices mentioned in the scope of validity:

4.7.1 Energy cable

Component	Description	Article number
Energy Cable 2 x 0.75	Energy cable for connection of signaling contact and power supply 24 V DC, 2-wire, stranded 2 x 0.75 mm^2, trailable, not assembled Sold by the meter	6XV1 812-8A
Robust Energy Cable 4 x 0.75	Energy cable for connection of power supply 24 V DC, 4-wire, stranded 4 x 0.75 mm^2, robust, flexible, not assembled Sold by the meter	6XV1 801-2A
Energy Cable 4 x 1.5	Energy cable for connection of power supply 24 V DC, 4-wire, stranded 4 x 1.5 mm^2, trailable, not assembled Sold by the meter	6XV1 801-2B

4.7.2 Serial USB cable

Component	Description	Article number
Connecting cable (USB Type A / USB Type B)	Preassembled USB cable with USB Type A and USB Type B connector, length: 2 m Pack of 1	7ML1930-1FN

4.7.3 SFP transceivers

Pluggable transceiver SFP (1000 Mbps)

Type	Property	Article number
SFP992-1	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 750 m	6GK5 992-1AL00-8AA0
	10 packing unit (VPE 10)	6GK5 992-1AL00-8AC0
SFP992-1 (C)	1 x 1000 Mbps, LC port optical, for glass FO cable (multimode), up to max. 750 m, varnished	6GK5 992-1AL00-8FA0
SFP992-1+	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 2 km	6GK5 992-1AG00-8AA0
SFP992-1LD	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km	6GK5 992-1AM00-8AA0
	10 packing unit (VPE 10)	6GK5 992-1AM00-8AC0
SFP992-1LD (C)	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km, varnished	6GK5 992-1AM00-8FA0
SFP992-1LD+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 30 km	6GK5 992-1AM30-8AA0
SFP992-1LH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 40 km	6GK5 992-1AN00-8AA0
SFP992-1LH+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5 992-1AP00-8AA0
SFP992-1ELH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 120 km	6GK5 992-1AQ00-8AA0

Pluggable transceivers with the supplement (C) in the type name have varnished printed circuit boards (conformal coating).

Bidirectional plug-in transceiver SFP

Bidirectional plug-in transceivers feature only one fiber connection. They transmit and receive on two different wavelengths. To establish a connection, you need two matching bidirectional SFPs. The connected SFPs must respectively transmit on the wavelength at which the connection partner receives.

Type	Properties	Article number
SFP992-1BXMT	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1550 nm, receives at 1310 nm	6GK5 992-1AL00-8TA0
SFP992-1BXMR	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1310 nm, receives at 1550 nm	6GK5 992-1AL00-8RA0
SFP992-1BX10T	1 x 1000 Mbps LC port optical for glass FO (single mode) with max. 10 km, transmits at 1550 nm, receives at 1310 nm	6GK5 992-1AM00-8TA0
SFP992-1BX10R	1 x 1000 Mbps LC port optical for glass FO (single mode) with max. 10 km, transmits at 1310 nm, receives at 1550 nm	6GK5 992-1AM00-8RA0

SFP+ transceiver

Type	Properties	Article number
SFP993-1	1 x 10 Gbps, LC port optical for glass FO cable (multimode), up to max. 550 m	6GK5 993-1AT00-8AA0
SFP993-1(C)	1 x 10 Gbps, LC port optical for glass FO cable (multimode), up to max. 550 m, coated	6GK5 993-1AT00-8FA0
SFP993-1LD	1 x 10 Gbps, LC port optical for glass FO cable (single mode), up to max. 10 km	6GK5 993-1AU00-8AA0
SFP993-1LD(C)	1 x 10 Gbps, LC port optical for glass FO cable (single mode), up to max. 10 km, coated	6GK5 993-1AU00-8FA0
SFP993-1LH	1 x 10 Gbps, LC port optical for glass FO cable (single mode), up to max. 40 km	6GK5 993-1AV00-8AA0
SFP993-1LH+	1 x 10 Gbps, LC port optical for glass FO cable (single mode), up to max. 80 km	6GK5 993-1AW00-8AA0

Can only be operated in SFP+ slots.

Pluggable transceivers with the suffix (C) in the type name have coated printed circuit boards (conformal coating).

Note

Restricted approvals

If you operate the device with an SFP transceiver of the type SFP993-1(C) or SFP993-1LD(C), the following approvals and certifications lose their validity for the device:

ATEX, IECEx, UKEX and CCC-Ex certification, FM, cULus approval Hazardous Location

If you operate the device with an SFP transceiver of the type SFP993-1LH+, the following approvals and certifications lose their validity for the device:

ATEX, IECEx, UKEX and CCC-Ex certification, FM, cULus approval Hazardous Location, cULus approvals

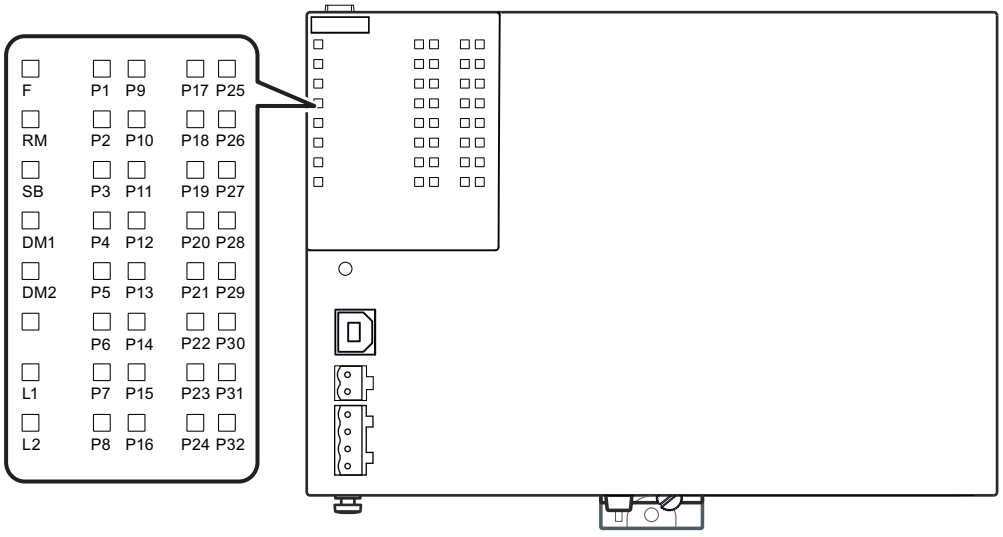
4.7.4 Terminal blocks (4-pin)

Component	Description	Article number
4-pin spring-loaded terminal block	4-pin spring-loaded terminal block for connecting the 24 V DC power supply pack of 5	6GK5980-1DB10-0AA5

4.8 LED display

4.8.1 Position and arrangement

The following figure shows the arrangement of the LEDs using the example of a device with 32 ports.



F	LED for displaying the fault/error status
RM	LED for displaying the "redundancy manager" function
SB	LED for displaying the "standby" function
DM1/DM2	LEDs for displaying the display mode
L1/L2	LEDs for displaying the power supply
P	LEDs for displaying the port status *)

Figure 4-4 Arrangement of the LEDs

*) The number of port LEDs depends on the device.

4.8.2 "F" LED

The "F" LED shows the fault/error status of the device.

Meaning during device startup

LED color	LED status	Meaning during device startup
-	Off	Device startup was completed successfully.
Red	On	Device startup is not yet completed or errors have occurred.
Red	Flashing	There are errors in the firmware.

Meaning during operation

LED color	LED status	Meaning during operation
-	Off	The device is operating free of errors. The signaling contact is closed.
Red	On	The device has detected a problem. The signaling contact has opened.
Red	Flashing	The device is starting up for the first time or has been reset to factory settings. The password of the default user "admin" has not yet been changed.

4.8.3 "RM" LED

The "RM" LED indicates whether the device has the Media Redundancy Manager (MRM) role and whether the MRP ring is operating error-free.

LED color	LED status	Meaning
-	Off	The device is not an MRM.
Green	On	The device has the MRM role. The MRP ring is in normal state. The MRM has blocked data traffic on one of its ring ports and is monitoring the MRP ring.
Green	Flashing	The device has the MRM role. The MRP ring is in error state. The MRM has detected an error in the MRP ring or at one of its ring ports and activates an alternative communication path.

4.8.4 "SB" LED

The "SB" LED shows the status of the standby function.

LED color	LED status	Meaning
-	Off	The standby function is disabled.
Green	On	The standby function is enabled. The standby section is passive.
Green	Flashing	The standby function is enabled. The standby section is active.

4.8.5 LEDs "DM1" and "DM2"

The "DM1" and "DM2" LEDs indicate which display mode is set.

There are 4 display modes (A, B, C and D). Display mode A is the default mode.

Depending on the set display mode, the "L1", "L2" LEDs and the port LEDs show different information.

LED color	LED status		Meaning
	DM1 LED	DM2 LED	
-	Off		Display mode A
Green	On	Off	Display mode B
Green	Off	On	Display mode C
Green	On		Display mode D

Setting the display mode

To set the required display mode, press the "SELECT/SET" button.

If you do not press the "SELECT/SET" button for longer than 1 minute, the device automatically changes to display mode A.

Pressing SELECT/SET button starting at display mode A	LED status		Display mode
	DM1	DM2	
-	Off		Display mode A
Press once	On	Off	Display mode B
Press twice	Off	On	Display mode C
Press three times	On		Display mode D

4.8.6 LEDs "L1" and "L2"

The "L1" and "L2" LEDs indicate the current range of the power supply at connectors L1 and L2.

The meaning of the "L1" and "L2" LEDs depends on the set display mode, see section "LEDs "DM1" and "DM2" (Page 36)".

Meaning in display modes A, B, C and E

In the display modes A, B, C and E, you can determine whether the power supply is connected by observing LEDs "L1" and "L2" .

L1/L2 LED		L1/L2 connector
LED color	LED status	
-	Off	No external power supply connected
Green	On	Power supply connected to L1/L2

Meaning in display mode D

In display mode D, the "L1" and "L2" LEDs indicate whether the power supply is monitored.

L1/L2 LED		L1/L2 connector
LED color	**LED status**	
-	Off	Power supply is not monitored. The signal contact does not respond if neither L1 nor L2 is connected to an adequate power supply.
Green	On	Power supply is monitored. The signal contact responds if neither L1 nor L2 is connected to an adequate power supply.

4.8.7 "P" LEDs

The port LEDs "P1", "P2" etc. show information about the corresponding ports.

The meaning of the Port LEDs depends on the set display mode, see section "LEDs "DM1" and "DM2" (Page 36)".

Meaning in display mode A

In display mode A, the port LEDs indicate whether a valid link exists.

LED color	LED status	Meaning
-	Off	No valid link to the port (for example station turned off or cable not connected).
Green	On	Link exists and port in normal status. In this state, the port can receive and send data.
	Flashes once per period*	Link exists and port in "blocking" status. In this state, the port only receives management data (no user data).
	Flashes three times per period*	Link exists and port turned off by management. In this state, no data is sent or received via the port.
	Flashes four times per period*	Link exists and port is in the "monitor port" status. In this state, the data traffic of another port is mirrored to this port.
Yellow	Flashing / lit	Receiving data at port

* 1 period ≙ 2.5 seconds

Meaning in display mode B

In display mode B, the port LEDs indicate the transmission speed.

LED color	LED status	Meaning
-	Off	Port operating at 10 Mbps
Green	On	Port operating at 100 Mbps
Yellow	On	Port operating at 1000 Mbps
Green	Flashing	Port operating at 10 Gbps

If a connection error occurs when the transmission mode is permanently set (autonegotiation off), the target state, i.e. the set transmission speed (10 Gbps, 1 Gbps,

100 Mbps, 10 Mbps), is still displayed. If there is a connection problem and autonegotiation is active, the port LED goes off.

Meaning in display mode C

In display mode C, the port LEDs indicate the mode.

LED color	LED status	Meaning
-	Off	Port operating in half duplex mode
Green	On	Port operating in full duplex mode

Meaning in display mode D

In display mode D, the port LEDs indicate whether the port is monitored.

LED color	LED status	Meaning
-	Off	Port is not monitored.
Green	On	Port is monitored for "Link up". Error handling is triggered when the port changes to the active status. If a link has been established at the port, but it should not be available, the signaling contact indicates an error.
Yellow	On	Port is monitored for "Link down". Error handling is triggered when the port changes to the inactive status. If no valid link has been established at the port (e.g. the communication partner is switched off or the cable is not connected), the signaling contact indicates an error.

4.9 SELECT/SET button

4.9.1 Position

The "SELECT/SET" button is located on the front of the device.

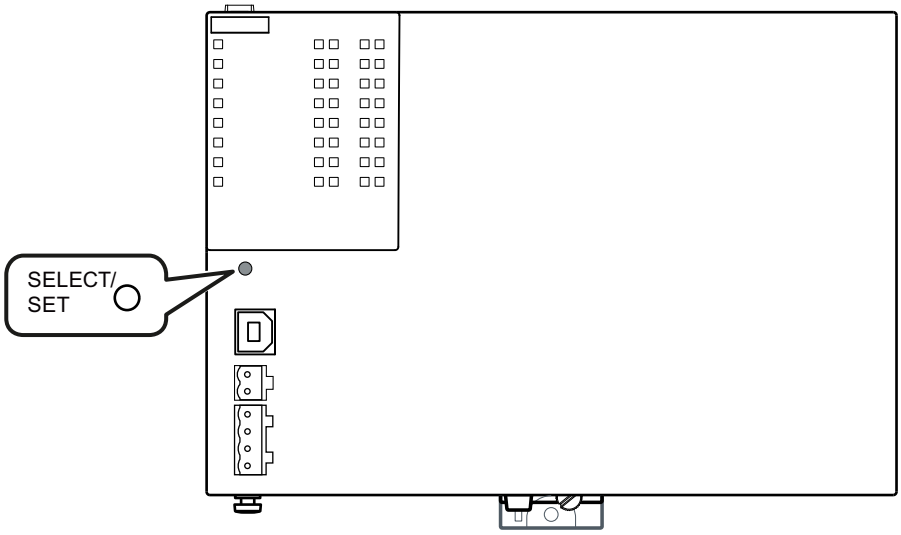


Figure 4-5 Position of the "SELECT/SET" button

4.9.2 Function

The device has a button with the following functions:

- **Reset the device to default settings**
  Please note that the button function distinguishes between the startup phase and running operation.
  For more information, refer to "Resetting the device to default settings with the button (in the startup phase) (Page 77)" and "Resetting the device to default settings with the button (during operation) (Page 78)".
- **Load a firmware file via TFTP**
  For more information, refer to "Loading a firmware file via TFTP (Page 79)".
- **Setting the display mode**
  The display mode is used for diagnostics of the device. Depending on the set display mode, the LEDs of the device show different information and indicate the state of the device.
  For more information, refer to "Setting the display mode (Page 41)".
  For more information on the display modes, refer to "LEDs "DM1" and "DM2" (Page 36)".

4.9.3 Setting the display mode

To set the display mode, press the button as follows:

Pressing the button starting at display mode A	LED status		Display mode
	DM1	DM2	
-	Off		Display mode A
Press once	On	Off	Display mode B
Press twice	Off	On	Display mode C
Press three times	On		Display mode D

Depending on the set display mode, the "L1", "L2" LEDs and the port LEDs show different information.

If you do not press the button for longer than 1 minute, the device automatically changes to display mode A.

4.10 Configuration License PLUG

The Configuration and License PLUG (CLP) is a USB storage medium for backing up and exchanging data and licenses.

The CLP has a USB type C interface and can be used with the following devices that have a corresponding interface:

- Siemens products
- Personal computers (PCs), such as desktop PCs, tablet PCs, laptops, or smartphones

4.10.1 Position

The CLP slot is located on the top of the device.

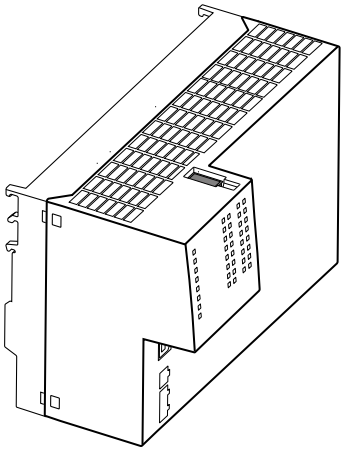


Figure 4-6 Position of the CLP slot

4.10.2 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 CLP **with no data** (default setting) is plugged into a device, the device automatically saves its configuration data on the CLP during the startup phase. After that, it behaves like a CLP with data.
  - If a CLP **with data** is plugged into a device, the device automatically adopts the configuration of the CLP during the startup phase.

  During operation:
  - During operation, changes to the configuration are saved on the CLP and in the internal memory.
  - The configuration data and firmware of the device are 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 hazard - risk 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 pulling and plugging the PLUG can be found in the section "Replacing a CLP (Page 74)".

Installing and removing

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.

⚠ WARNING
If a device is operated in an ambient temperature of more than 40 °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 40 °C.

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

⚠ WARNING
If the temperature of the cable or housing socket exceeds 70 °C or the temperature at the branching points of the cables exceeds 80 °C, special precautions must be taken. If the device is operated at max. ambient temperature, you must use cables with a permitted maximum operating temperature of at least 90 °C for power supply, functional grounding and signaling contact and of at least 75 °C for data cables.

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

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

WARNING
The device is intended for indoor use only.

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

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

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

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

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

Safety notices when using according to FM

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

⚠ WARNING

EXPLOSION HAZARD

For operation the device is intended to be installed within an enclosure/control cabinet. The inner temperature of the enclosure/control cabinet corresponds to the ambient temperature of the device. Use cables with a permitted maximum operating temperature of at least 90 °C for power supply, functional grounding and signaling contact and of at least 75 °C for data cables.

⚠ WARNING

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

⚠ 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

The IP degree of protection marking on the nameplate is not associated with FM approval.

Note

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

Note

Specific Conditions of Use

- The equipment shall be installed in compliance with the enclosure, mounting spacing and segregation requirements of the ultimate application, including a tool-secured cover.
- The maximum ambient temperature range is based on the orientation of the equipment when installed, and shall be as specified in section "Technical specifications (Page 81)" for each module.

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 device is operated at ambient temperatures of over 40 °C, you must use cables with a permitted maximum operating temperature of at least 90 °C for power supply, functional grounding and signaling contact and of at least 75 °C for data cables.

Further notes

NOTICE

Warming and premature aging of the network component due to direct sunlight

Direct sunlight can heat up the device and can lead to premature aging of the network component and its cabling.

Provide suitable shade to protect the network component against direct sunlight.

5.2 Types of installation

The devices can be installed in the following ways:

- DIN rail
- S7-300 standard rail
- S7-1500 standard rail
- Wall mounting

5.3 Installation clearance

Keep to the following minimum clearances so that the convection ventilation of the device is not blocked:

- Below at least 10 cm
- Above at least 10 cm

If you install the device with installation distances < 10 cm, you must observe the following:

- The minimum distance must not be less than 30 mm.
- The maximum permissible ambient temperature in the direct vicinity of the device must be observed.
- Sufficient convection ventilation of the device must be ensured.

5.4 Installation position

The following installation position is recommended:

- **Horizontal** (position 1)
  Horizontal installation of the rack (DIN rail/mounting rail)

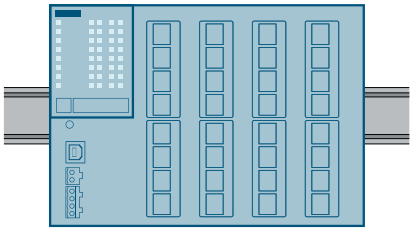


Figure 5-1 Horizontal installation position on a DIN rail

The following installation positions are permitted, but with deviating temperature values (Page 81):

- **Vertical** (position 2)
  Vertical installation of the rack (DIN rail/mounting rail)

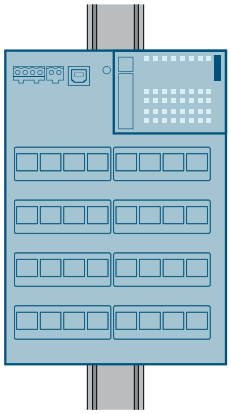


Figure 5-2 Vertical installation position on a DIN rail

- **Ceiling installation/Face down** (position 3)
  The device is installed on the ceiling of a control cabinet, for example.
- **Floor installation/Face up** (position 4)
  The device is installed on the floor of a control cabinet, for example.

Note

Other installation positions are not permitted.

Cooling

The devices do not require any air flow generated by a fan for cooling in the control cabinet.

SFP transceivers

Information about pulling and plugging SFP or SFP+ plug-in transceivers can be found in the section "Inserting and removing pluggable transceivers (Page 70)".

5.5 Mounting on DIN rails

Installation

Note

Note the position of the securing bar, see also section “Dimension drawings (Page 89)“.

When supplied, the securing bar is in the wall mounting position. To change the position of the securing bar, refer to the section “Changing the position of the securing bar (Page 53)“.

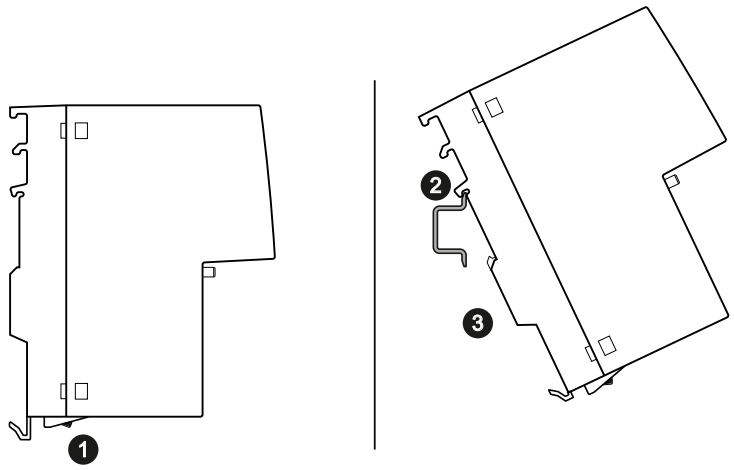


Figure 5-3 DIN rail mounting with securing bar in the wall mounting position.

Securing bar in the wall mounting position (as supplied).

To install the device on a 35 mm DIN rail complying with DIN EN 60715, follow the steps below:

1. Loosen the knurled screw with your hand or a screwdriver.
2. Place the third housing guide of the device on the top edge of the DIN rail.
3. Press the device down against the DIN rail until the spring securing bar locks in place.
4. When you tighten the knurled screw. you cannot release the securing bar (torque 0.5 Nm). The device is additionally fixed.
5. Connect the electrical connecting cables, refer to the section "Connecting up (Page 55)".

Removal

To remove the device from a DIN rail, follow the steps below:

1. Disconnect all connected cables.
2. If necessary, loosen the knurled screw with your hand or a screwdriver.
3. Lever the securing bar down using a screwdriver as far as it will go.
4. Pull the device away from the bottom of the DIN rail with the bar pulled.

5.6 Installation on a standard S7-300 rail

Installing on an S7-300 standard rail

Note

Note the position of the securing bar, see also section “Dimension drawings (Page 89)“.

When supplied, the securing bar is in the wall mounting position. To change the position of the securing bar, refer to the section “Changing the position of the securing bar (Page 53)“.

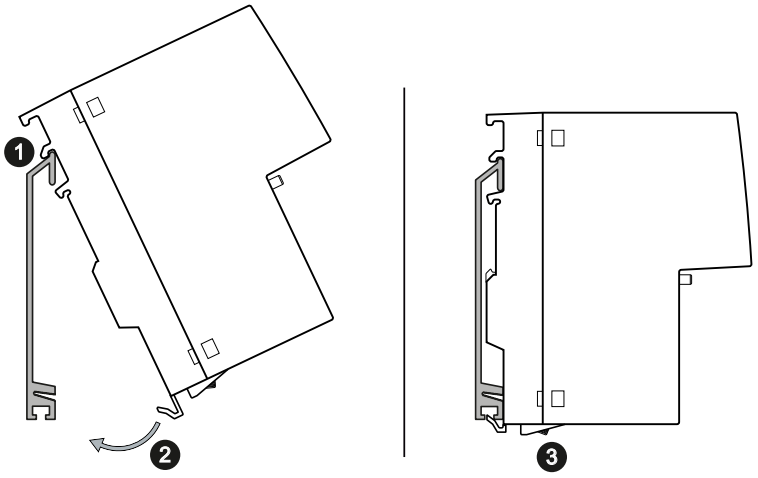


Figure 5-4 S7-300 mounting rail installation with the securing bar in the wall mounting position.

Securing bar in the wall mounting position (as supplied).

To install the device on an S7-300 standard rail, follow the steps below:

1. Place the second housing guide of the device on the top edge of the standard rail.
2. Swing the device down towards the back against the mounting rail.
3. Loosen the knurled screw with your hand or a screwdriver. The spring mounted securing bar locks in place.
4. When you tighten the knurled screw. you cannot release the securing bar (torque 0.5 Nm). The device is additionally fixed.
5. Connect the electrical connecting cables, refer to the section "Connecting up (Page 55)".

Removal

To remove the device from a standard rail, follow the steps below:

1. Disconnect all connected cables.
2. If necessary, loosen the knurled screw with your hand or a screwdriver.
3. Lever the securing bar down using a screwdriver as far as it will go.
4. Remove the device from the mounting rail with the bar pulled.

5.7 Installation on a standard S7-1500 rail

Installing on an S7-1500 standard rail

Note

Note the position of the securing bar, see also section “Dimension drawings (Page 89)“.

When supplied, the securing bar is in the wall mounting position. To change the position of the securing bar, refer to the section “Changing the position of the securing bar (Page 53)“.

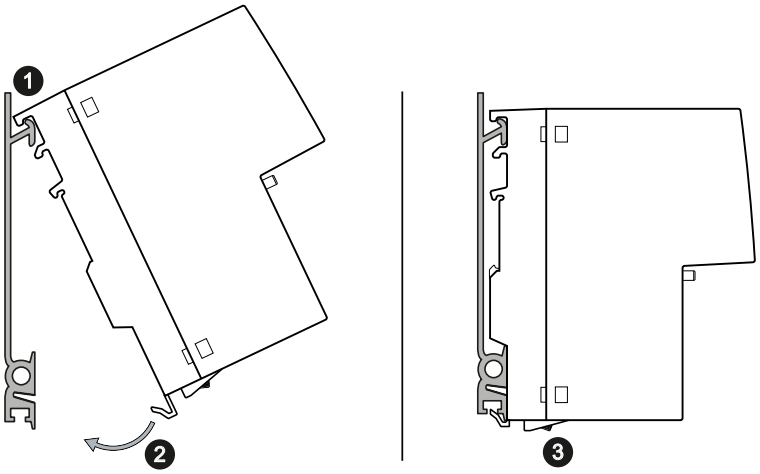


Figure 5-5 S7-1500 mounting rail installation with the securing bar in the wall mounting position.

Securing bar in the wall mounting position (as supplied).

To install the device on an S7-1500 standard rail, follow the steps below:

1. Place the first housing guide of the device on the top edge of the standard rail.
2. Swing the device down towards the back against the mounting rail.
3. Loosen the knurled screw with your hand or a screwdriver. The spring mounted securing bar locks in place.
4. When you tighten the knurled screw. you cannot release the securing bar (torque 0.5 Nm). The device is additionally fixed.
5. Connect the electrical connecting cables, refer to the section "Connecting up (Page 55)".

Removal

To remove the device from a standard rail, follow the steps below:

1. Disconnect all connected cables.
2. If necessary, loosen the knurled screw with your hand or a screwdriver.
3. Lever the securing bar down using a screwdriver as far as it will go.
4. Remove the device from the mounting rail with the bar pulled.

5.8 Wall mounting

Preparation

Note the position of the securing bar, see also section “Dimension drawings (Page 89)“.

When supplied, the securing bar is in the wall mounting position. You do not need to prepare the device any further.

If the securing bar is in the rail mounting position, note the section “Changing the position of the securing bar (Page 53)“.

Tools

To mount the device on a wall, you require the following:

- 2 wall plugs with a diameter of 6 mm and a minimum length of 35 mm.
- 2 oval-head screws with a diameter of 3.5 mm to 4 mm and a minimum length of 50 mm.

Note

Use suitable fitting material depending on the mounting surface.

Mounting on a concrete wall

The following table shows the size of the drill hole and the required fastening material using a concrete drill hole as an example:

Base	Concrete	
Drill hole	Depth	Min. 45 mm
	Diameter	6 mm
Fastening material	Plugs	6 x 35
	Oval-head screws	4 x 50

Assembly

Note

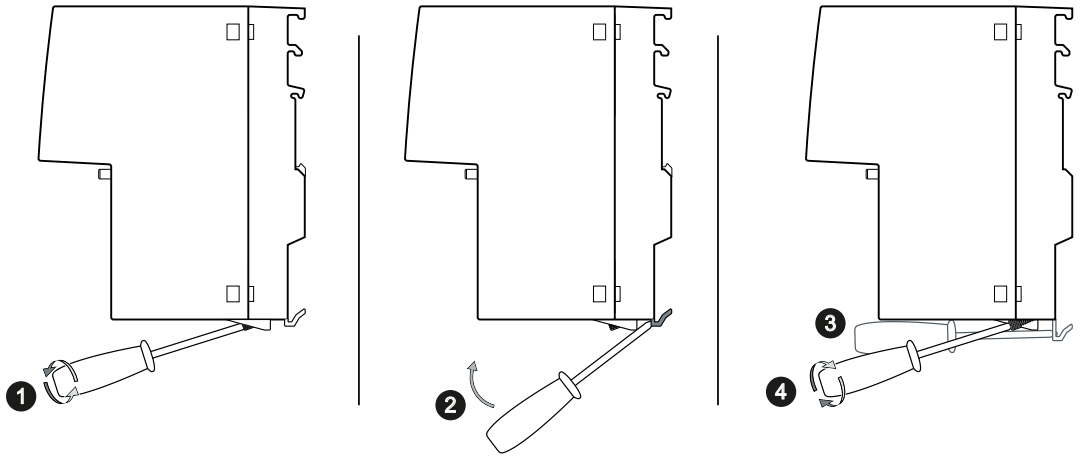
The wall mounting must be capable of supporting at least four times the weight of the device.

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

1. Prepare the wall mounting with drilled holes and plugs. For the precise dimensions, refer to the section "Dimension drawings (Page 89)".
2. Turn the upper screw in to the wall so that 10 mm remains jutting out.
3. Hang the device with the keyhole hanging mechanism on the rear on the screw.
4. Fix the device to the wall with the lower screw.
5. Connect the electrical connecting cables, refer to the section "Connecting up (Page 55)".

5.9 Changing the position of the securing bar

Rail mounting position - wall mounting position



To change the securing bar from the rail mounting position to the wall mounting position follow the steps below:

1. If necessary, loosen the knurled screw with your hand or a screwdriver.
2. Move the securing bar down as far as it will go.
   - Use the levering aid and level the securing bar down using a screwdriver into this position.
   - Push the securing bar down using your hand.
3. Hold the securing bar in this position.
   - Hold the securing bar with the screwdriver.
   - Use the gap on the rear of the device and fix the securing bar briefly with a pin.
4. Tighten the knurled screw (torque 0.5 Nm).
   The securing bar is fixed in the wall mounting position.
5. Remove the pin.

Wall mounting position - rail mounting position

To move the securing bar from the wall mounting position to the rail mounting position, loosen the knurled screw.

5.10 Disassembly

⚠ WARNING

Improper disassembly

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

For proper disassembly, observe the following:

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

Connecting up

6

6.1 Safety when connecting up

Safety notices for operation with a power supply according to NEC Class 2

If you are operating the device with a power supply in accordance with NEC Class 2, observe the safety instructions listed below when connecting the device.

⚠ WARNING

Power supply

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

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

- The conditions for ES1, PS2 according to IEC/EN/UL 62368-1 or SELV/LPS according to IEC/UL/EN 60950-1
- The conditions for NEC Class 2 according to the National Electrical Code (r) (ANSI/NFPA 70)

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

⚠ WARNING

Power supply

The device is designed for operation with a directly connectable power supply according to UL/IEC 61010-1 and UL/IEC 61010-2-201 whose output power corresponds to "Limited Energy" according to UL/IEC 61010-1.

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

NOTICE

Suitable fuse for the power supply cables (corresponds to "Limited Energy")

The current on the terminal must not exceed 3 A[2)]. Use a fuse for the power supply that is suitable for protection of AC/DC power supply circuits[1)] and protects against currents > 3 A[2)].

- In areas subject to the NEC or CEC, the fuse must meet the following requirements:
  - Suitable for AC/DC[1)] (min. 60 V / 3 A[2)])
  - Breaking current at least 10 kA
  - Approval according to ANSI/UL 248-14 (suppl. fuses), ANSI/UL 248-4 (Class CC), ANSI/UL 248-8 (J), ANSI/UL 248-15 (T), or CSA C22.2-4 No. 248.14 (suppl. fuses), No. 248-4 (Class CC), No. 248-8 (J), No. 248-15 (T)
- In other areas, the fuse must meet the following requirements:
  - Suitable for AC/DC[1)] (min. 60 V / 3 A[2)])
  - Breaking current at least 10 kA
  - Approval according to IEC/EN 60947-1/2/3 or IEC/EN 60898-1/2 for circuit breakers
  - Breaking characteristics: B or C
  - Approval according to IEC/EN 60127-1 for fuses
  - Breaking characteristics: Max. 120 s at 2 x I_n (corresponds to melting integral $I^2t < 4320$)

If the properties of the supplying current source are known, the following fuse is also possible:

- In areas subject to the NEC or CEC, the fuse must meet the following requirements:
  - Suitable for AC/DC[1)] (min. 60 V / 3 A[2)])
  - Breaking current > highest possible current of the current source (incl. short circuit current and fault)
  - Approval according to UL 1077 or CSA C22.2 No. 235
- In other areas, the fuse must meet the following requirements:
  - Suitable for AC/DC[1)] (min. 60 V / 3 A[2)])
  - Breaking current > highest possible current of the current source (incl. short circuit current and fault)
  - Approval according to IEC/EN 60934
  - Breaking characteristics: max. 120s at 2 x I_n

You do not need to fuse the connecting cable in the following cases:

- For devices with approval according to UL 62368:
  If you only use current sources with a limited power source (LPS) or current sources according to NEC Class 2 or PS2/LPS for the power supply of the devices.
- For devices with approval according to UL 61010:

If you only use current sources with "Limited Energy" or current sources according to NEC Class 2 for the power supply of the devices.

[1] Depending on the type of current of the power supply

[2] The fuse rating of 3 A applies to devices with a rated voltage of ≤ 24 V ± a tolerance of 30%. For devices with a larger rated voltage (incl. tolerance), you need to adjust the fuse rating accordingly. The maximum available power on the terminals must not exceed 100 VA.
If you operate a device with a redundant power supply (two separate power supplies), the fuse rating applies to the combination of the two power supplies. Depending on the relevant standard, the maximum permissible fuse rating is limited to 8 A.

Further notes

WARNING

Insulation of external power supplies

Ext. circuits intended to be connected to this device shall be galv. separated from hazardous live voltage by reinforced or double insulation.

WARNING

Safety notice for connecting with a LAN ID (Local Area Network)

A LAN or LAN segment with all the interconnected devices should be contained completely in a single low voltage power distribution in a building. The LAN is designed either for "Environment A" according to IEEE802.3 or "Environment 0" according to IEC TR 62102.

Do not connect any electrical connectors directly to the telephone network (telephone network voltage) or a WAN (Wide Area Network).

Note

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.

Note

The temperature stability of cables connected to terminals must be at least 90 °C for power supply, functional grounding and signaling contact, and at least 75 °C for data cables.

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 SELECT/SET button when there is an explosive atmosphere.

WARNING

Unsuitable cables or connectors

Risk of explosion in hazardous areas

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

WARNING

Lack of equipotential bonding

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

- Ensure that equipotential bonding is available for the device.

WARNING

Unprotected cable ends

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

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

⚠ WARNING

Improper installation of shielded cables

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

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

⚠ WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

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

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

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

⚠ WARNING

Transient overvoltages

Take measures to prevent transient surges of more than 40% of the rated voltage. Under no circumstances may transient surges exceed 119 V. This is the case if you only operate devices with SELV (safety extra low voltage).

⚠ WARNING

Suitable cables at high ambient temperatures in hazardous area

If the device is operated at max. ambient temperature, you must use cables with a permitted maximum operating temperature of at least 90 °C for power supply, functional grounding and signaling contact and of at least 75 °C for data cables. 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 the device according to Hazardous Locations (HazLoc)

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

WARNING

EXPLOSION HAZARD

You may only connect or disconnect cables carrying electricity when the power supply is switched off or when the device is in an area without inflammable gas concentrations.

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

Do not disconnect while circuit is live unless area is known to be non-hazardous.

6.2 Wiring rules

When wiring use cables with the following AWG categories or cross sections.

Wiring rules for ...		**Screw/spring-loaded terminals**
connectable cable cross sections for flexible cables ...	without wire end ferrule	0.25 - 2.5 mm^2
		AWG: 24 - 13
	with wire end ferrule with plastic ferrule**	0.25 - 2.5 mm^2
		AWG: 24 - 13
	with wire end ferrule without plastic ferrule**	0.25 - 2.5 mm^2
		AWG: 24 - 13
	with TWIN wire end ferrule**	0.5 - 1 mm^2
		AWG: 20 - 17
Stripped length of the cable		8 - 10 mm
Wire end ferrule according to DIN 46228 with plastic ferrule**		8 - 10 mm

* AWG: American Wire Gauge

** See note "Wire end ferrules"

Note

Wire end ferrules

Use crimp shapes with smooth surfaces, such as provided by square and trapeze shaped crimp cross sections.

Crimp shapes with wave-shaped profile are unsuitable.

6.3 Power supply

Notes on the power supply

⚠ WARNING

Operation only with safety extra low voltage

The equipment is designed for operation with a directly connectable safety extra low voltage (SELV).

- Do not operate the device with DC voltage higher than 32 V DC or AC voltage.

⚠ CAUTION

Damage to the device due to overvoltage

The connector of the external power supply is not protected against strong electromagnetic pulses that can, for example, result from lightning strikes or switching large loads.

One of the tests used to attest the immunity of the device to electromagnetic interference is the "surge immunity test" according to EN 61000-4-5. This test requires overvoltage protection for the power supply lines. A suitable device is, for example, the Dehn Blitzductor BVT AVD 24, article number 918 422 or a comparable protective element.

Manufacturer: DEHN+SOEHNE GmbH+Co. KG, Hans-Dehn-Str.1, Postfach 1640, D92306 Neumarkt, Germany

Operate the device with suitable overvoltage protection.

Note

The device can be disconnected from the power supply by pulling off the terminal block.

Information on the power supply

- The "L1" and "L2" LEDs indicate the current range of the power supply, see the section "LEDs "L1" and "L2" (Page 37)".
- You can use two 2-pin terminal blocks or one 4-pin terminal block (spring-loaded terminal) to connect the power supply.
  If you use two 2-pin terminal blocks, you can disconnect only the affected power supply from the device to perform repairs.
  Two 2-pin terminal blocks are included in the scope of delivery of the device. You can order 2- and 4-pin terminal blocks as spare parts, see section "Spare parts".
- The power supply can be connected redundantly. Both inputs are isolated. There is no distribution of load. When a redundant power supply is used, the power supply unit with the higher output voltage supplies the device alone.
- The power supply is connected over a high resistance with the enclosure to allow an ungrounded set up. The two power inputs are non-floating.

- Note the wiring rules (Page 60).
- The power supply must meet the requirements in relation to RF radiation according to IEC 61000-4-3/NAMUR NE21 so that the overall system meets these requirements; see also "RF radiation according to NAMUR NE21 (Page 88)".

Position and assignment

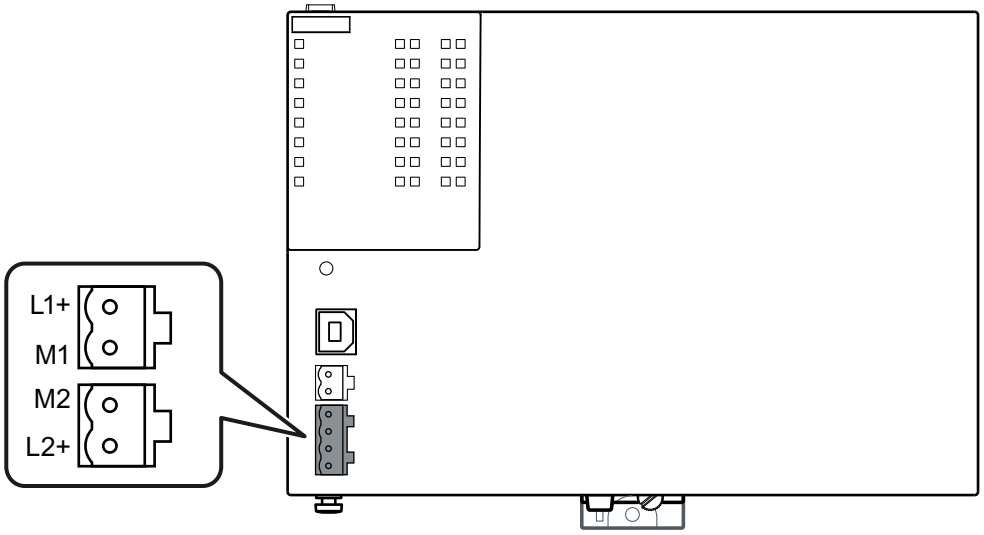


Figure 6-1 Position of the power supply and assignment of the terminal block

Contact	Assignment
L1+	24 V DC
M1	Ground
M2	Ground
L2+	24 V DC

6.4 Functional ground

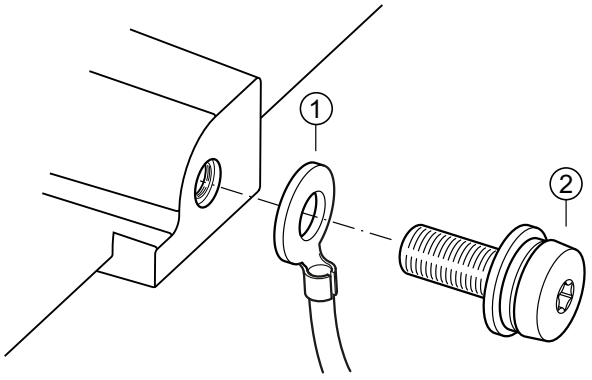
EMC disturbances are diverted to ground via the functional ground. This ensures the immunity of the data transmission.

The functional ground must be implemented with low impedance. The connection of the functional ground must be established directly on the mounting plate or the DIN rail terminal.

The IE switch has a grounding screw (fillister head screw with clamping washer und disk) for functional ground, refer to the section "Device views (Page 27)".

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

Follow the steps below to connect the functional ground:



① Grounding terminal with cable
② Fillister head screw with spring washer and washer

1. Loosen the grounding screw).
2. Put the grounding terminal and grounding screw together.
3. Tighten the grounding screw with a maximum torque of 0.75 Nm.

Protective/functional ground

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

Apart from the protective ground, 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.

6.5 Industrial Ethernet

6.5.1 Electrical

Note

Strain relief for the Ethernet cables

In order to avoid mechanical stress on the Ethernet cables and resulting interruption of the contact, fasten the cables at a short distance from the connector using a cable guide or busbar.

Note

Unlocking the plug with a screwdriver

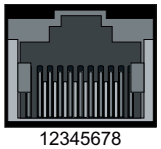
If installation space is limited, you can unlock the connectors using a screwdriver, see also "SIMATIC NET: IE FC RJ45 Plug 4x2 CAT 6A (https://support.industry.siemens.com/cs/ww/en/view/102047916)".

R-45 connector technology

The attachment to Industrial Ethernet uses RJ-45 connected technology with MDI-X assignment.

Pin assignment

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

Pin number	Assignments for ports up to			RJ45 connector
	Max. 100 Mbps	Max. 1000 Mbps	Max. 10000 Mbps	
Pin 1	RD+	D1+	D1+	 12345678
Pin 2	RD-	D1-	D1-	
Pin 3	TD+	D2+	D2+	
Pin 4	n. c. (Not connected)	D3+	D3+	
Pin 5	n. c. (Not connected)	D3-	D3-	
Pin 6	TD-	D2-	D2-	
Pin 7	n. c. (Not connected)	D4+	D4+	
Pin 8	n. c. (Not connected)	D4-	D4-	

MDI / MDI-X autocrossover

With the MDI/MDI-X autocrossover function, the send and receive contacts of an Ethernet port are assigned automatically. The assignment depends on the cable with which the communications partner is connected. This means that it does not matter whether the port is connected using a patch cable or crossover cable. This prevents malfunctions resulting from mismatching send and receive wires. This makes installation much easier for the user.

Note

Formation of loops

Please note that the direct connection of two ports on the IE switch or accidental connection over several IE switches causes an illegal loop. Such a loop can lead to network overload and network failures.

Autonegotiation

Autonegotiation means the automatic detection/negotiation of the transmission rate and the operating mode of ports at the opposite end. This makes it possible to configure different devices automatically.

Two components connected to a link segment can exchange information about the transfer and can adapt their settings to each other. The mode with the highest possible speed is set.

Note

- If a port is set permanently to full duplex, the connected partner port must also be set to full duplex.
- If a port operating in the "Auto negotiation" mode is connected to a partner port that is not operating in the"Auto negotiation" mode, the partner port setting must be fixed at 100 Mbps or 10 Mbps half duplex mode.
- If you disable the "Auto negotiation" function, the "MDI/MDI-X autocrossover" function remains active.

Fast Retrain

The devices support the Fast Retrain function in accordance with standard IEEE 802.3. The Fast Retrain function ensures that no link interruptions occur in the case of electromagnetic interferences (EMI) on the connection cable to the partner.

If a Fast Retrain event occurs, the device tries to reestablish the communication to the partner device for a duration of up to 30 ms. Only if this is unsuccessful, is the link disconnected.

During the Fast Retrain procedure no telegrams are transferred via the affected connection.

Note

The function is always enabled and cannot be deactivated.

The function is relevant only for 10 Gbps ports.

There are no Fast Retrain events for port speeds ≤ 1 Gbps.

6.5.2 Optical

NOTICE
Failure of the data traffic due to contamination of optical plug-in connections Optical sockets and plugs are sensitive to contamination of the end face. Contamination can lead to the failure of the optical transmission network. Take the following precautions to avoid functional impairments: • Clean the end face of field-assembled connectors carefully before connecting. No residues of processing may remain on the connector. • Only remove the dust caps of optical transceivers and pre-configured cables shortly before connecting the cables. • Close unused optical sockets and plugs as well as pluggable transceivers and slots with the supplied protective caps.

LC connector technology

The attachment to Industrial Ethernet uses LC connector technology (Lucent Connector).



Pluggable transceiver slot/ plugged in transceiver

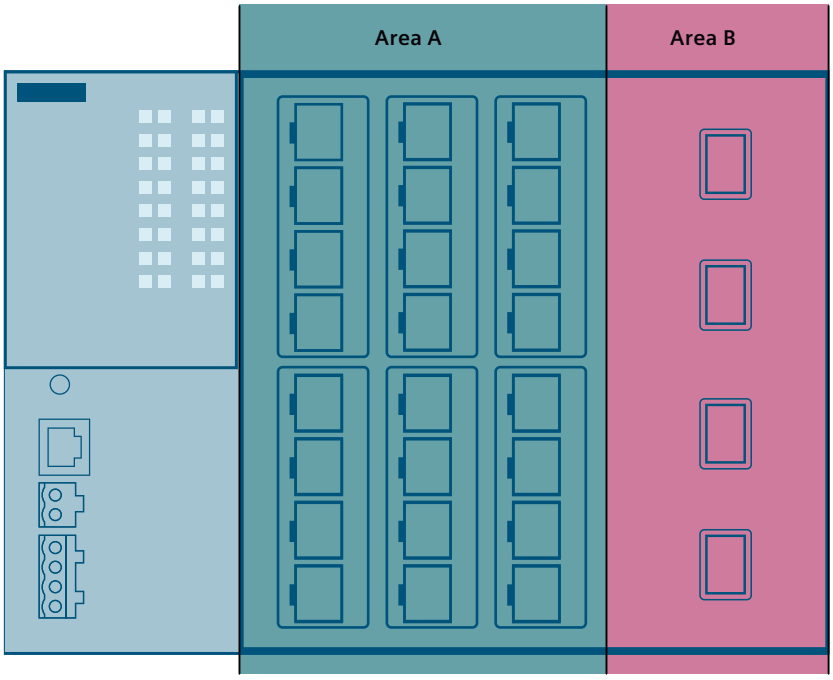
6.5.3 Dependency between ports and ambient temperature (derating)

The figures in this section show which ports you can use in which area so that the maximum ambient temperature specified in the left-hand column is permissible.

The table below shows the assignment of the SFP transceivers to the specified groups.

Category	Group	Type	Article number
SFP	Group 1	SFP991-1	6GK5 991-1AD00-8AA0
		SFP991-1 (C)	6GK5 991-1AD00-8FA0
		SFP991-1LD	6GK5 991-1AF00-8AA0
		SFP992-1	6GK5 992-1AL00-8AA0
		SFP992-1LD	6GK5 992-1AM00-8AA0
		SFP992-1LD (C)	6GK5 992-1AM00-8FA0
	Group 2	SFP991-1LH+	6GK5 991-1AE00-8AA0
		SFP991-1ELH200	6GK5 991-1AE30-8AA0
		SFP992-1+	6GK5 992-1AG00-8AA0
		SFP992-1LD+	6GK5 992-1AM30-8AA0
		SFP992-1LH	6GK5 992-1AN00-8AA0
		SFP992-1LH+	6GK5 992-1AP00-8AA0
		SFP992-1ELH	6GK5 992-1AQ00-8AA0
		SFP992-1BXMT	6GK5 992-1AL00-8TA0
		SFP992-1BXMR	6GK5 992-1AL00-8RA0
		SFP992-1BX10T	6GK5 992-1AM00-8TA0
		SFP992-1BX10R	6GK5 992-1AM00-8RA0
SFP+	Group 1	SFP993-1	6GK5 993-1AT00-8AA0
		SFP993-1 (C)	6GK5 993-1AT00-8FA0
		SFP993-1LD	6GK5 993-1AU00-8AA0
		SFP993-1LD (C)	6GK5 993-1AU00-8FA0
	Group 2	SFP993-1LH	6GK5 993-1AV00-8AA0
		SFP993-1LH+	6GK5 993-1AW00-8AA0

6.5.3.1 Devices with 4 SFP/SFP+ slots



Temperature Horizontal installation position (position 1)	Area A	Area B
-40 °C ... 60 °C *)	RJ45 to 1 Gbps	SFP group 1
-40 °C ... 55 °C **)	RJ45 to 1 Gbps	SFP group 1 SFP group 2 SFP+ group 1 Restriction 1)
-40 °C ... 40 °C	RJ45 to 1 Gbps	SFP group 1 SFP group 2 SFP+ group 1 SFP+ group 2 Restriction 2)

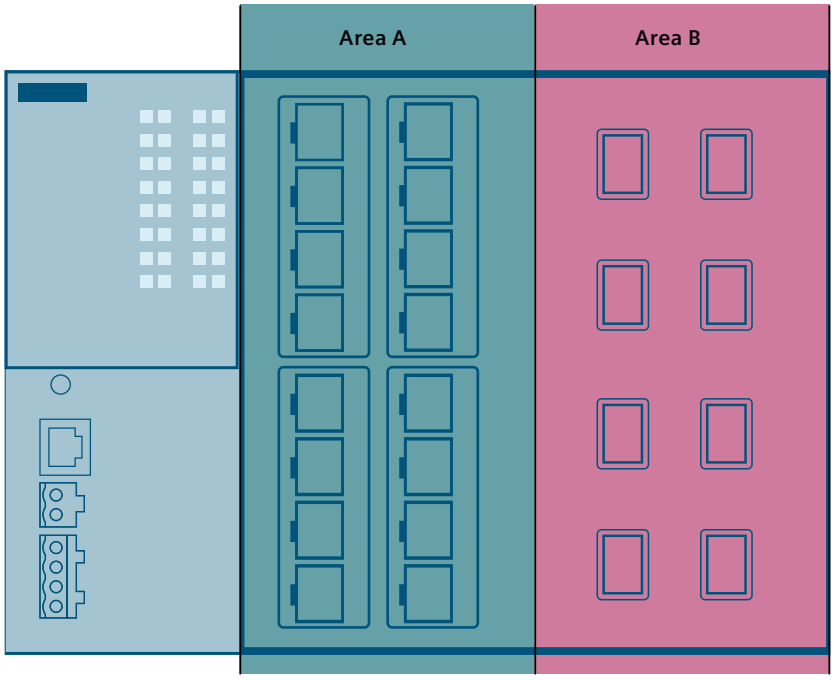
1) SFP transceivers of the type SFP993-1 (C) cannot be used. SFP transceivers of the SFP group 2 can be used in a maximum of two of these ports. Only use the P27 and P28 slots for this. The remaining ports of the area can be filled with SFP transceivers from SFP group 1 or SFP+ group 1.

2) SFP transceivers from the SFP group 2 or SFP+ group 2 can be used in a maximum of two of these ports. Only use the P27 and P28 slots for this. If you use SFP transceivers from SFP+ group 2, only the horizontal installation position (position 1) is permissible. The remaining ports of the area can be filled with SFP transceivers from SFP group 1 or SFP+ group 1.

*) The installation positions 2, 3 and 4 reduce the maximum temperature to 50 °C.

*) The installation positions 2 and 3 reduce the maximum temperature to 50 °C. The installation position 4 reduces the maximum temperature to 40 °C.

6.5.3.2 Devices with 8 SFP/SFP+ slots



Temperature Horizontal installation position (position 1)	Area A	Area B
-40 °C ... 60 °C *)	RJ45 to 1 Gbps	SFP group 1
-40 °C ... 55 °C **)	RJ45 to 1 Gbps	SFP group 1 SFP group 2 SFP+ group 1 Restriction 1)
-40 °C ... 40 °C	RJ45 to 1 Gbps	SFP group 1 SFP group 2 SFP+ group 1 SFP+ group 2 Restriction 2)

1) SFP transceivers of the type SFP993-1 (C) cannot be used. SFP transceivers of the SFP group 2 can be used in a maximum of two of these ports. Only use the P19, P20, P23 or P24 slots for this. The remaining ports of the area can be filled with SFP transceivers from SFP group 1 or SFP+ group 1.

2) SFP transceivers from the SFP group 2 or SFP+ group 2 can be used in a maximum of two of these ports. Only use the P19, P20, P23 or P24 slots for this. If you use SFP transceivers from SFP+ group 2, only the horizontal installation position (position 1) is permissible. The remaining ports of the area can be filled with SFP transceivers from SFP group 1 or SFP+ group 1.

*) The installation positions 2, 3 and 4 reduce the maximum temperature to 50 °C.

*) The installation positions 2 and 3 reduce the maximum temperature to 50 °C. The installation position 4 reduces the maximum temperature to 40 °C.

6.5.4 Inserting and removing pluggable transceivers

6.5.4.1 General notes for SFP transceivers

⚠ WARNING

Use only approved plug-in transceivers

If you use plug-in transceivers that have not been approved by Siemens AG, there is no guarantee that the device will function according to its specifications.
If you use unapproved plug-in transceivers, this can lead to the following problems:

- Damage to the device
- Loss of the approvals
- Violation of the EMC regulations

Use only approved plug-in transceivers.

Note

Plugging and pulling during operation

You can plug and pull plug-in transceivers with the device in operation.

Note

LASER Class 1

All plug-in transceivers you use in the devices must comply with LASER Class I according to IEC/EN 60825-1. All plug-in transceivers from Siemens AG comply with LASER Class I according to IEC/EN 60825-1.

Documentation for plug-in transceivers

You will find detailed information in the operating instructions of the plug-in transceivers, see the chapter "Introduction (Page 7)" section "Additional documentation".

6.5.4.2 Inserting a plug-in transceiver (SFP/SFP+)

Follow the steps below to insert a pluggable transceiver:

1. Remove the sealing plug of the pluggable transceiver slot.
2. Close the clip of the pluggable transceiver.
3. Insert the pluggable transceiver in the pluggable transceiver slot until you hear it engage. The pluggable transceiver is then firmly secured.
4. Insert the connecting cable into the pluggable transceiver until you hear it engage. The connecting cable is then firmly secured.

6.5.4.3 Removing a pluggable transceiver (SFP/SFP+)

Notes on deinstallation



⚠ CAUTION

Risk of burns due to the high temperatures of the pluggable transceiver

The pluggable transceivers can be plugged and pulled during operation. Leave the transceiver to cool down.

Procedure

Follow the steps below to remove a pluggable transceiver:

1. Remove the connecting cable of the pluggable transceiver.
2. Open the clip of the pluggable trabsceiver.
3. Remove the pluggable transceiver from the pluggable transceiver slot.

   Note

   Do not use force

   It must be possible to remove the pluggable transceiver easily and without applying any force.

4. Close the pluggable transceiver slot with a sealing plug.

6.6 Signaling contact

Information on the signaling contact

- The signaling contact is a floating switch that signals error states by interrupting the contact. If an error occurs, the signaling contact opens. In normal operation, the signaling contact is closed.
- The signaling contact is connected using a 2-pin plug-in terminal block (spring-loaded terminal). The terminal block is included in the scope of delivery of the device and can be ordered as a spare part, see section "Spare parts".
- Note the wiring rules (Page 60).
- The signaling contact can be controlled manually via the user interfaces. Information on this can be found in the Configuration manuals (Page 8).

⚠ WARNING

Risk of electric shock and property damage due to voltage being too high

The signaling contact can be operated in the voltage range of 19.2 to 31.2 V DC or 19.2 to 30.0 V AC and subjected to a maximum load of 100 mA.

With higher voltages or currents, there is a risk of electric shock and damage to the device.

Position and assignment

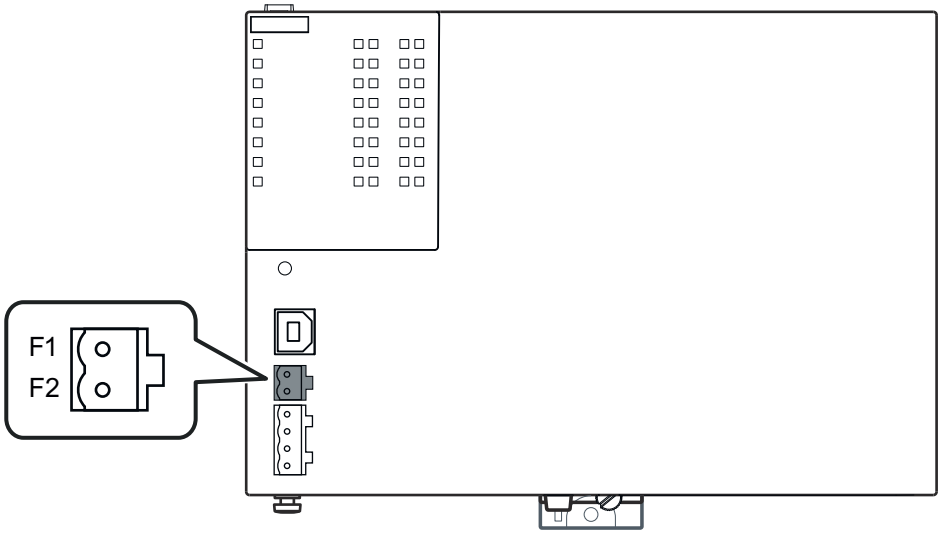


Figure 6-2 Position of the signaling contact and assignment of the terminal block

Contact	Assignment
F1	Fault contact 1
F2	Fault contact 2

Signaling faults

- The signaling of errors by the signaling contact is synchronized with the fault LED "F", see section ""F" LED (Page 35)".
  All errors that the fault LED "F" indicates (freely configurable) are also signaled by the signaling contact.
- If an internal fault occurs, the fault LED "F" lights up and the signaling contact opens.
- If you connect a communications node to an unmonitored port or disconnect it, this does not cause an error message.
- The signaling contact remains open until one of the following events occurs:
  - The problem is eliminated.
  - The current status is entered in the fault mask as the new desired status.

6.7 USB console interface

Information on the USB console interface

- Via the USB console interface on the device (USB socket Type B), you can access the device directly via a virtual serial interface (115200 8N1) without assigning an IP address.
- Access to the device is possible independent of the Ethernet ports.
- To connect the USB console interface to a PC, you require a cable with a USB Type B plug and USB Type A plug. The connecting cable for the USB console interface can be ordered as accessory; see section "Accessories (Page 31)".

Driver for the USB console interface

To use the USB console interface under Windows, you must download and install the following driver: Drivers (https://support.industry.siemens.com/cs/ww/en/ps/6GK5998-3GS00-2AC2/dl).

Position

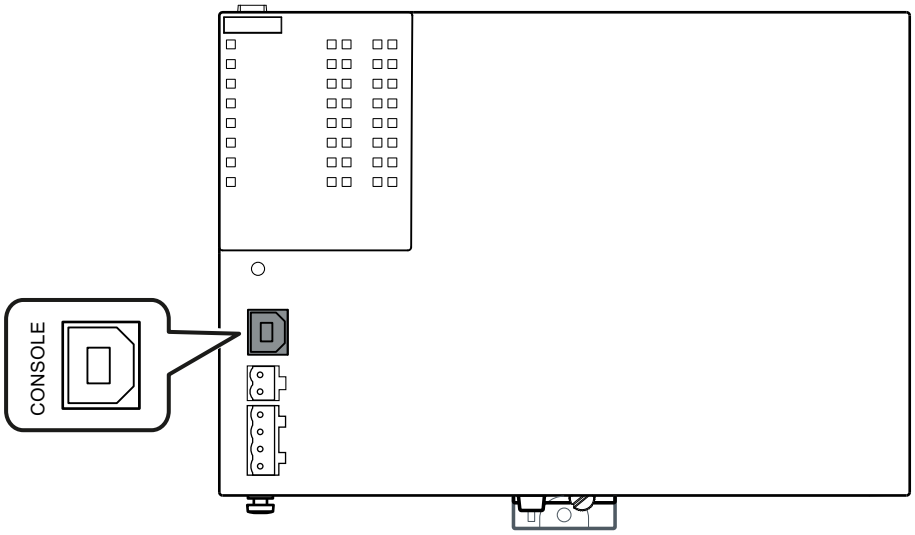
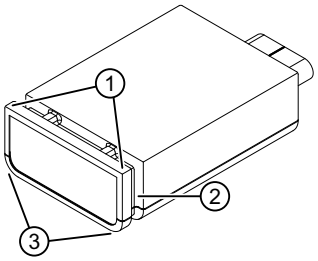


Figure 6-3 Position of the USB console interface (USB socket Type B)

6.8 Replacing a CLP

To use the CLP correctly, note the structure of the CLP:



① Square edges
② Front edge of the CLP
③ Round edges

Removing a CLP

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

1. Turn off the power to the device.
2. To release the CLP, insert a screwdriver between the front edge of the CLP ② and the slot.
3. Remove the CLP from the slot.

Inserting the CLP

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

1. Turn off the power to the device.
2. The CLP housing has two square ① and two round ③ edges. Accordingly, the slot opening has two square and two round edges. Note this orientation when inserting the CLP. Insert the CLP in the correct orientation into the slot.

Maintenance and cleaning

7

⚠ WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

- Repair work may only be performed by personnel authorized by Siemens.
- For function checks, maintenance and servicing work, you need to observe the requirements on checking and maintaining plants in hazardous areas according to the standards EN / IEC 60079-17.

⚠ WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

- Only use original accessories (Page 31) 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 Resetting the device to default settings with the button (in the startup phase)

NOTICE
Connection hazard - risk of communication failure
Depending on the configuration of your network, a reset device can cause circular frames and thus the loss of data traffic.

NOTICE
Configuration hazard - risk of data loss
If a CLP is inserted in the device, the CLP is also reset to default settings.

Note

When you reset the device to the default settings, all configurations are deleted, including:

- The IP address
- The created user
- The passwords
- The user-defined keys and certificates

Following this, the device can only be reached via the serial interface.

If you assign an IP address to the device via DHCP or DCP (e.g. SINEC PNI), you can access the CLI and WBM of the device via a network connection with a preset user profile.

Note

Reset despite disabled "SELECT/SET" button

Using the "SELECT/SET" button, you can always reset the device parameters to the factory settings during the startup phase of the device. This applies also if the "Reset to Factory Defaults" function was disabled in the configuration. This allows you to reset the device to the factory defaults in an emergency.

If the function has been disabled in the configuration, it is only disabled on completion of the startup phase.

Resetting the device to factory defaults

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. Now press the "SELECT/SET" button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red error LED **F** stops flashing and is permanently lit.
4. Now release the button and wait until the fault LED **F** goes off again.
5. The device starts automatically with the factory defaults.

8.2 Resetting the device to default settings with the button (during operation)

NOTICE
Connection hazard - risk of communication failure Depending on the configuration of your network, a reset device can cause circular frames and thus the loss of data traffic.

NOTICE
Configuration hazard - risk of data loss If a CLP is inserted in the device, the CLP is also reset to default settings.

Note

When you reset the device to the default settings, all configurations are deleted, including:

- The IP address
- The created user
- The passwords
- The user-defined keys and certificates

Following this, the device can only be reached via the serial interface.

If you assign an IP address to the device via DHCP or DCP (e.g. SINEC PNI), you can access the CLI and WBM of the device via a network connection with a preset user profile.

Requirement

- The device is in operation.
- The "Reset to factory defaults**"** button function is enabled.
  You can enable or disable this button function. For more information, refer to "Additional documentation (Page 8)".

Resetting the device to factory defaults

To reset the device to default settings during operation, do the following:

1. Switch the device to display mode **A**.
   Display mode **A** is active if the LEDs **DM1** and **DM2** are unlit.
   If the **DM1** and **DM2** LEDs are lit or flashing, press the button briefly several times until the LEDs are off.
   If you do not press the button for longer than 1 minute, the device automatically changes to display mode **A**.
2. Hold down the button for 12 seconds.

   Note

   If you release the button before the 12 seconds have elapsed, the operation is canceled.

3. Release the button after 12 seconds.
   The device restarts with default settings.

8.3 Loading a firmware file via TFTP

Firmware

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

Procedure with Microsoft Windows

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, observe the information in the section "SELECT/SET button (Page 40)".

Follow the steps below to load new firmware using TFTP:

1. Turn off the power to the device.
2. Press the SELECT/SET button and reconnect the device to the power supply with the button pressed.
3. Hold down the button until the red fault LED "F" starts to flash.
4. Release the button as long as the red error LED is still flashing..
   This time only lasts a few seconds.
   The bootloader of the device waits in this status for a new firmware file that you can download by TFTP.
5. Connect a PC to an Ethernet port of the device with an Ethernet cable.

6. Assign an IP address to the device using DHCP or SINEC PNI.
7. In a Windows command prompt, go to the directory where the file with the new firmware is located and use the following command:
   `tftp -i <IP address> put <firmware file>`.

Note

You can enable TFTP in Microsoft Windows as follows:

"Control Panel" > "Programs and Features" > "Turn Windows features on or off" > "TFTP Client".

Once the firmware has been transferred completely to the device and validated, the device restarts. This may take a few minutes.

Technical specifications

9

9.1 Technical specifications of SCALANCE XC416-8

The following technical specifications apply to the SCALANCE XC416-8.

Technical specifications			
Connection to Industrial Ethernet			
Electrical connectors	Quantity		16
	Connector		RJ45 jack
	Properties		Half/full duplex, MDI-X pinning
	Transmission speed		10 / 100 / 1000 Mbps
Slots for plug-in transceiver (SFP+)	Quantity		8
	Connector		SFP / SFP+ plug-in transceiver
	Transmission speed		1 / 10 Gbps
Diagnostics interface			
Serial interface	Quantity		1
	Connector		USB Type B
Signaling contact [1)]	Quantity		1
	Design		Spring-loaded terminal block, 2-pin
	Permitted voltage range		24 V DC
	Load rating		Max. 100 mA
Button	Quantity		1
Configuration interface			
Removable data storage medium	Quantity		1
	Product name		Siemens Configuration and License PLUG (CLP)
Electrical data			
Power supply [1)]	Rated voltage		24 V DC
	Voltage range (incl. tolerance)		19.2 to 28.8 V DC, safety extra-low voltage (SELV)
	Design		2x spring-loaded terminal block, 2-pin
	Property		Implemented redundantly; The connected power supply must meet the requirements of NEC Class 2.
	Fusing		10A / 250V
Current consumption	DC rated voltage		1.8 A
Effective power loss	DC rated voltage	maximum	43.2 W
		typical	35.8 W
Cable cross-section	Minimum		0.75 mm^2 (AWG 18)
	Maximum		2.5 mm^2 (AWG 12)

Technical specifications		
Permitted ambient conditions		
Ambient temperature [2]	Property	Startup at -40 °C
	With LAN operation with RJ45 plug	During operation in horizontal installation position (position 1):
	Up to 2000 m above sea level	-40 °C to +60 °C
		During operation in a different installation position (positions 2, 3 and 4):
		-40 °C ... +50 °C
	When operating with SFP transceivers up to 2000 m above sea level, refer to "Devices with 8 SFP/SFP+ slots (Page 69)"	
	With operation between 2000 m and 3000 m above sea level	The maximum ambient temperature is reduced by 5 °C [3]
	With operation between 3000 m and 4000 m above sea level	The maximum ambient temperature is reduced by 10 °C [3]
	During storage	-40 °C to +85 °C
	During transportation	-40 °C to +85 °C
Relative humidity	During operation at 25 °C	≤ 95% without condensation
Housing, dimensions and weight		
Design	compact	
Housing material	Basic housing	Die cast aluminum, powder coated
	Front cover	Polycarbonate (PC-GF10)
Degree of protection	IP20	
Dimensions (W x H x D)	210 x 147 x 125 mm	
Weight	1800 g	
Installation options	• Wall mounting • Installation on a DIN rail • Mounting on an S7-300 standard rail • Mounting on an S7-1500 standard rail	
Mounting restriction	Observe mounting positions (Page 47)	
Conformal coating of the PCBs	No	
Mean time between failure (MTBF)		
MTBF (EN/IEC 61709; 40 °C)	13.4 years	

[1] Wiring rules

Note the wiring rules (Page 60).

[2] Ambient temperature with SFP

The maximum ambient temperature during operation depends on the operating elevation and the installed plug-in transceivers; refer also to "SFP plug-in transceiver (Page 32)" in the "Accessories" section.

[3] Derating

The derating values depend on the maximum ambient temperatures during operation up to 2000 m.

9.2 Technical specifications of SCALANCE XC424-4

The following technical specifications apply to the SCALANCE XC424-4.

Technical specifications			
Connection to Industrial Ethernet			
Electrical connectors	Quantity		24
	Connector		RJ45 jack
	Properties		Half/full duplex, MDI-X pinning
	Transmission speed		10 / 100 / 1000 Mbps
Slots for plug-in transceiver (SFP+)	Quantity		4
	Connector		SFP / SFP+ plug-in transceiver
	Transmission speed		1 / 10 Gbps
Diagnostics interface			
Serial interface	Quantity		1
	Connector		USB Type B
Signaling contact [1]	Quantity		1
	Design		Spring-loaded terminal block, 2-pin
	Permitted voltage range		24 V DC
	Load rating		Max. 100 mA
Button	Quantity		1
Configuration interface			
Removable data storage medium	Quantity		1
	Product name		Siemens Configuration and License PLUG (CLP)
Electrical data			
Power supply [1]	Rated voltage		24 V DC
	Voltage range (incl. tolerance)		19.2 to 28.8 V DC, safety extra-low voltage (SELV)
	Design		2x spring-loaded terminal block, 2-pin
	Property		Implemented redundantly; The connected power supply must meet the requirements of NEC Class 2.
	Fusing		10 A / 250 V
Current consumption	DC rated voltage		1.8 A
Effective power loss	DC rated voltage	maximum	43.2 W
		typical	35.8 W

Technical specifications		
Cable cross-section	Minimum	0.75 mm^2 (AWG 18)
	Maximum	2.5 mm^2 (AWG 12)
Permitted ambient conditions		
Ambient temperature [2)]	Property	Startup at -40 °C
	With LAN operation with RJ45 plug Up to 2000 m above sea level	During operation in horizontal installation position (position 1): -40 °C to +60 °C During operation in a different installation position (positions 2, 3 and 4): -40 °C ... +50 °C
	When operating with SFP transceivers up to 2000 m above sea level, refer to "Devices with 4 SFP/SFP+ slots (Page 68)"	
	With operation between 2000 m and 3000 m above sea level	The maximum ambient temperature is reduced by 5 °C [3)]
	With operation between 3000 m and 4000 m above sea level	The maximum ambient temperature is reduced by 10 °C [3)]
	During storage	-40 °C to +85 °C
	During transportation	-40 °C to +85 °C
Relative humidity	During operation at 25 °C	≤ 95% without condensation
Housing, dimensions and weight		
Design	compact	
Housing material	Basic housing	Die cast aluminum, powder coated
	Front cover	Polycarbonate (PC-GF10)
Degree of protection	IP20	
Dimensions (W x H x D)	210 x 147 x 125 mm	
Weight	1900 g	
Installation options	• Wall mounting • Installation on a DIN rail • Mounting on an S7-300 standard rail • Mounting on an S7-1500 standard rail	
Mounting restriction	Observe mounting positions (Page 47)	
Conformal coating of the PCBs	No	
Mean time between failure (MTBF)		
MTBF (EN/IEC 61709; 40 °C)	15.6 years	

[1)] Wiring rules

Note the wiring rules (Page 60).

[2)] Ambient temperature with SFP

The maximum ambient temperature during operation depends on the operating elevation and the installed plug-in transceivers; refer also to "SFP plug-in transceiver (Page 32)" in the "Accessories" section.

[3] Derating

The derating values depend on the maximum ambient temperatures during operation up to 2000 m.

9.3 Technical specifications of SCALANCE XC432

The following technical specifications apply to the SCALANCE XC432.

Technical specifications			
Connection to Industrial Ethernet			
Electrical connectors	Quantity		32
	Connector		RJ45 jack
	Properties		Half/full duplex, MDI-X pinning
	Transmission speed		10 / 100 / 1000 Mbps
Diagnostics interface			
Serial interface	Quantity		1
	Connector		USB Type B
Signaling contact [1]	Quantity		1
	Design		Spring-loaded terminal block, 2-pin
	Permitted voltage range		24 V DC
	Load rating		Max. 100 mA
Button	Quantity		1
Configuration interface			
Removable data storage medium	Quantity		1
	Product name		Siemens Configuration and License PLUG (CLP)
Electrical data			
Power supply [1]	Rated voltage		24 V DC
	Voltage range (incl. tolerance)		19.2 to 28.8 V DC, safety extra-low voltage (SELV)
	Design		2x spring-loaded terminal block, 2-pin
	Property		Implemented redundantly; The connected power supply must meet the requirements of NEC Class 2.
	Fusing		10 A / 250 V
Current consumption	DC rated voltage		1.8 A
Effective power loss	DC rated voltage	maximum	43.2 W
		typical	35.8 W
Cable cross-section	Minimum		0.75 mm^2 (AWG 18)
	Maximum		2.5 mm^2 (AWG 12)
Permitted ambient conditions			

Technical specifications		
Ambient temperature	Property	Startup at -40 °C
	With operation up to 2000 m above sea level	During operation in horizontal installation position (position 1): -40 °C to +60 °C During operation in a different installation position (positions 2, 3 and 4): -40 °C ... +50 °C
	With operation between 2000 m and 3000 m above sea level	The high value of the temperature range is reduced by 5 °C [2)].
	With operation between 3000 m and 4000 m above sea level	The high value of the temperature range is reduced by 10 °C [2)].
	During storage	-40 °C to +85 °C
	During transportation	-40 °C to +85 °C
Relative humidity	During operation at 25 °C	≤ 95% without condensation
Housing, dimensions and weight		
Design	compact	
Housing material	Basic housing	Die cast aluminum, powder coated
	Front cover	Polycarbonate (PC-GF10)
Degree of protection	IP20	
Dimensions (W x H x D)	210 x 147 x 125 mm	
Weight	2040 g	
Installation options	• Wall mounting • Installation on a DIN rail • Mounting on an S7-300 standard rail • Mounting on an S7-1500 standard rail	
Mounting restriction	Observe mounting positions (Page 47)	
Conformal coating of the PCBs	No	
Mean time between failure (MTBF)		
MTBF (EN/IEC 61709; 40 °C)	11.6 years	

[1)] Wiring rules

Note the wiring rules (Page 60).

[2)] Derating

The derating values depend on the maximum ambient temperatures during operation up to 2000 m.

9.4 Mechanical stability (in operation)

The devices listed in the scope of validity meet the following requirements for mechanical stability during operation:

IEC 60068-2-27 shock	IEC 60068-2-6 vibration
• 15 g, 11 ms duration • 6 shocks per axis	• 10 - 58 Hz: 0.075 mm • 85 - 150 Hz: 1 g • 1 octave/min, 20 sweeps

9.5 Resistance to harmful gases according to ISA-71.04

The devices listed in the scope of validity meet the following requirements regarding resistance to harmful gases:

Corrosive gases as airborne contaminants Reactive species H_2S and SO_2	ISA-71.04 severity level	G1, G2, G3 RH ≤ 75%, no condensation
	Test according to	IEC 60068-2-42 (SO_2 10ppm)
		IEC 60068-2-43 (H_2S 1ppm)

9.6 Cable lengths

The cable lengths listed below apply to the devices named in the scope of validity:

Cable	Permitted cable length
IE TP torsion cable with IE FC Outlet RJ-45 + 10 m TP cord	0 to 45 m + 10 m TP cord
IE TP torsion cable with IE FC RJ-45 Plug 180	0 to 55 m
IE FC TP Marine / Trailing / Flexible cable with IE FC Outlet RJ-45 + 10 m TP cord	0 to 75 m + 10 m TP cord
IE FC TP Marine / Trailing / Flexible cable with IE FC RJ-45 Plug 180	0 to 85 m
IE FC TP standard cable with IE FC Outlet RJ-45 + 10 m TP cord	0 to 90 m + 10 m TP cord
IE FC TP standard cable with IE FC RJ-45 Plug 180	0 to 100 m

9.7 Switching properties

The switching characteristics listed below apply to the devices named in the scope of validity.

Switching properties				
Aging time	Can be configured (default value: 300 seconds)			
Maximum frame size	2048			
Max. number of learnable addresses	16382			
Response to LLDP frames	Blocking			
Response to spanning tree BPDU frames	Forwarding			
CoS acc. to IEEE 802.1Q	Yes			
QoS priority queues	8			
Switching technique	Store and forward			
Latency	10 microseconds			
Full wire speed switching	**Frame length (bytes)**	**Number of frames per second**		
		At 100 Mbps	At 1000 Mbps	With 10 Gbps
	64	148810	1488095	14880952
	128	84459	844595	8445946
	256	45290	452899	4528986
	512	23496	234962	2349664
	1024	11973	119732	1197318
	1280	9615	96154	961538
	1518	8127	81274	812744

Note

The number of devices connected in a line, which are named in the scope of validity, influences the frame delay. When a frame passes through an IE switch, it is delayed by the store-and-forward function of the device:

- With a 64-byte frame length by about 10 microseconds (at 100 Mbps)
- With a 1500-byte frame length by about 130 microseconds (at 100 Mbps)

This means that the more devices the frame passes through, the higher the frame run time.

9.8 RF radiation according to NAMUR NE21

The devices listed in the scope of validity meet the following requirements regarding RF radiation:

RF radiation according to IEC 61000-4-3/NAMUR NE21	
80 MHz - 2.0 GHz	2.0 GHz - 2.7 GHz
10 V/m	3 V/m
80% AM (1kHz)	

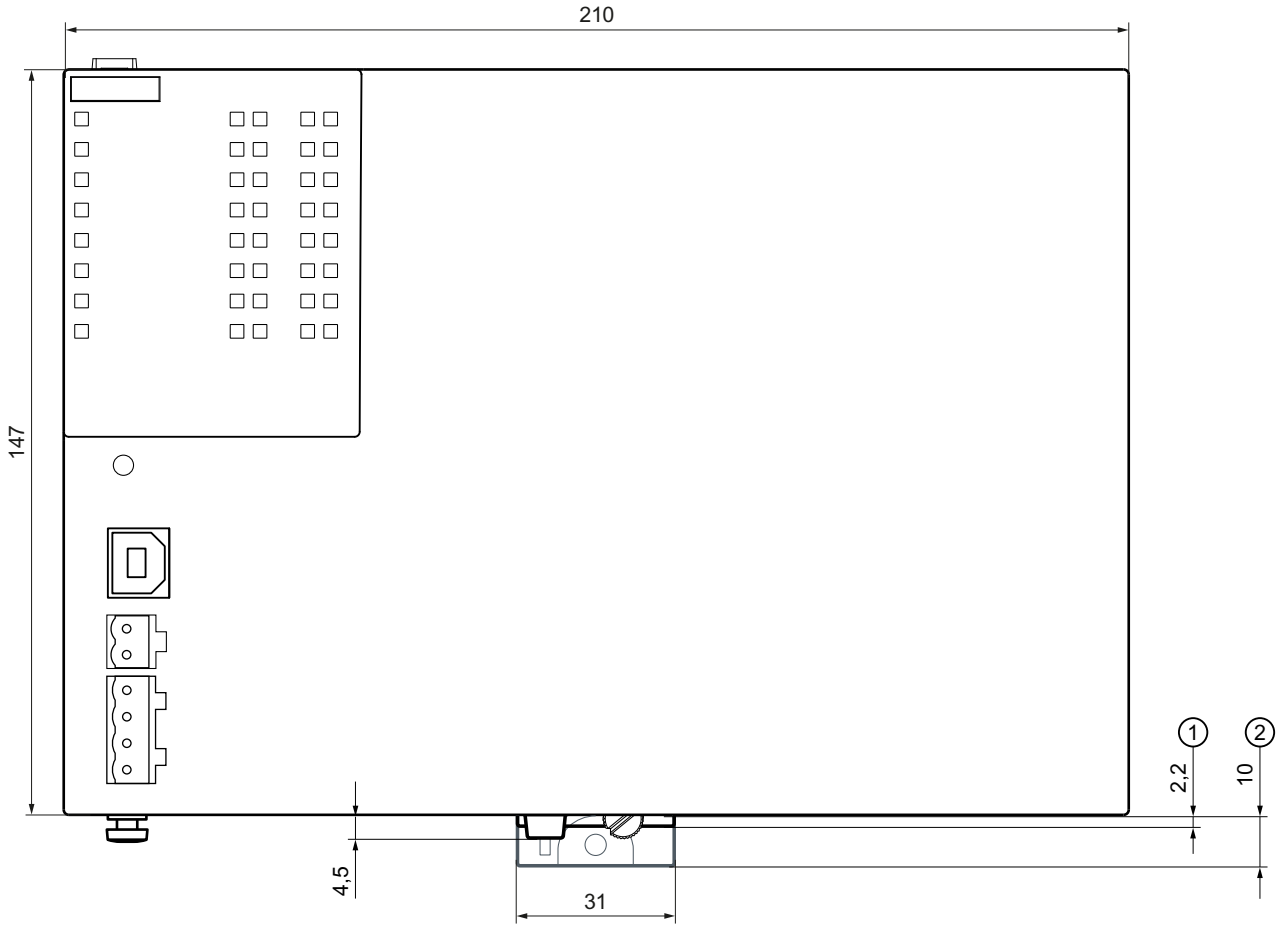
Dimension drawings

10

Note

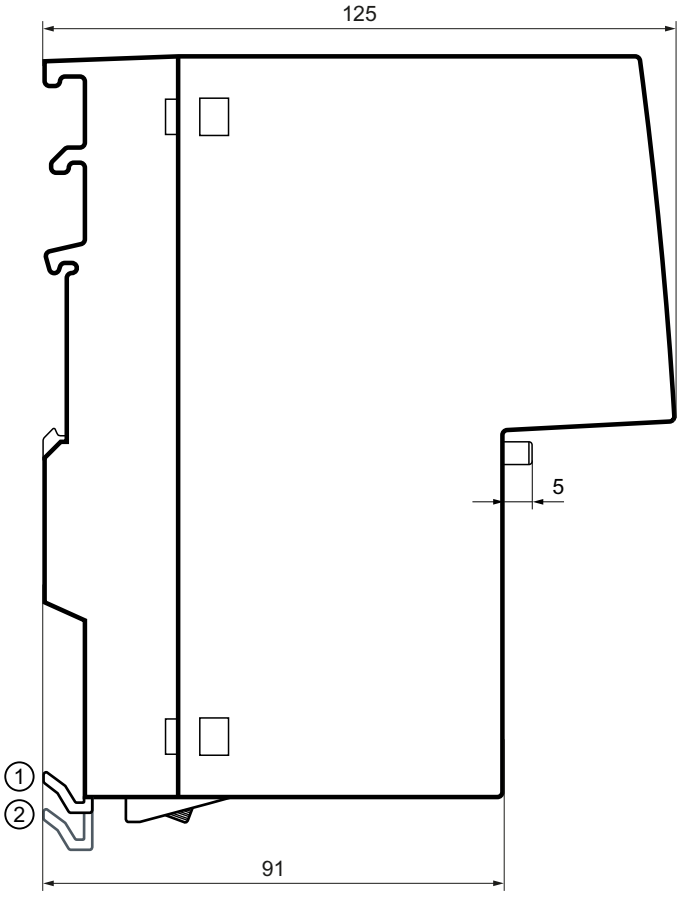
Dimensions are specified in mm.

Front view



① Securing bar in the rail mounting position
② Securing bar in the wall mounting position (as supplied)

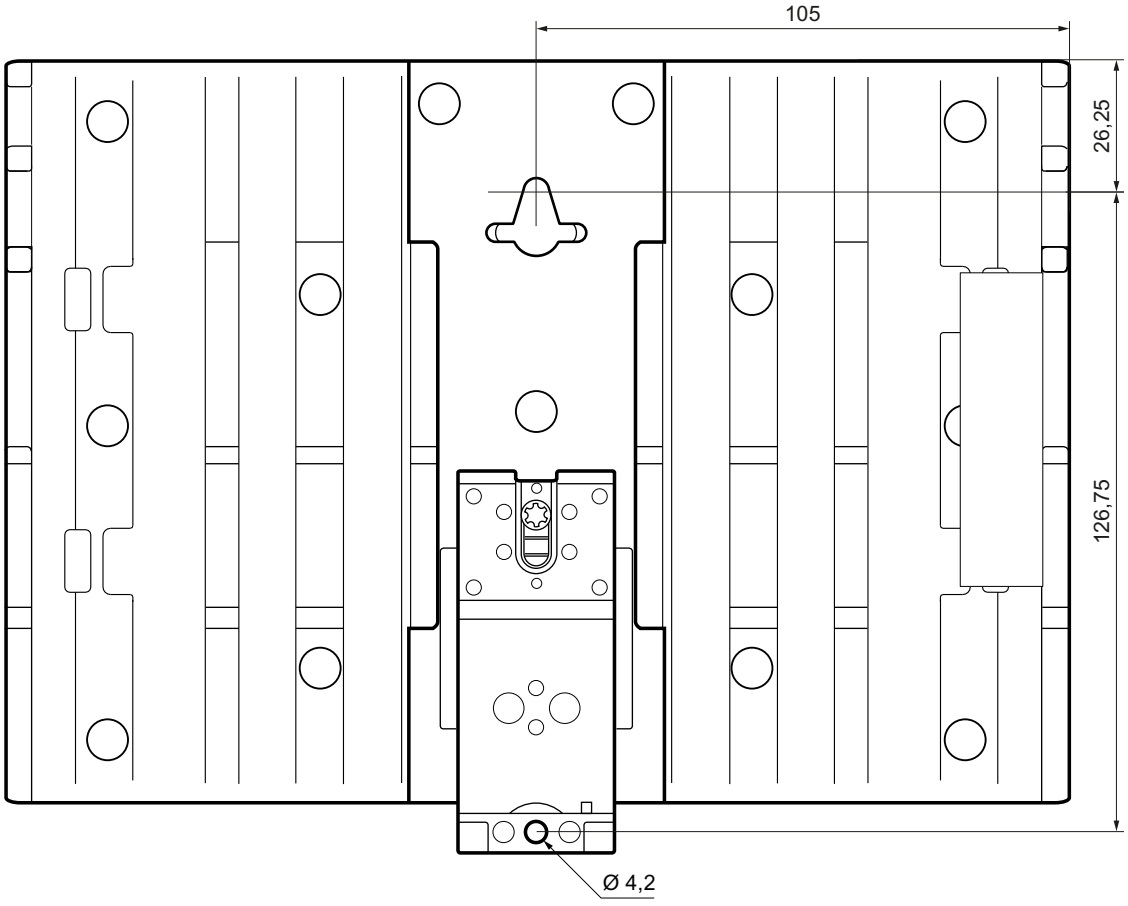
Side view



① Securing bar in the rail mounting position
② Securing bar in the wall mounting position (as supplied)

Figure 10-1 Depth

Drilling template for wall mounting



Certifications and approvals

11

The SIMATIC NET products described in these Operating Instructions have the approvals listed below.

Note

Issued approvals on the type plate of the device

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

Current approvals on the Internet

You will find the current approvals for the product on the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15273/cert).

Notes for the manufacturers of machines

This product is not a machine in the sense of the EC Machinery Directive or the Supply of Machinery (Safety) Regulations (UK).

There is therefore no declaration of conformity relating to the EC Machinery Directive 2006/42/EEC or the Supply of Machinery (Safety) Regulations 2008 (UK) for this product.

If the product is part of the equipment of a machine, it must be included in the procedure for obtaining the EU/UK conformity assessment by the manufacturer of the machine.

Machinery directive

The product is a component in compliance with the EC Machinery Directive 2006/42/EEC and the Supply of Machinery (Safety) Regulations 2008 (UK).

According to the Machinery Directive respectively the Supply of Machinery (Safety) Regulations (UK), we are obliged to point out that the product described is intended solely for installation in a machine.

Before the final product can be put into operation, it must be tested to ensure that it conforms with the Machinery Directive 2006/42/EEC and the Supply of Machinery (Safety) Regulations 2008 (UK).

EC Declaration of Conformity

CE

The SIMATIC NET products described in these operating instructions meet the requirements and safety objectives of the following EC directives and comply with the harmonized

European standards (EN) which are published in the official documentation of the European Union and here.

- **2014/34/EU (ATEX explosion protection directive)**
  Directive of the European Parliament and the Council of 26 February 2014 on the approximation of the laws of the member states concerning equipment and protective systems intended for use in potentially explosive atmospheres, official journal of the EU L96, 29/03/2014, pages. 309-356
- **2014/30/EU (EMC)**
  EMC directive of the European Parliament and of the Council of February 26, 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility; official journal of the EU L96, 29/03/2014, pages. 79-106
- **2011/65/EU (RoHS)**
  Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment, official journal of the EC L174, 01/07/2011, pages 88-110

You will find the EC Declaration of Conformity for these products on the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15273/cert).

The EC Declaration of Conformity is available for all responsible authorities at:

Siemens Aktiengesellschaft

Digital Industries
DE-76181 Karlsruhe
Germany

UK Declaration of Conformity

UK CA

The UK declaration of conformity is available to all responsible authorities at:

Siemens Aktiengesellschaft
Digital Industries
Process Automation
DE-76181 Karlsruhe
Germany

Importer UK:

Siemens plc,
Manchester M20 2UR

You can find the current UK Declaration of Conformity for these products on the Internet pages under Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15273/cert).

The SIMATIC NET products described in this document meet the requirements of the following directives:

- UKEX Regulation
  SI 2016/1107 Equipment and Protective Systems Intended for use in Potentially Explosive Atmospheres Regulations 2016, and related amendments
- EMC Regulation
  SI 2016/1091 Electromagnetic Compatibility Regulations 2016, and related amendments
- RoHS Regulation
  SI 2012/3032 Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments

ATEX, IECEx, UKEX and CCC Ex certification

⚠ WARNING

Risk of explosion in hazardous areas

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

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

You will find this document

- on the data medium that ships with some devices.
- on the Internet pages under Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/78381013).

Enter the document identification number "C234" as the search term.

The markings of the electrical devices are:

II 3 G Ex ec IIC T4 Gc
DEKRA 18ATEX0025 X
IECEx DEK 18.0017X

II 3 G Ex ec IIC T4 Gc
DEKRA 21UKEX0001 X

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

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

The products meet the requirements of the following standards:

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

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

Note for devices with CLASS 1 LASER

Important note on products certified according to Type Examination Certificate KEMA 07ATEX0145 X as of Issue 95 / DEKRA 18ATEX0025 X and IECEx Certificate of Conformity DEK 14.0025X as of Issue 43 / DEK 18.0017X and containing Class 1 optical radiation sources.

Note

CLASS 1 LASER

The device contains optical radiation sources which comply with the limits of Class 1 according to IEC 60825-1. Fiber-optic cables connected to these optical radiation sources may therefore be routed either to or through hazardous areas requiring Category 2G, 3G, 2D or 3D equipment.

EMC (electromagnetic compatibility)

The SIMATIC NET products described in these operating instructions meet the electromagnetic compatibility requirements according to the EU Directive 2014/30/EU as well as the UK-Regulation SI 2016/1091 and their associated amendments.

Applied standards:

- EN 61000-6-2 Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
- EN 61000-6-4 Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments

You will find the current versions of the standards in the currently valid EC/UK Declaration of Conformity.

RoHS

The SIMATIC NET products described in these operating instructions meet the requirements on the restriction of the use of certain hazardous substances in electrical and electronic equipment according to the EU Directive 2011/65/EU as well as the UK-Regulation SI 2012/3032 and their associated amendments.

Applied standard:

- EN IEC 63000

FM

The product meets the requirements of the standards:

- Factory Mutual Approval Standard Class Number 3611
- FM Hazardous (Classified) Location Electrical Equipment:
  Non Incendive / Class I / Division 2 / Groups A,B,C,D / T4 and
  Non Incendive / Class I / Zone 2 / Group IIC / T4

cULus approval PROG. CNTLR.



cULus Listed PROG. CNTLR.

Underwriters Laboratories Inc. complying with

- UL 61010-2-201
- CAN/CSA C22.2 No. 61010-2-201

Report no. E85972

cULus Approval Hazardous Location



cULus Listed PROG.CNTLR. FOR HAZ.LOC.

Underwriters Laboratories Inc. complying with

- UL121201
- ANSI/ISA 12.12.01
- CSA C22.2 No. 213

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

Report no. E223122

Note for Australia - RCM

The product meets the requirements of the RCM standard.

Applied standards:

- AS/NZS CISPR11 (Industrial, scientific and medical equipment - Radio-frequency disturbance characteristics - Limits and methods of measurement).
- EN 61000-6-4 Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments

You will find the current versions of the standards in the currently valid RCM SDoCs (Self-Declaration of Conformity).

MSIP 요구사항 - For Korea only

A급 기기(업무용 방송통신기자재)

이 기기는 업무용(A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는것을 목적으로 합니다.

Marking for the customs union



EAC (Eurasian Conformity)

Eurasian Economic Union of Russia, Belarus, Armenia, Kazakhstan and Kyrgyzstan

Declaration of conformity according to the technical regulations of the customs union (TR ZU)

FDA and IEC marking

The following devices meet the FDA and IEC requirements listed below:

Device	CLASS 1 LASER Product
SCALANCE XC432	-
SCALANCE XC416-8	(*)
SCALANCE XC424-4	(*)

* In modular devices, you can find the marking on the plug-in transceiver used or in the relevant operating instructions.

CAUTION

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

Installation guidelines

The devices meet the requirements if you adhere to the installation and safety instructions contained in this documentation and in the following documentation when installing and operating the devices.

- "Industrial Ethernet / PROFINET Industrial Ethernet" System Manual (https://support.industry.siemens.com/cs/ww/en/view/27069465)
- "Industrial Ethernet / PROFINET - Passive Network Components" System Manual (https://support.industry.siemens.com/cs/ww/en/view/84922825)
- "EMC Installation Guidelines" configuration manual (https://support.industry.siemens.com/cs/ww/en/view/60612658)

WARNING

Personal injury and property damage can occur

The installation of expansions that are not approved for SIMATIC NET products or their target systems may violate the requirements and regulations for safety and electromagnetic compatibility.

Only use expansions that are approved for the system.

Note

The test was performed with a device and a connected communications partner that also meets the requirements of the standards listed above.

When operating the device with a communications partner that does not comply with these standards, adherence to the corresponding values cannot be guaranteed.

Index

A

Accessories, 31
Approvals, 93
Article numbers, 25
Autonegotiation, 65

C

CE mark, 93
Clip, 70
CLP, 27, 28, 29, 31
  Position, 41
  Replacing, 74
Command Line Interface (CLI), 79
Components of the product, 30
Connecting
  Power supply, 61
Connecting cable, 73
Connecting up
  Grounding, 62
Connection to Industrial Ethernet, 81, 83, 85

D

Dimensions, 82, 84, 86
Display mode, 36, 38
DM LED, 27, 28, 29

E

Electrical data, 81, 83, 85
Environmental conditions, 82, 84, 85
ESD directives, 12

F

Factory settings, 78
Fault LED, 27, 28, 29
Fault/error status, 35
Firmware, 35

G

Grounding, 27, 28, 29, 62
Grounding screw, 27, 28, 29

H

Housing, 82, 84, 86

I

Installation, 82, 84, 86
  Installation on a DIN rail, 49
  Installation on a standard rail, 50, 51
  Wall mounting, 52
Installation on a DIN rail, 49
Installation on a standard rail, 50, 51

K

Knurled screw, 27, 28, 29, 49, 50, 51

L

L LED, 27, 28, 29
LED display, 35
  DM LED, 27, 28, 29
  Fault LED, 27, 28, 29
  L LED, 27, 28, 29
  Port LED, 27, 28, 29
  RM LED, 27, 28, 29
  SB LED, 27, 28, 29
Levering aid, 53
  Securing bar, 27, 28, 29

M

MDI / MDI-X autocrossover, 64
MTBF, 82, 84, 86

O

Operating mode, 39

P

Permitted ambient conditions, 82, 84, 85
Pin assignment, 64
PLUG, 31

Pluggable transceiver
Inserting, 70
Notes on deinstallation, 71
Removing, 71
SFP, 32
Pluggable transceiver slot, 70, 71
Plug-in transceiver
SFP bidirectional, 33
Port LED, 27, 28, 29
Port status, 38
Power supply, 27, 28, 29, 61

R

Removable data storage medium, 31
RM LED, 27, 28, 29

S

S7-1500, 51
S7-300, 50
Safety extra low voltage, 61
Safety notices
for installation, 43
general, 13
Use in hazardous areas, 13, 43, 55
when connecting up, 55
SB LED, 27, 28, 29
Sealing plug, 70, 71
Securing bar, 27, 28, 29, 49, 50, 51, 89
SELECT/SET button, 27, 28, 29, 37, 40, 78, 79
Serial cable, 32
Serial interface, 73
SFP transceiver, 32
SFP/SFP+ plug-in transceiver
Slots, 27, 28
SFP+ transceiver, 33
Signaling contact, 27, 28, 29, 35, 71
Slot, 70
Spare parts, 31
Spring-loaded terminal, 61, 71
Startup phase, 35, 77
System manual, 98

T

Transmission speed, 38
Type designation, 30

U

USB cable, 32
USB console interface, 27, 28, 29

W

Web Based Management (WBM), 79
Weight, 82, 84, 86
Wiring rules, 62, 71