SIEMENS

SIMATIC NET

Industrial Ethernet Switches SCALANCE XRH-300 with integrated SCALANCE LPE9433

Equipment Manual

Introduction 1

Safety notices 2

Security recommendations for SCALANCE XRH334 3

Available services for SCALANCE XRH334 4

Security recommendations and available services for SCALANCE LPE9433 5

Description of the device 6

Installing and removing 7

Connecting up 8

Maintenance and cleaning 9

Troubleshooting for SCALANCE XRH334 10

Troubleshooting for SCALANCE LPE9433 11

Technical specifications 12

Dimension drawings 13

Approvals 14

06/2025
C79000-G8976-C768-01

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C768-01
Ⓟ 06/2025 Subject to change

Copyright © Siemens 2025.
All rights reserved

Table of contents

1 Introduction 7

1.1 Purpose 7

1.2 Scope of validity 7

1.3 Designations used 8

1.4 Supplementary documentation 8

1.5 Open Source 10

1.6 Service & Support 10

1.7 SIMATIC NET glossary 11

1.8 Cybersecurity information 11

1.9 Firmware/software support 12

1.10 Error/fault 12

1.11 Decommissioning 12

1.12 Recycling and disposal 12

1.13 Trademarks 13

1.14 Electrostatic discharge 13

2 Safety notices 15

3 Security recommendations for SCALANCE XRH334 17

4 Available services for SCALANCE XRH334 21

5 Security recommendations and available services for SCALANCE LPE9433 25

6 Description of the device 31

6.1 Article numbers 31

6.2 Factory settings 32

6.2.1 SCALANCE XRH334 32

6.2.2 SCALANCE LPE9433 32

6.3 Device view 33

6.4 Components of the product 33

6.5 Spare parts 34

6.6 Accessories 34

6.6.1 Installation 35

6.6.2 Serial USB cable 35

6.6.3 Configuration and License PLUG 35

6.6.4 SFP Transceivers 35

6.7 LED display 39

6.7.1 Position ... 39
6.7.2 P LEDs ... 39
6.7.3 A LED ... 41
6.7.4 L1 and L2 LEDs ... 41
6.7.5 RM LED ... 42
6.7.6 DM1 and DM2 LEDs ... 42

6.8 SELECT / SET button ... 42
6.8.1 Position ... 42
6.8.2 Function ... 43
6.8.3 Setting the display mode ... 43

6.9 Configuration License PLUG ... 43
6.9.1 Position ... 44
6.9.2 Function ... 44

7 Installing and removing ... 45

7.1 Safety during installation ... 45

7.2 Types of installation ... 49

7.3 19" rack mounting ... 51

7.4 Four-point mounting ... 53

7.5 Disassembly ... 56

8 Connecting up ... 57

8.1 Safety when connecting up ... 57

8.2 Wiring rules ... 61

8.3 24 V AC/DC power supply ... 62

8.4 Grounding ... 65
8.4.1 Functional ground ... 66
8.4.2 Protective grounding (24 V AC/DC device versions) ... 66
8.4.3 Connecting the grounding via a grounding bolt ... 67

8.5 Industrial Ethernet ... 68
8.5.1 Electrical ... 68
8.5.2 Optical ... 70
8.5.3 Dependency between ports and ambient temperature (derating) ... 70
8.5.3.1 Devices with 12 SFP/SFP+ slots ... 72
8.5.4 Inserting and removing pluggable transceivers ... 73
8.5.4.1 General notes for SFP transceivers ... 73
8.5.4.2 Inserting a plug-in transceiver (SFP/SFP+) ... 73
8.5.4.3 Removing a pluggable transceiver (SFP/SFP+) ... 74

8.6 Signaling contact ... 74

8.7 USB console interface ... 76

8.8 Replacing a CLP ... 77

9 Maintenance and cleaning ... 79

10 Troubleshooting for SCALANCE XRH334 ... 81

10.1 Resetting the device to default settings with the button (in the startup phase) ... 81

10.2 Resetting the device to default settings with the button (during operation) ... 82
10.3 Load a firmware file via TFTP ... 83
11 Troubleshooting for SCALANCE LPE9433 ... 85
11.1 Restarting a SCALANCE LPE9433 ... 85
11.2 Starting a SCALANCE LPE9433 in the Rescue system ... 85
11.3 Loading a firmware file via TFTP ... 85
11.4 Resetting the configuration of a SCALANCE LPE9433 ... 87
11.5 Starting up a switched off SCALANCE LPE9433 ... 88
12 Technical specifications ... 89
12.1 Technical specifications of the 24 V AC/DC device version ... 89
12.2 Technical specifications of the SCALANCE LPE9433 ... 91
12.3 Mechanical stability (in operation) ... 92
12.4 Resistance to harmful gases according to ISA-71.04 ... 92
12.5 Cable lengths ... 92
12.6 Switching properties ... 93
13 Dimension drawings ... 95
13.1 SCALANCE XRH334 dimension drawings ... 95
13.2 Mounting brackets for use on ships ... 96
14 Approvals ... 97
Index ... 105

Introduction

1

These operating instructions support you when installing and connecting up devices of the product group SCALANCE XRH334 with integrated SCALANCE LPE9433.

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

1.1 Purpose

The SCALANCE XRH334 switches are rack switches for installation in the 19" control cabinet. Up to 12 SFP transceivers can be plugged in, thus enabling flexible network construction and expansions. On both the field level and the control level, the control cabinet switches perform networking with the distributed field devices and ensure high plant availability with extensive diagnostics options and high transmission speeds. The switches feature high immunity and can also be used in extended temperature ranges (Enhanced Environmental Conditions).

A SCALANCE LPE9433 is integrated in the enclosure of a SCALANCE XRH334. The SCALANCE LPE9433 is an industrial IoT (Internet of Things) device with a Linux operating system that was developed for use in the Siemens Industrial Edge ecosystem. The device provides computing power for a wide range of Industrial Edge applications (Edge Computing). As Industrial Edge Device with connection to the Industrial Edge Management (IEM), it offers special advantages during configuration and operation:

- Central management of Edge Devices
- Efficient software update for Edge Devices and Edge apps through the IEM
- Monitoring of the device and device groups by the IEM

1.2 Scope of validity

This manual is valid for the following devices:

- SCALANCE XRH334 with integrated SCALANCE LPE9433

The descriptions in this manual generally apply to the SCALANCE XRH334 devices. Descriptions that apply to an integrated SCALANCE LPE9433 are specifically marked.

1.3 Designations used

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

Classification	Description	Terms used	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-300/SCALANCE LPE is used.	SCALANCE X-300	SCALANCE LPE
Product group	If information applies to all devices and versions of a product group, the term SCALANCE XRH-300/ SCALANCE XRM-300 is used.	SCALANCE XRH-300	-
Device	If information relates to a specific device, the device name is used.	SCALANCE XRH334	SCALANCE LPE9433 Integrated SCALANCE LPE
Device version	For a version of the device, the device name contains the special feature of the version.	e.g. SCALANCE XRH334 AC/DC 24 V device version	-

1.4 Supplementary 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/15247).

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	Description
"Command Line Interface (CLI) SINEC OS" configuration manual	Visit (https://support.industry.siemens.com/cs/ww/en/ps/15298/man)	Describes how to configure and manage SINEC OS via the CLI user interface
"Web User Interface (Web UI) SINEC OS" configuration manual	Visit (https://support.industry.siemens.com/cs/ww/en/ps/15298/man)	Describes how to configure and manage SINEC OS via the Web UI user interface

Document title	Link	Description
Getting Started "SCALANCE LPE9433 integrated in SCALANCE XRH334"	Visit (https://support.industry.siemens.com/cs/document/109972622)	Supports you with the integration of a SCALANCE LPE in Industrial Edge Management
"Get Started and Operate" manual	Visit (https://docs.industrial-operations-x.siemens.cloud/access?ft:clusterId=ie_platform_operation_get_started_and_operate&ft:locale=en-US)	Contains the following information: • You can find operating instructions for Industrial Edge Devices under **Industrial Edge Device** • You can find instructions on updating Industrial Edge and the associated components under **Updates and Migrations** • You can find a general security overview of Industrial Edge under **Security** • You can find installation and operating instructions for Industrial Edge Management under **Industrial Edge Management**
"Develop an Application" operating instructions	Visit (https://docs.industrial-operations-x.siemens.cloud/access?ft:clusterId=ie_platform_operation_develop_an_application&ft:locale=en-US)	Contains operating instructions for the Industrial Edge App Publisher
"Transceiver SFP/SFP+/SCP/STP" Operating Instructions	Visit (https://support.industry.siemens.com/cs/ww/en/ps/25547/man)	Describes safety, operation, installation, connection, maintenance, technical specifications and approvals of the SFP transceivers
"Industrial Ethernet/PROFINET Industrial Ethernet" System Manual	Visit (https://support.industry.siemens.com/cs/ww/en/view/27069465)	Contains information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network. Among other information, you will find the optical performance data of the communication partners that you require for the design.
"Industrial Ethernet/PROFINET Passive Network Components" System Manual	Visit (https://support.industry.siemens.com/cs/ww/en/view/84922825)	

Catalogs

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

- 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.

1.5 Open Source

SCALANCE XRH334

SINEC OS is based on Linux® and contains open source software. The open source software (OSS) information is saved as PDF file.

To view the OSS information, do the following:

- Download the OSS information from the device.
- Download the OSS information together with a firmware version from the Siemens Portal.

For more information, refer to the SINEC OS configuration manuals.

SCALANCE LPE9433

The SCALANCE LPE9433 Industrial Edge uses Debian GNU/Linux as the operating system and includes other open source software. The license terms are stored on the device.

To display the OSS license conditions, enter the following in the address bar of your web browser:
`https://<IP address of the device>/OSS`

1.6 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)

Pascal Janitschke
Siemens AG
Gleiwitzer Str. 555
90475 Nuremberg
Germany

1.7 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)

1.8 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).

1.9 Firmware/software support

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

1.10 Error/fault

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

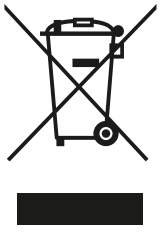
1.11 Decommissioning

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.

1.12 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).

Note the different national regulations.

1.13 Trademarks

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

- SCALANCE
- SINEC

Linux® is the registered trademark of Linus Torvalds in the United States of America and other countries.

The registered trademark Linux® is used according to a sublicense of LMI, the exclusive licensee of Linus Torvalds, owner of the trademark on a global basis.

1.14 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 for SCALANCE XRH334

3

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

General

- Periodically audit the device to make sure it complies with these recommendations and/or any internal security policies.
- Backup the device configuration to an external server following the initial setup and after each major configuration change.
- Evaluate the security of your site and use a cell protection concept with suitable products. For more information, visit Industrial Security (https://www.siemens.com/industrialsecurity).
- Review the user documentation for other Siemens products used along with the device for further security recommendations.
- Use remote system logging to forward system logs to a central logging server. Make sure the server is within the protected network and check the logs regularly to identify potential security breaches/vulnerabilities.
  For more information, refer to "Supplementary documentation (Page 8)".

Authentication

NOTICE
Accessibility hazard - risk of data loss
Do not misplace passwords for the device. Access to the device can only be restored by resetting it to factory defaults, which will remove all configuration data.

- Each device has a default **admin** profile with administrator access rights. During commissioning, this profile should be replaced by a unique, user-defined profile that is assigned the admin role.
  At least one user profile with the admin role is required.
- Replace the default passwords for all user accounts, access modes and applications (where applicable) before the device is deployed.
- Use strong passwords. Avoid weak passwords (e.g. password1, 123456789, abcdefgh) or repeated characters (e.g. abcabc).
  This recommendation also applies to symmetric passwords/keys configured on the device.
- Make sure passwords are protected and not shared with unauthorized personnel.
- Do not re-use passwords across different user names and systems.
- Record passwords in a safe, secure, off-line location for future retrieval should they be misplaced.
- Change passwords regularly and often.

- When RADIUS or TACACS+ are utilized for user authentication, make sure all communications are within the security perimeter or protected by a secure channel.
- Be aware of any link layer protocols that do not provide any inherent authentication between endpoints, such as ARP in IPv4. A malicious entity could exploit weaknesses in these protocols to attack hosts, switches, and routers connected to your Layer 2 network, for example, by poisoning the ARP caches of systems within the subnet and subsequently intercepting traffic. Appropriate safeguards against non-secure Layer 2 protocols, such as securing physical access to the local network and using secure higher layer protocols, should be taken to prevent unauthorized access to the network.
- Take precautions to protect your 2FA authenticator devices/applications. This includes maintaining individual possession of authenticators, not sharing authenticators with others, and immediately reporting lost or compromised authenticators.

Certificates and keys

- Use a trusted Certificate Authority (CA) that supports key revocation and certificate signing.
- SINEC OS includes default vendor certificates and keys for the purpose of initial onboarding. Do not deploy the device before installing certificates and keys signed by a trusted Certificate Authority (CA).
- Certificates and keys must be unique to each device. Do not reuse certificates and keys between devices and servers.
- Immediately change all certificates and keys upon suspision of a security breach.
- SSH and SSL keys are accessible to admin users. Make sure to take appropriate precautions when shipping the device beyond the boundaries of the trusted environment:
  - Replace the SSH and SSL keys with throwaway keys prior to shipping.
  - Take the existing SSH and SSL keys out of service. When the device returns, create and program new keys for the device.
- Use password-protected certificates that are in PKCS #12 format.
- Use certificates with a key length of 4096 bits.
- Before returning the device to Siemens for repair, replace the current certificates and keys with temporary throwaway certificates and keys that can be destroyed upon the device's return.
- Verify certificates and fingerprints on the server and client to prevent Man-in-the-Middle (MitM) attacks.

Physical/remote access

- Only operate the devices in a protected network area. Attackers cannot access internal data from outside when the internal and external network are disconnected.
- Restrict physical access to the device to only trusted personnel. A malicious user in possession of the device's removable media could extract critical information, such as certificates, keys, etc. (user passwords are protected by hash codes), or reprogram the media.
- Control access to the serial console to the same degree as any physical access to the device.
- Never allow the serial console port to be accessible from the Internet. This port is exempt from Brute Force Attack (BFA) prevention measures to allow administrators to access the device during an active Denial of Service (DoS) attack.

- It is highly recommended to keep Brute Force Attack (BFA) protection enabled to prevent a third-party from obtaining unauthorized access to the device.
  For more information, refer to "Supplementary documentation (Page 8)".
- For communication via non-secure networks, use additional devices with VPN functionality to encrypt and authenticate communications.
- When securely connecting to a server (e.g. in the case of a secure upgrade), make sure the server side is configured with strong ciphers and protocols.
- Terminate management connections (e.g. HTTP, HTTPS, SSH, etc.) properly.
- Make sure the device is fully decommissioned before taking the device out of service.
  For more information, refer to "Supplementary documentation (Page 8)".

Secure/non-secure protocols

- Use secure protocols when access to the device is not prevented by physical protection measures.
- Disable or limit the use of non-secure protocols. While some protocols are secure (e.g. HTTPS, SSH, 802.1X, etc.) , others were not designed for secure applications (e.g. SNMPv1/v2c, RSTP, etc.).
  Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to the device/network.
- Whenever possible, use the SSH File Transfer Protocol (SFTP) to transfer files. While other protocols are available (e.g. FTP, TFTP, HTTP), SFTP is the only protocol that transfers files encrypted. The other protocols are not protected against interception and manipulation.
- If non-secure protocols and services are required, make sure the device is operated within a protected network area.
- When a secure alternative is available for a protocol, use the secure version instead. For example:
  - Use HTTPS instead of HTTP
  - Use SNMPv3 instead of SNMPv1/v2c
- Avoid or limit use of the following:
  - Non-authenticated and unencrypted protocols
  - Link Layer Discovery Protocol (LLDP)
- After commissioning the device, access rights for the Discovery and basic Configuration Protocol (DCP) are automatically set to read-only. If your environment does not require DCP, it is recommended to disable it fully.
  For more information, refer to "Supplementary documentation (Page 8)".

Hardware/software

- Limit critical applications and access to management services to private networks. Connecting a SINEC OS device to the Internet is possible. However, the utmost care should be taken to protect the device and the network behind it using secure means, such as a firewall and IPsec.
- Whenever possible, use VLANs to protect against Denial of Service (DoS) attacks and unauthorized access.

- Select services are enabled by default in SINEC OS. It is recommended to only enable the minimum services that are required for your setup.
  For more information about available services, "Available services for SCALANCE XRH334 (Page 21)".
- Use the latest Web browser version compatible with SINEC OS to make sure the most secure ciphers available are employed. Additionally, 1/n-1 record splitting is enabled in the latest Web browser versions of Mozilla Firefox, Google Chrome and Microsoft Edge, and mitigates against attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (e.g. BEAST).
- Make sure the latest firmware version is installed, including all security-related patches. For the latest information on security patches for Siemens products, visit the Industrial Security (https://www.siemens.com/industrialsecurity) website or the ProductCERT Security Advisories (https://www.siemens.com/cert/en/cert-security-advisories.htm) website. Updates to the Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the Siemens ProductCERT Security Advisories website, or by following @ProductCert on Twitter.
- Only enable services that will be used on the device, including physical ports. Unused physical ports could potentially be used to gain access to the network behind the device.
- For optimal security, use the authentication and encryption mechanisms in SNMPv3 whenever possible, and apply strong passwords.
- Configuration files can be downloaded from the device. Make sure configuration files are properly protected. For instance, digitally sign and encrypt the files, store them in a secure place, and only transfer configuration files via secure communication channels. Configuration files can be password-protected when downloaded. For information about protecting a configuration file with a password, refer to "Supplementary documentation (Page 8)".
- When using SNMP (Simple Network Management Protocol):
  - Configure SNMP to raise a trap upon authentication failures.
    For more information, refer to "Supplementary documentation (Page 8)".
  - Make sure the default community strings are changed to unique values.
  - Use SNMPv3 whenever possible. SNMPv1 and SNMPv2c are considered non-secure and should only be used when necessary.
  - Whenever possible, prevent write access.

Available services for SCALANCE XRH334

4

The following is a list of all available protocols or services and their ports through which the device can be accessed, including the following information:

- **Service**
  The service supported by the device.
- **Protocol**
  The protocol used by the service.
- **Default port number**
  The default port number assigned to the client/service.
- **Default status**
  The default state of the service.
- **Status**
  The state of the service when active.
- **Configurable service**
  Specifies whether or not the service can be configured.
- **Configurable port number**
  Specifies whether the port number is configurable.
- **Authentication**
  Specifies whether an authentication of the communication partner takes place or whether an authentication can be configured.
- **Encryption**
  Specifies whether the transfer is encrypted or whether the encryption is configurable.

Clients

Service	Protocol	Default port number	Default status	Status	Configurable service	Configurable port number	Authentication	Encryption
DHCP Client	UDP	67/68	Open	Open if configured	✓	-	-	-
DNS	UDP/ TCP	53	Closed	Only outgoing open if configured	✓	-	-	-
FTP	TCP	20 (local) 21 (remote)	Closed	Only outgoing open	✓	-	✓	-
HTTP	TCP	80	Closed	Open if configured with login	✓	✓	-	-
NTP	UDP	123	Closed	Open if configured	✓	-	-	-
RADIUS	UDP	1812	Closed	Only outgoing open if configured	✓	✓	✓	-
RIPv2	UDP	520	Closed	Open if configured	✓	-	-	-
Secure NTP	UDP	123	Closed	Open if configured	✓	-	Configurable	-

Service	Protocol	Default port number	Default status	Status	Configurable service	Configurable port number	Authentication	Encryption
Secure Syslog	TCP	6514	Closed	Only outgoing open if configured	✓	✓	✓	✓
SFTP	TCP	22	Closed	Only outgoing open if configured	✓	✓	✓	✓
SNMP trap	UDP	162	Closed	Only outgoing open if configured	✓	-	-	-
Syslog	UDP	514	Closed	Only outgoing open if configured	✓	✓	-	-
TACACS+	TCP	49	Closed	Open if configured	✓	✓	✓	-
TFTP	UDP	69	Closed	Only outgoing open if configured	✓	-	-	-
SMTP	TCP	25	Closed	Only outgoing open if configured	✓	-	✓	-

Servers

Service	Protocol	Default port number	Default status	Status	Configurable service	Configurable port number	Authentication	Encryption
EtherNet/IP	UDP	2222 and four ports in the range of 49152 to 65535	Closed	Only outgoing open if configured	✓	-	-	-
	TCP	44818						
DHCP Server	UDP	67	Closed	Open if configured	✓	-	-	-
HTTP	TCP	80	Closed	Open if configured with login	✓	✓	-	-
HTTPS	TCP	443	Open	Open if configured with login	✓	✓	✓	✓
VRRP ARP Sync	UDP	50000	Closed	Open if configured	✓	-	-	-
NTP	UDP	123	Closed	Open if configured	✓	-	Configurable	-
PROFINET	UDP	One port in the range of 49152 to 65535	Open	Open because of base function	-	-	-	-
PROFINET Device	UDP	34964 and one port in the range of 49152 to 65535	Open	Open because of base function	-	-	-	-

Service	Protocol	Default port number	Default status	Status	Configurable service	Configurable port number	Authentication	Encryption
SNMPv1/v2c	UDP	161	Closed	Open if configured	✓	✓	Configurable	-
SNMPv3	UDP	161	Closed	Open if configured with login	✓	✓	Configurable	Configurable
SSH	TCP	22	Open	Open if configured with login	✓	✓	✓	✓
NETCONF (SSH)	TCP	830	Open	Open if configured	✓	✓	✓	✓

Security recommendations and available services for SCALANCE LPE9433

5

To prevent unauthorized access, note 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.
- 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.
- Use VPN to encrypt and authenticate communication from and to the devices.
- Terminate connections correctly (WBM 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.

Physical 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.
- Restrict physical access to the device to trusted personnel.
- Lock unused physical ports on the device. Unused ports can be used to access the system without authorization.
- Terminate the management connections (e.g. HTTP, HTTPS) properly.
- Make sure that the device has been powered down completely before you decommission it.

Software (security functions)

- Inform yourself regularly about security recommendations published by Siemens ProductCERT (https://www.siemens.com/cert/en/cert-security-advisories.htm).
- Only activate protocols that you require to use the device.
- Disable encryption methods with a low security level.
- 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.
- To ensure you are using the most secure encryption methods available, use the latest web browser version compatible with the product. Also, the latest web browser versions of Mozilla Firefox, Google Chrome, and Microsoft Edge have 1/n-1 record splitting enabled, which reduces the risk of attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (for example, BEAST).
- Ensure that the latest firmware version is installed, including all security-related patches. You can find the latest information on security patches for Siemens products on the Industrial Security (https://www.siemens.com/industrialsecurity) or ProductCERT Security Advisories (https://www.siemens.com/cert/en/cert-security-advisories.htm) website.
  For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.

Authentication

Note

Accessibility risk - Risk of data loss

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

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

Certificates and keys

- There is a preset SSL/TLS (RSA) certificate with 4096 bit key length in the device. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority.
- Use a 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 side and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Secure/non-secure protocols and services

- Check whether use of the following protocols and services is necessary:
  - Non-authenticated and unencrypted ports
  - Syslog
  - DHCP options 66/67
  - TFTP (The TFTP service is only active in the Rescue system.)
- Use secure protocols when access to the device is not secured by physical protection measures.
- If you require non-secure protocols and services, operate them only within a protected network area.
- Restrict the services and protocols available to the outside to a minimum.
- If you use RADIUS for management access to the device, enable secure protocols and services.

Interface security

- Disable unused interfaces.
- Use IEEE 802.1X for interface authentication.

List of available protocols

The following is a list of all available protocols and services as well as their ports through which the device can be accessed, including the following information:

- **Protocol/service**
  The protocols/services supported by the device.
- **Protocol**
  The protocol used by the service.
- **Port number**
  The port number assigned to the service.

Note

The table contains the preset ports. Additional ports can be opened for protocols with a configurable port number.

- **Default port status/protocol status**
  The default state (i.e. open, closed, active).
- **Protocol/service configurable**
  Specifies whether or not the protocol or service can be configured.
- **Port number configurable**
  Specifies whether the port number can be configured.
- **Authentication**
  Specifies whether an authentication of the communication partner takes place or whether an authentication can be configured.
- **Encryption**
  Specifies whether the transfer is encrypted or whether the encryption can be configured.

Service	Protocol	Port number	Default port status	Configurable		Authentication	Encryption
				Protocol/ service	Port number		
DHCP	UDP	- [1]	Closed	-	-	-	-
HTTPS	TCP	443	Open	-	-	✓ [2]	✓
NTP	UDP	- [3]	Closed	✓	-	-	-
TFTP	UDP	69	Open [4]	-	-	-	-

[1] DHCP only outbound, port number is not configured.

[2] Authentication is only possible after successful onboarding.

[3] Only client.

[4] The TFTP service is only active in the Rescue system.

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**.**
- **Protocol**
  The protocol used by the service.
- **Default protocol status**
  The default status of the service (enabled or disabled).
- **Service configurable**
  Indicates whether the service can be configured via WBM / CLI.

Layer 2 service	Protocol	Default protocol status	Protocol/service configurable
DCP	PROFINET	Active [1)]	-
Ping	ICMP	Active	-

[1)] In Rescue mode only.

Description of the device

6

6.1 Article numbers

Device	Properties	Article number
SCALANCE XRH334	**24 V AC/DC version** • 20 x 10 / 100 / 1000 Mbps RJ45 ports • 2 x 1 / 2.5 / 5 / 10 Gbps RJ45 ports • 4 x SFP slot for plug-in transceiver with 100 / 1000 Mbps • 8 x SFP / SFP+ plug-in transceiver slots with 1 / 10 Gbps • 2 x 2-pin terminal block 24 V DC / 24 V AC, 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 • Integrated SCALANCE LPE9433	6GK5334-3TS01-2SR3
SCALANCE LPE9433	An integrated SCALANCE LPE9433 is not physically accessible. Therefore, the following applies: • The alarm LED signals the state of the SCALANCE XRH334 and is checked by SINEC OS. An alarm of the SCALANCE LPE9433 is not signaled. • The CLP is only used by SINEC OS. A SCALANCE LPE9433 does not support CLP functionality. • The button only influences the SCALANCE XRH334. Known SCALANCE button functions are available for a SCALANCE LPE9433 via configuration options of SINEC OS. • Access to the USB console interface can be switched between SCALANCE XRH334 and the integrated SCALANCE LPE9433. The ports of the SCALANCE LPE9433 work as function extender interface (FEI) ports of the SCALANCE XRH334 with the following speeds: • 2 x 1 Gbps • 1 x 10 Gbps The three FEI ports are available as bridge ports within the SCALANCE XRH334.	6GK5998-3GS11-2AC2 [1]

[1] This is a virtual article number that is only used to identify the SCALANCE LPE9433. The virtual article number cannot be used to place an order.

6.2 Factory settings

6.2.1 SCALANCE XRH334

The devices are supplied with the following factory settings:

- Spanning Tree Protocol: Enabled
- Spanning Tree version: RSTP
- Operating mode: VLAN-capable (IEEE 802.1Q)
- PROFINET: Enabled
- DCP mode: Setup
- IGMP Snooping: Enabled
- IGMP Querier: Disabled
- EtherNet/IP: Disabled
- DLR: Disabled
- Trust mode: PCP
- DHCP: Enabled for VLAN 1

6.2.2 SCALANCE LPE9433

The tables below show the factory settings of the SCALANCE LPE.

Port status for services

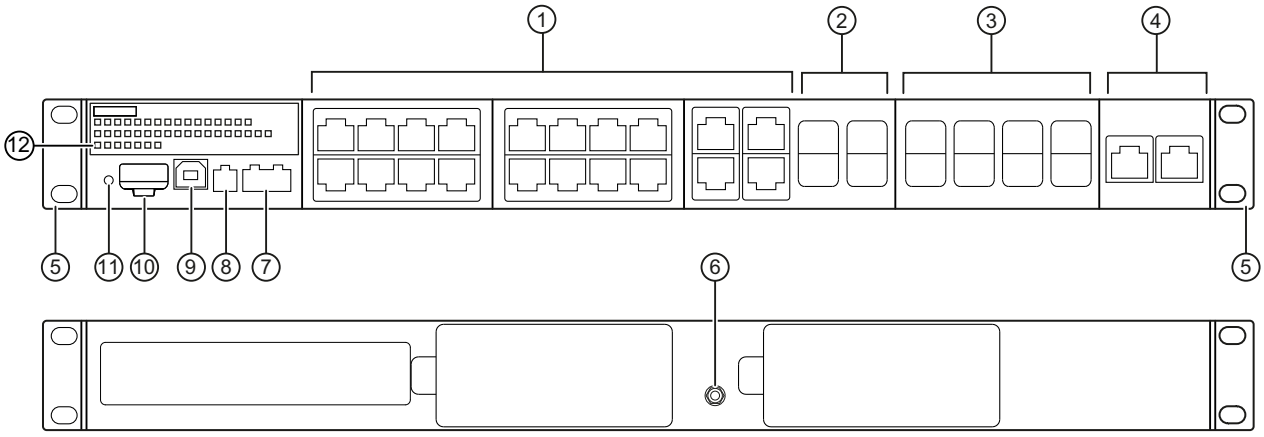
Service	Port status	
DHCP	EXTENDER1	Enabled
	EXTENDER2	Not enabled
	EXTENDER3	Not enabled
HTTPS	Open	
NTP	Closed	
TFTP	Enabled in Rescue system.	

Protocol status for Layer2 services

Layer 2 service	Protocol status
DCP	Read/write in Rescue system.
Ping/ICMP	Enabled

6.3 Device view

The following figure shows an overview of the components of a 24 V AC/DC device version of the SCALANCE XRH334 with 12 SFP/SFP+ slots.



① Electrical ports with 10/100/1000 Mbps
② Slots for SFP transceiver with 100/1000 Mbps
③ Slots for SFP/SFP+ transceiver with 1/10 Gbps
④ Electrical ports with 1/2.5/5/10 Gbps
⑤ Mounting brackets for 19" rack installation
⑥ Grounding bolt for connecting the protective grounding, on the back of the device
⑦ 24 V AC/DC power supply, redundant
⑧ Signaling contact
⑨ USB console interface (2.0 port, Type B, serial via USB)
⑩ CLP slot with an inserted CLP
⑪ "SELECT/SET" button
⑫ LED display

- Port LEDs
- "A" LED for the alarm display
- "L1/L2" LED for the power supply
- "RM" LED for the "Redundancy manager" function
- "CM" LED without function
- "DM1/DM2" LED for the display mode

Figure 6-1 24 V AC/DC device version with 12 SFP/SFP+ slots, front and back

6.4 Components of the product

The following components are supplied with a SCALANCE XRH334:

- SCALANCE XRH334 with integrated SCALANCE LPE9433
- A CLP removable data storage medium
  Article number 6GK1900-0UQ00-0AA0

- Two brackets for 19" rack installation,
  pre-assembled with 8 screws M3 x 5 recessed head, drive: Torx
- A 2-pin spring-loaded terminal block for the signaling contact
- 12 covers for the SFP transceiver slots
- Two 2-pin spring-loaded terminal blocks 24 V for 24 V AC/DC power supply

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.

6.5 Spare parts

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

Component	Description	Article number
Spring-loaded terminal block, 2-pins	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-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

6.6 Accessories

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

6.6.1 Installation

Component	Description	Article number
SCALANCE XR-300 Rack Mount Kit	Mounting bracket for four-point mounting Pack of 4	6GK5980-2BA00-0AA4

6.6.2 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

6.6.3 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
SCALANCE CLP EEC 2 GB	Configuration and License PLUG, removable data storage medium for configuration data, 2 GB conformal-coated PCBs	6GK1900-0UQ00-0AA0

6.6.4 SFP Transceivers

Pluggable transceiver SFP (100 Mbps)

Type	Property	Article number
SFP991-1	1 x 100 Mbps, LC port optical for glass FO cable (multimode), up to max. 5 km	6GK5 991-1AD00-8AA0
	10 packing unit (VPE 10)	6GK5 991-1AD00-8AC0
SFP991-1 (C)	1 x 100 Mbps, LC port optical, for glass FO cable (multimode), up to max. 5 km, varnished	6GK5 991-1AD00-8FA0
SFP991-1LD	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km	6GK5 991-1AF00-8AA0
	10 packing unit (VPE 10)	6GK5 991-1AF00-8AC0
SFP991-1LD (C)	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km, varnished	6GK5 991-1AF00-8FA0

Type	Property	Article number
SFP991-1LH+	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5 991-1AE00-8AA0
SFP991-1ELH200	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 200 km	6GK5 991-1AE30-8AA0

The SFP plug-in transceiver (100 Mbps) cannot be operated in SFP+ slots.

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

Active plug-in transceiver SFP (100 Mbps)

With active plug-in transceivers, Gigabit slots can be used as Fast Ethernet interfaces.

Type	Property	Article number
SFP991-1A	1 x 100 Mbps, LC port optical for glass FO cable (multimode), up to max. 5 km	6GK5 991-1AD00-8GA0
SFP991-1LD A	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km	6GK5 991-1AF00-8GA0

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).

Note

Restriction for SFP transceivers

The maximum ambient temperature changes if you use SFP transceivers:

- If you use SFP transceivers of the types LH, LH+ or ELH, the maximum ambient temperature is reduced to 50 °C.
  For more information, refer to "Dependency between ports and ambient temperature (derating) (Page 70)".

For the values of the ambient temperature without SFP transceivers, refer to the section "Technical specifications (Page 89)".

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

Type	Properties	Article number
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

Restriction for SFP transceivers

The maximum ambient temperature changes if you use SFP transceivers:

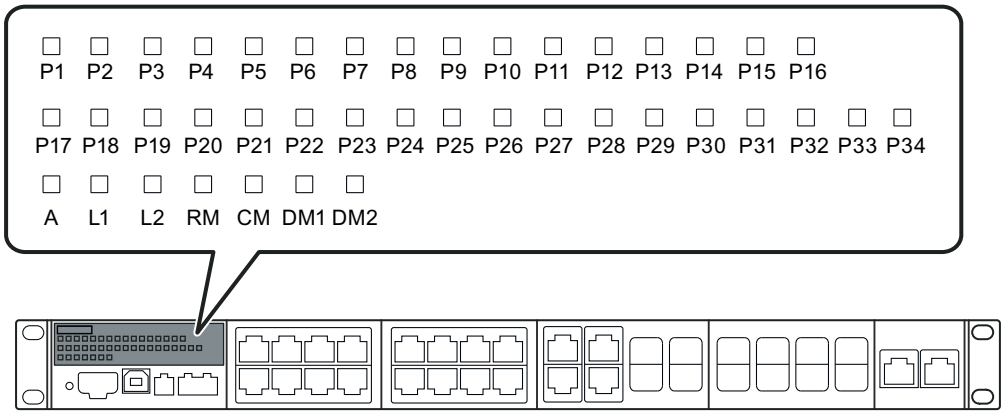
- If you use SFP transceivers of the types SFP993-1LH or SFP993-1LH+, the maximum ambient temperature is reduced to 50 °C.
  For more information, refer to "Dependency between ports and ambient temperature (derating) (Page 70)".

For the values of the ambient temperature without SFP transceivers, refer to the section "Technical specifications (Page 89)".

6.7 LED display

6.7.1 Position

The following figure shows the arrangement of the LEDs.



P	LEDs for displaying the port status *)
A	LED for displaying the fault status (alarm display)
L1/L2	LEDs for displaying the power supply
RM	LED for displaying the "redundancy manager" function
CM	LED without function
DM1/DM2	LEDs for displaying the display mode

Figure 6-2 Arrangement of the LEDs using a 24 V AC/DC device version with 12 SFP-/SFP+ slots

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

6.7.2 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, refer to section "DM1 and DM2 LEDs (Page 42)".

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 on the port (e.g. the communication partner is switched off or the cable is not connected) or the link is present but the port is switched off by management. In this state, no data is sent or received via the port.
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 four times per period*	Link exists and 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
	Flashes once per period*	Port operating at 10 Gbps
Yellow	On	Port works at 1 Gbps
	Flashes twice per period*	Port works at 2.5 Gbps
	Flashes five times per period*	Port works at 5 Gbps

* 1 period ≙ 2.5 seconds

When the transfer settings of a port are permanently set (autonegotiation disabled) and a connection error occurs, the port LED will still show the set transmission rate. When autonegotiation is enabled, the port LED will go off in case of a connection error.

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 the current version, the display mode D does not display any information.

6.7.3 A LED

The **A** LED (alarm LED) indicates the fault 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 complete yet.

Meaning during operation

LED color	LED status	Meaning during operation
-	Off	The device is operating free of errors.
Red	On	The device has detected a problem.
Red	Flashes once per period*	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.
* 1 period ≙ 2.5 seconds		

6.7.4 L1 and L2 LEDs

The **L1** and **L2** LEDs indicate the current state of the power supply at connectors **L1** and **L2**.

The meaning of the **L1** and **L2** LEDs depends on the set display mode; refer to section "DM1 and DM2 LEDs (Page 42)".

Meaning in display modes A, B and C

In the specified display modes, the **L1** and **L2** LEDs tell you whether the power supply is connected.

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 the current version, the display mode D does not display any information.

6.7.5 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.

6.7.6 DM1 and DM2 LEDs

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.

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

6.8 SELECT / SET button

6.8.1 Position

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

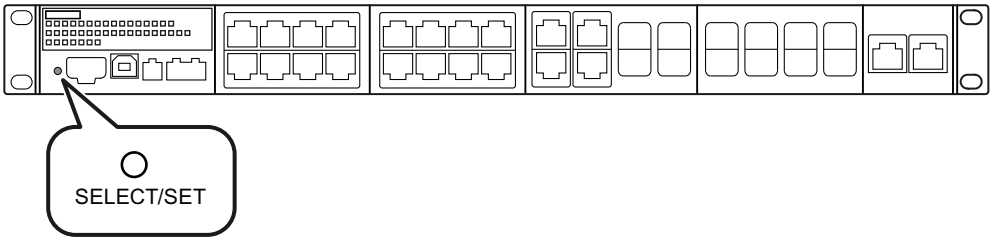


Figure 6-3 Position of the "SELECT/SET" button using a 24 V AC/DC device version with 12 SFP/SFP+ slots as an example

6.8.2 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 81)" and "Resetting the device to default settings with the button (during operation) (Page 82)".
- **Load a firmware file via TFTP**
  For more information, refer to "Load a firmware file via TFTP (Page 83)".
- **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 43)".
  For more information on the display modes, refer to "DM1 and DM2 LEDs (Page 42)".

6.8.3 Setting the display mode

To set the display mode, press the SELECT/SET button as follows:

Pressing the 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

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

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

6.9 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

6.9.1 Position

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

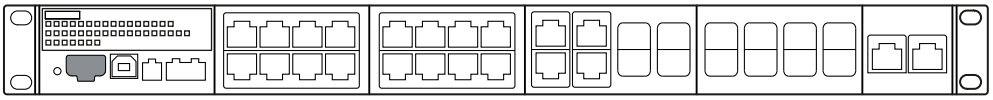


Figure 6-4 Position of the CLP slot using a 24 V AC/DC device version with 12 SFP/SFP+ slots as an example

6.9.2 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 77)".

Installing and removing

7

7.1 Safety during installation

Safety notices

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

⚠ 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.

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.

Note

The device is intended for stationary operation only.

Note

This device is not suitable for use in areas where children may be present.

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.

⚠ WARNING
If the temperature of the cable or housing socket exceeds 70 °C or the branching point of conductors exceeds 80 °C, special precautions must be taken. If the equipment is operated in an air ambient in excess of 50 °C to 60 °C, only use cables with a permissible operating temperature of at least 85 °C.

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

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

WARNING

To fulfill the requirements of the FM approval rack mounting is only possible in a vent free, tool-secured enclosure.

WARNING

If a device is operated in an ambient temperature of more than 60 °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 60 °C.

WARNING

Substitution of components may impair suitability of the equipment.

WARNING

Substitution of components may impair suitability for Division 2.

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 installation wiring connections with admitted maximum operating temperature of at least 30 °C higher than maximum ambient temperature.

WARNING

The IP rating marking is not associated with the FM approvals certification.

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" acc. 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 control cabinet protected against electric shock and spread of fire
- Installation in a suitable protective housing protected against electric shock and spread of fire
- Installation in a suitable closed control room protected against electric shock and spread of fire

⚠ WARNING

Damage in the event of improper use

The protection offered by the device can be impaired if the device is used differently to the description in section Proper use.

The device cannot be opened and repaired independently in the event of a fault; see Fault (Page 12).

⚠ WARNING

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

Additional notes

⚠ CAUTION

Use only approved components

If you use components and accessories that are not approved for SIMATIC NET devices or their target systems, this may violate the requirements and regulations for safety and electromagnetic compatibility.
Only use components approved for the SIMATIC NET devices.

NOTICE
Warming and premature aging of the IE switch due to direct sunlight
Direct sunlight can heat up the device and can lead to premature aging of the IE switch and its cabling.
Provide suitable shade to protect the IE switch against direct sunlight.

Note

During installation and operation, keep to the installation guidelines and safety notices described in this document and in the system manuals "Industrial Ethernet / PROFINET Industrial Ethernet" and "Industrial Ethernet / PROFINET passive network components".

You will find information on the system manuals in the section "Introduction", under "Further documentation".

7.2 Types of installation

The devices can be installed in the following ways:

- 19" rack mounting
- Four-point mounting using special mounting brackets

Installation clearances

Adhere to the following minimum clearances so that the convection ventilation of the devices is not blocked:

- At least 1 height unit (43.6 mm) below
- At least 1 height unit (43.6 mm) above

Installation position

Only the following installation position is permitted for all installation types of the devices:

- **Horizontal**
  The horizontal installation position is shown using the example of a control cabinet.

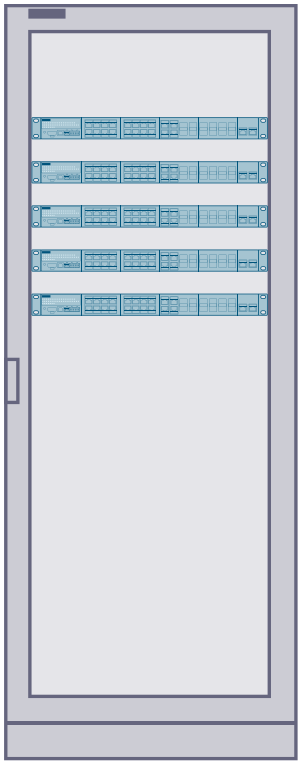


Figure 7-1 Horizontal installation position of devices in a control cabinet

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+ transceivers can be found in the section "Inserting and removing pluggable transceivers (Page 73)".

7.3 19" rack mounting

Notes on 19" rack mounting

WARNING

Increased ambient temperature

When installed in a closed rack or a rack unit with several devices, the ambient temperature of the rack may be higher than the room temperature. Install the devices in an environment compatible with the maximum ambient temperature specified by the manufacturer.

WARNING

Reduced air flow

Install the devices in a rack so that there is an adequate air flow for the reliable operation of the devices.

WARNING

Mechanical load

When installing the devices in a rack, avoid the dangers of unequal mechanical load.

WARNING

Circuit overload

When connecting the devices to the power supply, avoid the effects of circuit overload on the overcurrent protection and the power supply cables. Take into account the rated values on the nameplate of the devices.

WARNING

Reliable grounding

Devices mounted in racks must be reliably grounded. Pay particular attention to supply connectors that are not directly connected to the circuit branch (e.g. socket strip).

Note

Mounting with two mounting brackets

Mounting in a 19" rack is performed with two mounting brackets, which are pre-installed on the front of the rack unit.

Alternatively, you can mount the rack unit in a 19" control cabinet from the rear. To do this, unscrew the two mounting brackets from the rack unit and attach them upside down to the two side panels at the rear of the unit. The rack unit can then be installed in a 19" control cabinet.

Note

Installation with four-point mounting

Where mechanical strain is liable to be high, for example when used on a ship, four-point mounting is necessary.

You will find details in the sections "Four-point mounting (Page 53)" and "Mechanical stability (in operation) (Page 92)".

Mounting

⚠ CAUTION

Risk of injury if subjected to irregular mechanical strain

The device must be mounted in the 19" rack so that even if there is irregular mechanical strain, no dangerous situation can result.

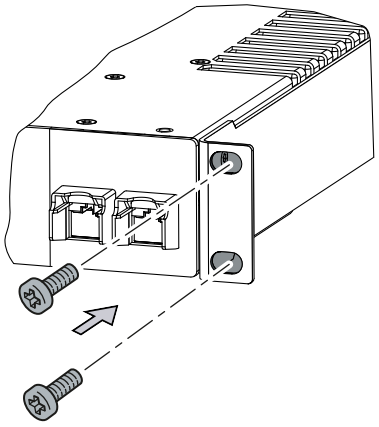


Figure 7-2 19" rack mounting

To install the device in a 19" rack, follow the steps below:

1. Position the device at the required location in the 19" rack.
2. Screw the two brackets to the 19" rack in each case with 2 securing screws.
3. Connect the cables, see section "Connecting up (Page 57)".

Uninstalling

To remove the device from a 19" rack, follow the steps below:

1. Disconnect all connected cables.
2. Undo the securing screws on the mounting brackets
3. Remove the device from the 19" rack.

NOTICE

Rack-mount instructions

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack, the operating ambient temperature of the rack environment may be greater than the room ambient. Therefore consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e. g. use of power strips).

7.4 Four-point mounting

Notes on four-point mounting

Note

Installation with four-point mounting

Where mechanical strain is liable to be high, for example when used on a ship, four-point mounting is necessary.

You will find details in the section "Mechanical stability (in operation) (Page 92)".

Example of a four-point mounting: Two mounting brackets on the left-hand side of the device (front and back) and two mounting brackets on the right-hand side of the device (front and back).

Requirements

For the four-point mounting, you require the following:

- 4 suitable brackets
- 4 recessed head screws (M3 x 6) per mounting bracket for fastening the mounting bracket to the device
- 2 suitable half-round screws (6 mm diameter) per mounting bracket for fastening the mounting bracket to the base.

Mounting bracket

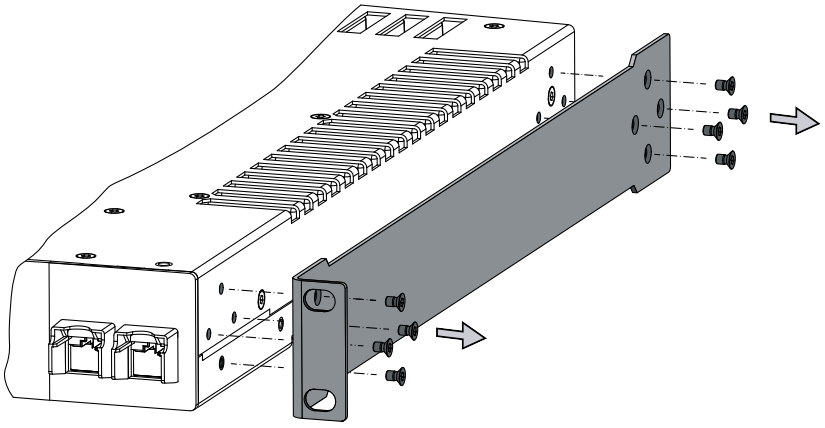
For the four-point mounting, you require special mounting brackets. You can order four mounting brackets as accessories (Page 35) or manufacture them yourself according to the design drawings. The design drawings can be found in the section "Mounting brackets for use on ships (Page 96)".

The brackets for left and right are identical.

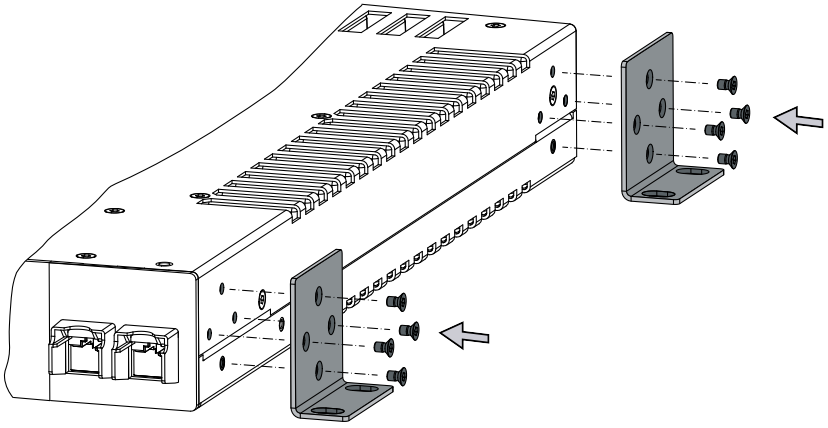
Procedure

To install the device with a four-point mounting, follow the steps below:

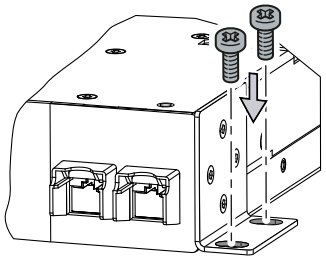
1. Remove the mounting brackets for 19" rack installation, if necessary. To do so, loosen the 8 screws on each side and remove the mounting bracket.



2. Secure the four mounting brackets each with four recessed head screws (M3 x 6 in the scope of delivery) to the side panels of the device.
   The maximum tightening torque for these screws is 0.5 Nm.



3. Position the device at the desired location and secure the four mounting brackets with two round-head screws each (6 mm diameter).



7.5 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

8

8.1 Safety when connecting up

Safety notices

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

If using power sources according to NEC Class 2 or PS2/LPS complying with UL 62368-1, please note the following information.

⚠ 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 must meet the requirements for ES1/SELV and PS2/LPS complying with IEC/UL 62368-1.

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

- Only safety extra low voltage (SELV) with limited power source (Limited Power Source, LPS / Power Source Class 2, PS2) complying with IEC 62368-1 / EN 62368-1 / VDE 62368-1 may be connected to the power supply terminals.
- The power supply unit for the device must meet NEC Class 2 according to the National Electrical Code (r) (ANSI / NFPA 70).

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

⚠ WARNING

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

Note

No light power measurement (PROFINET diagnostics)

The devices do not support diagnostics with light power measurement.

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

⚠ WARNING

Unsuitable cables or connectors

Risk of explosion in hazardous areas

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

⚠ WARNING

Lack of equipotential bonding

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

- Ensure that equipotential bonding is available for the device.

⚠ WARNING

Unprotected cable ends

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

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

⚠ WARNING

Improper installation of shielded cables

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

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

⚠ WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

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

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

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

⚠ WARNING

Transient overvoltages

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

⚠ WARNING

Suitable cables at high ambient temperatures in hazardous area

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

⚠ 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

The USB console interface is intended to serve as a service interface for repairs, commissioning and maintenance. Remove the USB plug before you operate the device in a hazardous atmosphere.

⚠ WARNING

EXPLOSION HAZARD

Electrical connectors including SFP/SFP+ transceivers must not be connected to the device or disconnected from the device in a hazardous atmosphere.

⚠ WARNING

EXPLOSION HAZARD

Do not press the SELECT/SET button when there is an explosive atmosphere.

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:

⚠ 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.

⚠ WARNING

Explosion hazard

Do not disconnect equipment when a flammable or combustible atmosphere is present.

Safety instructions when using in accordance with UL 61010-1 / CSA-C22.2 No. 61010-1

If you use the device under UL 61010-1 / CSA-C22.2 No. 61010-1 conditions, you must also keep to the following safety instructions in addition to the general safety instructions for protection against explosion:

⚠ WARNING

Connecting cables for DC power supply

To connect the power supply in the scope of validity of UL 61010-1 / CSA-C22.2 No. 61010-1, only use copper cables.

⚠ WARNING

Circuit breaker for DC power supply

An external switch or miniature circuit breaker must be provided and marked as circuit breaker for the device. The circuit breaker must be located close to the device and easily accessible for actuation.

For operation with AC power supply, the IEC plug is provided for disconnecting the device.

Further notes

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).

8.2 Wiring rules

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

Wiring rules for ...		**Spring-loaded terminals**
connectable cable cross sections for flexible cables ...	without wire end ferrule	0.75 - 2.5 mm^2
		AWG: 20 - 14
	with wire end ferrule**	0.75 - 2.5 mm^2
		AWG: 20 - 14
	with TWIN wire end ferrule**	0.75 - 1 mm^2
		AWG: 20 - 18
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.

8.3 24 V AC/DC power supply

Safety extra low voltage

WARNING

Power supply

The equipment is designed for operation with a directly connectable safety extra low voltage (SELV) or with a power supply unit that meets the requirements ES1/SELV and PS2/LPS according to IEC/UL 62368-1.

NOTICE

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

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

- In areas subject to the NEC or CEC, the fuse must meet the following requirements:
  - Suitable for AC/DC *) (min. 60 V / 3 A)
  - 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 *) (min. 60 V / 3 A)
  - Breaking current at least 10 kA
  - Approval according to IEC/EN 60947-1/2/3 or IEC/EN 60898-1/2 for circuit breakers
  - Switch off characteristics: B or C
  - Approval according to IEC/EN 60127-1 for fuses
  - Switch off 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 *) (min. 60 V / 3 A)
  - 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 *) (min. 60 V / 3 A)
  - Breaking current > highest possible current of the current source (incl. short circuit current and fault)
  - Approval according to IEC/EN 60934
  - Switch off characteristics: max. 120 s at 2 x I_n

You do not need to fuse the supply cable if you only use power sources with a limited power source (LPS) or power sources according to NEC Class 2 or PS2/LPS according to UL 62368-1 for the power supply of the devices.

*) AC or DC depending on availability

Notes on the power supply

⚠ WARNING

Incorrect power supply

The power supply unit for supplying the devices must comply with NEC Class 2 or PS2/LPS according to UL 62368-1:

- Voltage range 19.2 - 30.0 V for AC (50 / 60 Hz) and 19.2 - 31.2 V for DC
- Current requirements
  - Max. 3.2 A for AC (24 V AC/DC device version with 32 SFP/SFP+ slots)
  - Max. 3.0 A for AC (all other 24 V AC/DC device versions)
- Current requirements
  - Max. 3.2 A for DC (24 V AC/DC device version with 32 SFP/SFP+ slots)
  - Max. 3.0 A for DC (all other 24 V AC/DC device versions)

Do not operate the devices on AC voltages higher than 30.0 V AC.

Do not operate the devices on DC voltages higher than DC 31.2 V.

⚠ CAUTION

Overvoltage protection for the power supply cables

If the device is supplied over long 24 V power cables or extensive power grids, measures against coupling of strong electromagnetic pulses to the power cables are required. These can result, for example, due to lightning or switching of large inductive 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. The following Blitzductors are suitable, for example:

24 V DC: Dehn Blitzductor BVT AVD 24, order number 918 422

24 V AC: Dehn Blitzductor BVT ALD 60, order number 918 409

Manufacturer: DEHN + SÖHNE GmbH + Co. KG, Hans Dehn Str. 1, Postfach 1640, D-92306 Neumarkt, Germany.

Information on the power supply

- The power supply is connected using two 2-pin plug-in terminal blocks. The terminal blocks ship with the device.
- The power supply can be connected redundantly. Both inputs are isolated. There is no load distribution. 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 61).

WARNING

Operation only with safety extra-low voltage

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

- Do not operate the device with an AC voltage higher than 30 V AC or a DC voltage higher than 31.2 V DC.

Note

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

Position and assignment

The connection is located on the front of the device.

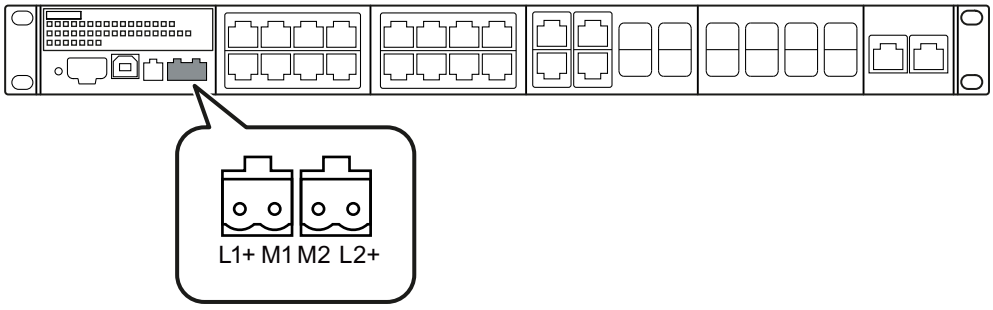


Figure 8-1 Position of the power supply using a 24 V AC/DC device version with 12 SFP/SFP+ slots

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

8.4 Grounding

WARNING

Danger from line voltage

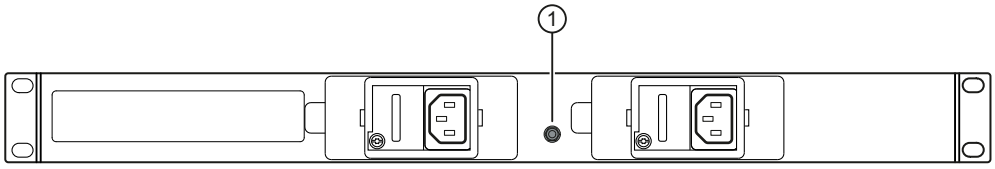
Grounding simply via the housing is inadequate.

- To ensure safe operation, connect the protective grounding in any case.

For device versions with connection to the power supply via a terminal block, grounding is performed via the mounting brackets on the device or via the grounding bolt on the rear of the device.

The grounding bolt is used as follows:

- For functional grounding
- For protective and functional grounding according to UL 62368-1 / CSA-C22.2 No. 62368-1 and UL 61010-1 / CSA-C22.2 No. 61010-1



① Grounding bolt

Figure 8-2 Position of the grounding bolt on the rear of the device

8.4.1 Functional ground

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

According to EN60204-1 (DIN/VDE 0113 T1) electrical circuits must be grounded. The chassis (0 V) is grounded at one defined point. 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.

Requirements for functional grounding

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.

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

8.4.2 Protective grounding (24 V AC/DC device versions)

Note

Protective grounding during operation in compliance with UL 62368-1 / CSA-C22.2 No. 62368-1 and UL 61010-1 / CSA-C22.2 No. 61010-1

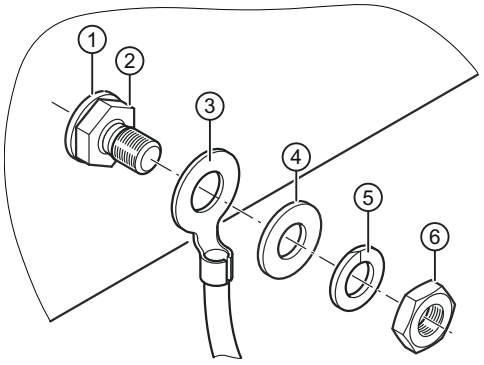
When you operate the device in compliance with UL 62368-1 / CSA-C22.2 No. 62368-1 and UL 61010-1 / CSA-C22.2 No. 61010-1, you must connect the protective grounding via the grounding bolt to meet the conditions for recognition of the UL approval. The work must be performed by a specialist according to UL 62368-1 / CSA-C22.2 No. 62368-1 and UL 61010-1 / CSA-C22.2 No. 61010-1.

You can find the procedure described in the section "Connecting the grounding via a grounding bolt (Page 67)".

Requirements for protective grounding

To wire a permanently connected protective grounding, use copper cables with a cross-section of ≥ 2.5 mm^2 if the cables are mechanically protected. If the cables are not mechanically protected, use cables with a cross-section of 4.0 mm^2.

8.4.3 Connecting the grounding via a grounding bolt



① Toothed washer
② Grounding bolt
③ Grounding terminal with cable
④ Washer
⑤ Spring washer
⑥ Nut

To connect the functional or protective grounding on devices with a screw-in grounding bolt, follow these steps:

1. Place the toothed washer ① on the screw-in grounding bolt ② and tighten the grounding bolt into the grounding connection thread on the device with a maximum torque of 2 Nm.
2. Put the ground terminal ③, the washer ④ and the spring lock washer together ⑤ on the grounding bolt as shown in the drawing.
3. Tighten the nut ⑥ with a maximum tightening torque of 0.5 Nm.

8.5 Industrial Ethernet

8.5.1 Electrical

Note

Strain relief for the Ethernet cables

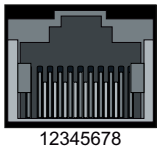
In order to avoid mechanical stress on the Ethernet cables and resulting interruption of the contact, fasten the cables at a short distance from the connector using a cable guide or busbar.

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 is also turned off. Then use a crossover cable.

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.

8.5.2 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

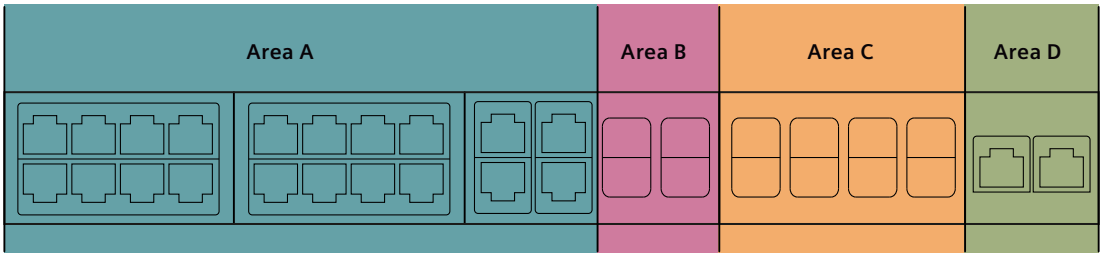
8.5.3 Dependency between ports and ambient temperature (derating)

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
SFP Active		SFP991-1A	6GK5 991-1AD00-8GA0
		SFP991-LD A	6GK5 991-1AF00-8GA0

8.5.3.1 Devices with 12 SFP/SFP+ slots



Temperature	Area A	Area B	Area C	Area D
-40 °C ... 65 °C	RJ45 to 1 Gbps	-	-	RJ45 to 10 Gbps
-40 °C ... 55 °C	RJ45 to 1 Gbps	SFP group 1	SFP group 1 SFP+ group 1 SFP Active Restriction [1]	RJ45 to 10 Gbps
-40 °C to 50 °C	RJ45 to 1 Gbps	SFP group 1 SFP group 2 Restric-tion [2]	SFP group 1 SFP group 2 SFP+ group 1 SFP+ group 2 SFP Active Restriction [3]	RJ45 to 10 Gbps

The following restrictions apply to the areas:

1) SFP transceivers of the type SFP993-1 (C) cannot be used.

2) SFP transceivers of the SFP group 2 can be used in a maximum of two of these ports. The remaining ports of the area can be filled with SFP transceivers from SFP group 1.

3) SFP transceivers of the SFP group 2 or SFP+ group 2 can be used in a maximum of two of these ports. The remaining ports of the area can be filled with SFP transceivers from SFP group 1, SFP+ group 1 or SFP Active.

8.5.4 Inserting and removing pluggable transceivers

8.5.4.1 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".

8.5.4.2 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.

8.5.4.3 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.

8.6 Signaling contact

The signaling contact is an event-driven or manually controlled failsafe alarm relay. Individual alarms can be configured to trigger the relay when the associated event occurs. The relay can also be fixed in an open or closed state.

Manually controlling the relay may be useful to:

- Verify the failsafe relay is properly connected following the installation of the device
- Verify the open/close state is caused by the device itself or some other hardware
- Keep the relay in an open/close state while troubleshooting a network issue

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 (Page 34)".

- Note the wiring rules (Page 61).
- 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

The connection is located on the front of the device.

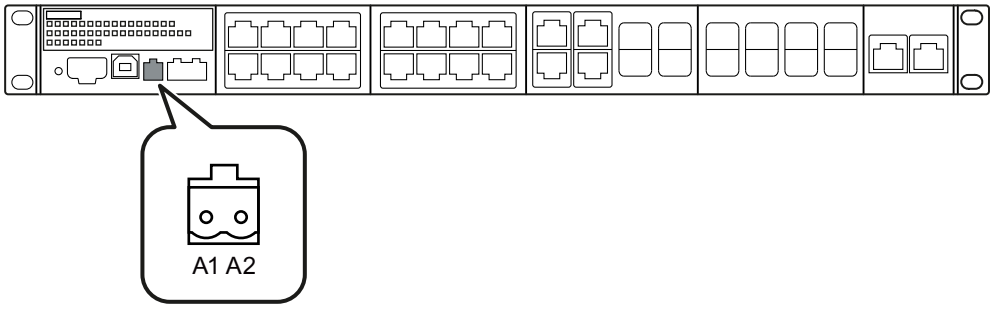


Figure 8-3 Position of the signaling contact using a 24 V AC/DC device version with 12 SFP/SFP+ slots as an example

Contact	Assignment
A1	Alarm contact 1
A2	Alarm contact 2

Signaling faults

- The indication of errors by the signaling contact is synchronous to the "A" alarm LED, see section "A LED (Page 41)".
  All errors indicated by the "A" alarm LED (configurable) are also signaled by the signaling contact.
- If an internal fault occurs, the "A" alarm LED 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.

8.7 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 34)".

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).

Switching the USB console interface

Access to the USB console interface can be switched between SCALANCE XRH334 and the integrated SCALANCE LPE9433.

For more information, refer to the SINEC OS configuration manuals.

Position

The interface is located on the front of the device.

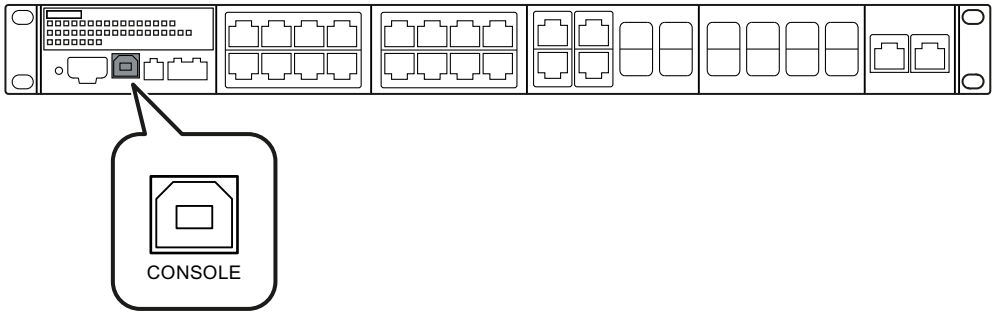
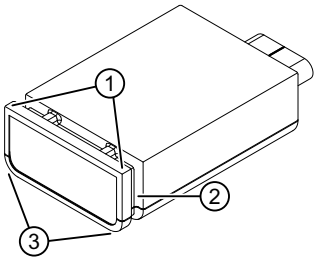


Figure 8-4 Position of the USB console interface using a 24 V AC/DC device version with 12 SFP/SFP+ slots as an example

8.8 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

9

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 34) and original spare parts (Page 34).
- 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 for SCALANCE XRH334 10

10.1 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 Web UI of the device via a network connection with a preset user profile.

To reset the device to default settings in the startup phase, do the following:

1. Turn off the power to the device.
2. Press the button and reconnect the power supply to the device while holding down the button.
3. Hold down the button until the red alarm LED **A** stops flashing and is permanently lit.
4. Release the button and wait until the alarm LED **A** goes off again.
   The device starts automatically with the default settings.

10.2 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 Web UI of the device via a network connection with a preset user profile.

Requirements

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

Resetting the device to default settings

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

1. Switch 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.

10.3 Load 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.

Initial situation

If you cannot access the device via HTTPS (Web UI) or SSH (CLI), you can upload firmware to the device using the Trivial File Transfer Protocol (TFTP).

This situation can arise, for example, if a power failure has occurred during a firmware update.

When pressing the button, observe the information in the section "SELECT / SET button (Page 42)".

Requirements

- There is a client PC in the same network as the device
  If Microsoft Windows runs on the client PC, make sure that TFTP is enabled.

  Note

  You can enable TFTP in Microsoft Windows as follows:

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

- A copy of the target firmware is saved on the client PC.

Procedure

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 power supply to the device while holding down the button.
3. Hold down the button until the alarm LED A starts to flash.
4. Release the button as long as the red alarm LED A is still flashing.
   This time only lasts a few seconds.
   In this state, the device is ready to receive a firmware file from a TFTP server (update mode).
5. Connect a client PC to an Ethernet port of the device via an Ethernet cable.

   Note

   In this state, only direct communication with the device is possible. Data traffic is not forwarded across ports.

6. Assign an IP address for the device using DHCP or SINEC PNI.
7. Carry out the following steps on the client PC:
   - Open a command prompt and go to the directory containing the firmware file.
   - Start the file transfer TFTP.
     If you are using Microsoft Windows, for example, execute the following command:
     `tftp -i { IP address of device } put { firmware file }`

   Once the firmware has been transferred completely to the device and validated, the device restarts. This may take a few minutes.
8. [Optional] Log into the device using CLI or Web UI and check the firmware version.
   For more information, refer to the SINEC OS configuration manuals for the loaded firmware version.

Troubleshooting for SCALANCE LPE9433 11

11.1 Restarting a SCALANCE LPE9433

You have the following options for restarting a SCALANCE LPE9433:

- Via the Web UI of the SCALANCE LPE9433 (IED)
- Via the Web UI of the IE Management (IEM)
- Via SINEC OS
  For more information, refer to the SINEC OS configuration manuals (Page 8).

11.2 Starting a SCALANCE LPE9433 in the Rescue system

A SCALANCE LPE has a Rescue system. A Rescue system has all necessary components of an operating system to start a device independently of the firmware. The Rescue system is used to enable access to a non-functional device or to reset the device to the delivery state.

To leave the Rescue system again, restart the SCALANCE LPE. When you restart a SCALANCE LPE, the SCALANCE LPE automatically performs a restart.

Because this action is usually performed using the button, but an integrated SCALANCE LPE9433 is not physically accessible, there are specific configuration options via SINEC OS.

For more information, refer to the SINEC OS configuration manuals (Page 8).

11.3 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.

NOTICE
Observe information on new firmware version The improper use of a new firmware can lead to a malfunction or to failure of the device. When updating to a new firmware version, consider all information to be published for this firmware version. The firmware is provided via the Industrial Edge Management. If the firmware update needs to take place via the Rescue system, the firmware file can be obtained via the Siemens Industrial Online Support (https://support.industry.siemens.com/cs/ww/en/ps/26683/dl).

Initial situation

If you cannot access a SCALANCE LPE9433 via HTTPS (Web UI), you can upload firmware to the SCALANCE LPE9433 using the Trivial File Transfer Protocol (TFTP).

This situation can arise, for example, if a power failure has occurred during a firmware update.

NOTICE
Previous configurations and applications are lost When firmware is loaded in this way, the configuration is reset to factory settings and all information saved on the SCALANCE LPE9433 is deleted. This also affects all Docker components (containers, networks, volumes, images, bind mounts, etc.) present on the SCALANCE LPE9433. • Back up your previous configurations before you load a new firmware via the Rescue system.

Note

Onboarding after resetting the configuration

After the configuration is reset, the icon for the SCALANCE LPE9433 is still shown in the Industrial Edge Management. However, access to the device via Industrial Edge Management is no longer possible after the reset. The icon for SCALANCE LPE9433 IEM has no function and should be removed.

To be able to access the device with the Industrial Edge Management again, perform the onboarding process once more.

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

Requirements

- There is a client PC in the same network as a SCALANCE XRH334
  If Microsoft Windows runs on the client PC, make sure that TFTP is enabled.

  Note

  You can enable TFTP in Microsoft Windows as follows:

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

- Ensure that the TFTP client is active in the Windows network (domain, private, public) that is connected with the SCALANCE XRH334.
- A copy of the target firmware is saved on the client PC

Procedure

NOTICE
Danger of damage to property If the power supply to the device is lost while a firmware file is being loaded, an error state can occur. Do not disconnect the device from the power supply while a firmware file is being loaded. Do not switch off the device during the reboot after loading the firmware. The firmware update is not complete until you are able to log in after the device has restarted. If the power supply is interrupted during the reboot, the device may not be functional any longer. Such a functional disruption can only be remedied with the help of our technical support.

Using TFTP, you can supply a SCALANCE LPE9433 with new firmware even when a connection via the Web UI is not possible. This section explains the procedure based on the example of Microsoft Windows.

To load a new firmware via TFTP, do the following:

1. Check the firewall settings of the client PC on which you start the TFTP client.
   With incorrect settings, the bidirectional connection establishment can cause communication problems.
2. Connect the client PC to an Ethernet port of the SCALANCE XRH334 via an Ethernet cable.
3. Start the SCALANCE LPE9433 via SINEC OS in the Rescue system.
   For more information, refer to "Starting a SCALANCE LPE9433 in the Rescue system (Page 85)".
   In this state, the SCALANCE LPE9433 is ready to receive a firmware file from a TFTP server.
4. Assign an IP address for the SCALANCE LPE9433 using DHCP or SINEC PNI.
5. Carry out the following steps on the client PC:
   - Open a command prompt and go to the directory containing the firmware file.
   - Start the file transfer via TFTP.
     If you are using Microsoft Windows, for example, execute the following command:
     `tftp –i { IP address of the SCALANCE LPE9433 } put { firmware file }`

   Once the firmware has been transferred completely to the SCALANCE LPE9433 and validated, the SCALANCE LPE9433 restarts. This may take a few minutes.

11.4 Resetting the configuration of a SCALANCE LPE9433

NOTICE
Previous configuration settings will be lost By resetting the configuration, all the settings you have made will be overwritten by factory defaults. The software components you have installed or other changes to the device, depending on the configuration directory, are retained.

Note

Onboarding after resetting the configuration

After the configuration is reset, the icon for the SCALANCE LPE9433 is still shown in the Industrial Edge Management. However, access to the device via Industrial Edge Management is no longer possible after the reset. The icon for SCALANCE LPE9433 IEM has no function and should be removed.

To be able to access the device with the Industrial Edge Management again, perform the onboarding process once more.

Because this action is usually performed using the button, but an integrated SCALANCE LPE9433 is not physically accessible, there are specific configuration options via SINEC OS.

For more information, refer to the SINEC OS configuration manuals (Page 8).

11.5 Starting up a switched off SCALANCE LPE9433

When a SCALANCE LPE9433 has been shut down, you can start up the device in the following ways:

- Connect to the CLI or Web UI of the SCALANCE XRH334 and perform one of the following actions:
  - Restarting a SCALANCE LPE9433
  - Starting a SCALANCE LPE9433 in the Rescue system
  - Resetting the configuration of a SCALANCE LPE9433

  All of these actions trigger a restart of the SCALANCE LPE9433.
- Restart the SCALANCE XRH334.
  When you restart SINEC OS, the SCALANCE LPE9433 is also restarted.

Technical specifications

12

12.1 Technical specifications of the 24 V AC/DC device version

The following technical specifications apply to the 24 V AC/DC version of the SCALANCE XRH334 with 12 SFP/SFP+ slots.

Technical specifications			
Connection to Industrial Ethernet			
Electrical connectors	Quantity	20	2
	Connector	RJ45 jack	RJ45 jack
	Transmission speed	10 / 100 / 1000 Mbps	1 / 2.5 / 5 / 10 Gbps
	Properties	Half/full duplex, MDI-X pinning	
Slots for plug-in transceivers (SFP)	Quantity	4	
	Connector	SFP plug-in transceiver	
	Transmission speed	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)	
Connection to power supply			

Technical specifications		
Power supply [1]	Design	Spring-loaded terminal block, 2-pin
	Rated voltage	24 V AC / 24 V DC
	Voltage range	19.2 to 30.0 V AC 19.2 to 31.2 V DC
	Frequency	50 / 60 Hz (with AC)
	Frequency range	50 Hz to 60 Hz
	Fusing	10 A / 250 V
	Properties	Implemented redundantly. The connected power supply must meet the requirements of NEC Class 2 or PS2/LPS in compliance with UL 62368-1. If you connect the power supply redundantly, you are operating the device either only with alternating voltage or only with direct voltage. Do not connect alternating voltage to one connector and direct voltage to the other.
	Degree of pollution	2
Current consumption	At nominal voltage	3.2 A
Effective power loss	At nominal voltage	76.8 W
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	During operation in horizontal installation position:
	Up to 2000 m above sea level	-40 °C ... +65 °C
	When operating with SFP transceivers up to 2000 m above sea level, refer to "Dependency between ports and ambient temperature (derating) (Page 70)"	
	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 If the storage period exceeds one year, the storage temperature can be max. 55 °C.
	During transportation	-40 °C to +85 °C
Relative humidity	During operation at 25 °C	≤ 95% without condensation
Housing, dimensions and weight		
Design	Rack	
Housing material	Metal	
Degree of protection	IP20 [4] [5]	
Dimensions (W x H x D)	446 x 43.5 x 374.8 mm (1 height unit)	
Weight	8000 g	
Installation options	• 19" rack mounting • Four-point mounting	

Technical specifications	
Mounting restriction	None
Conformal-coated PCBs	Yes
Design of the mounting bracket for four-point mounting	
Dimensions (W x H x D)	43.6 x 43.6 x 18.3 mm (1 height unit)
Plate thickness	1.5 mm
Bending radii	1.5 mm
Surface of the housing	Stainless steel X6CR17
Mean time between failure (MTBF)	
MTBF (EN/IEC 61709; 40 °C)	> 10.6 years

1) Wiring rules

Note the wiring rules (Page 61).

2) Ambient temperature with SFP

The maximum ambient temperature during operation depends on the operating elevation and the inserted SFP transceivers.

3) Derating

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

4) Degree of protection

The degree of protection was not examined in the context of UL certification.

5) Degree of protection

The degree of protection was not examined in the context of FM certification.

12.2 Technical specifications of the SCALANCE LPE9433

The following technical specifications apply to the integrated SCALANCE LPE9433.

Technical specifications		
Connection to Industrial Ethernet		
Transmission speed RDI ports	extender0/1	1000 Mbps
	extender0/2	1000 Mbps
	extender0/3	10 Gbps
Processor, RAM and storage medium		
Processor	Type	64-bit ARMv8 A53
	Number of cores	4
	Cycle	1.6 GHz
Work memory	Type and size	8 GB DDR4 RAM
Storage medium		38 GB eMMC (pSLC)

12.3 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

12.4 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)

12.5 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

12.6 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: 30 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	811688

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.

Dimension drawings

13

13.1 SCALANCE XRH334 dimension drawings

Note

Dimensions are specified in mm.

Front view

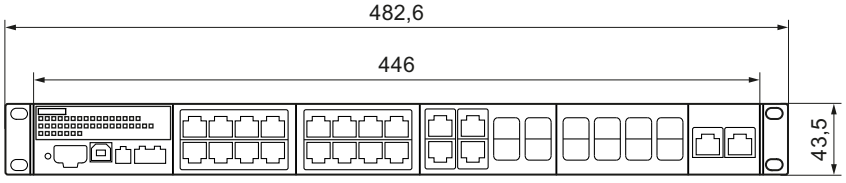


Figure 13-1 Width and height

Top view

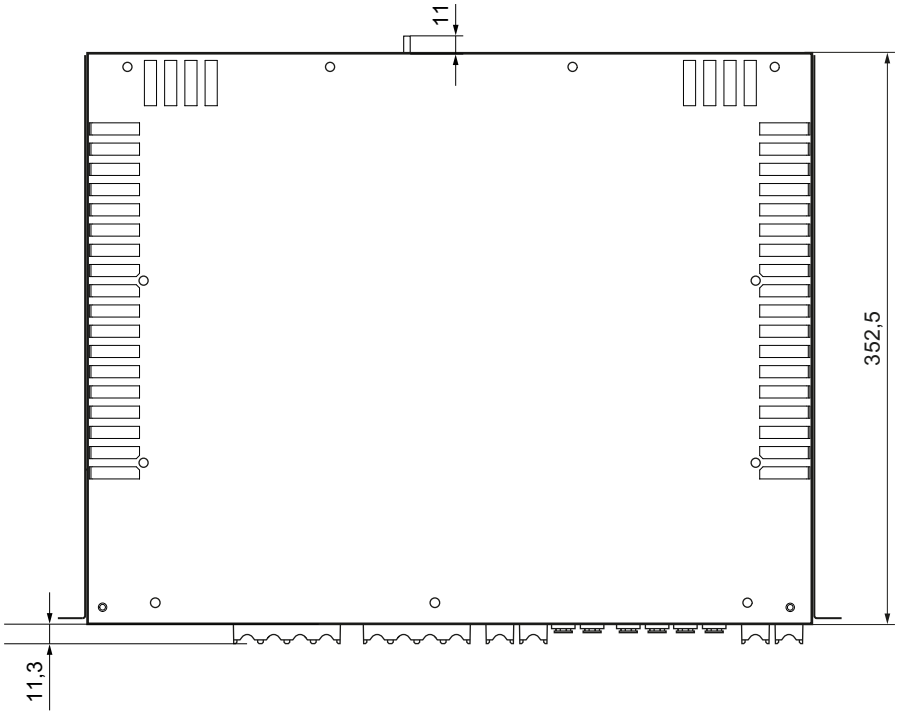


Figure 13-2 Depth

13.2 Mounting brackets for use on ships

You need special mounting brackets to install the device horizontally on a ship.

Below you will find the design drawing for making the mounting brackets.

You will find the more information on the construction of the mounting brackets in the section "Technical specifications (Page 89)".

Note

ISO tolerance and punching burr

For dimensions without tolerance details, the general tolerances "medium" acc. to DIN ISO 2768 apply. No punching burrs are permitted.

Mounting bracket for four-point mounting

Dimensions are specified in mm.

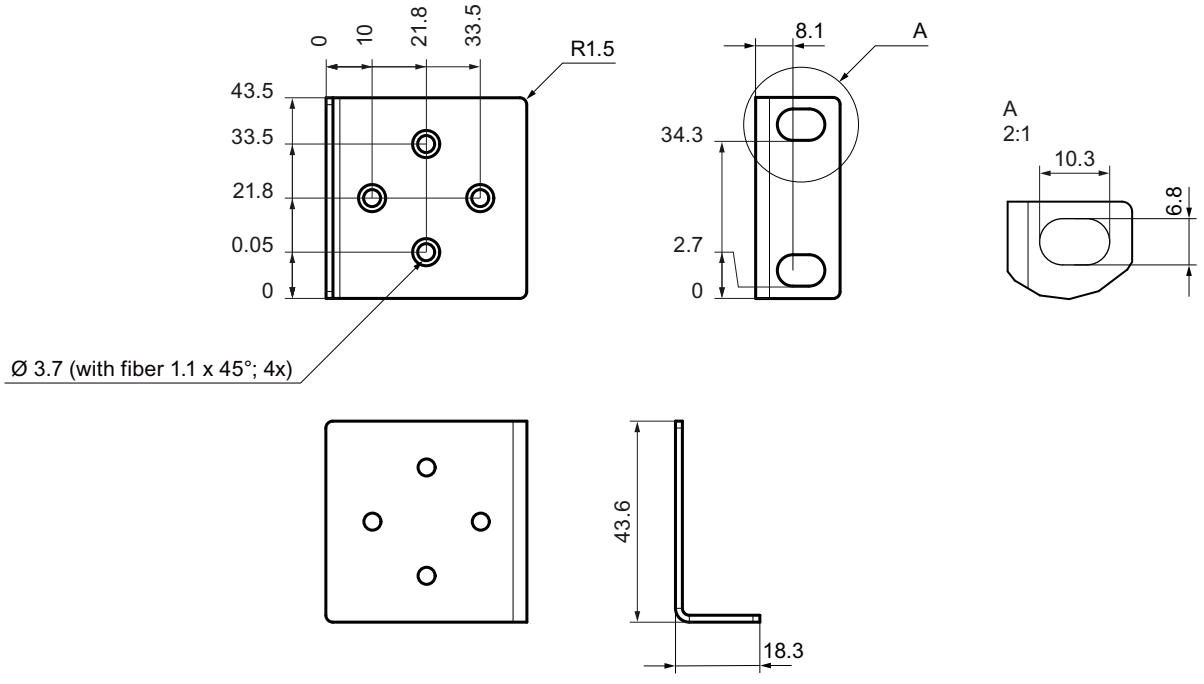


Figure 13-3 View from the front, top, and side

Approvals

14

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

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 for industrial control equipment



cULus Listed IND. CONT. EQ.

Underwriters Laboratories Inc. complying with

- UL 61010-1
- UL 61010-2-201
- CAN/CSA-IEC 61010-2-201

Report no. E85972

cULus Approval for Information Technology Equipment



cULus Listed I. T. E.

Underwriters Laboratories Inc. complying with

- UL 62368-1 (information/communication technology)
- CSA C22.2 No. 62368-1 (information/communication technology)

Report no. E115352

cULus Approval Hazardous Location



cULus Listed I. T. E. 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. E240480

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 XRH334	(*)

* 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

1

19" rack mounting, 33, 52

A

Accessories, 34
Alarm LED, 33
Approvals, 97
Article numbers, 31
Autonegotiation, 69
AWG, 61

C

Cable cross section, 61
CE mark, 97
Certificates, 27
Clip, 73
CLP, 33, 35
    Position, 44
    Replacing, 77
Command Line Interface (CLI), 84
Components of the product, 33
Connecting
    24 V AC/DC power supply, 64
Connecting cable, 76
Connection to Industrial Ethernet, 89, 91
Control cabinet, 51
Cross section, 61

D

Dimensions, 90
DM LED, 33

E

Electrical data, 89
Environmental conditions, 90
ESD directives, 13

F

Firmware, 87
Firmware update, 87
Four-point mounting, 52, 53
Functional ground, 65

G

Grounding, 65

H

Housing, 90

I

Installation, 90

K

Key, 27

L

L LED, 33
LED display, 39
    Alarm LED, 33
    DM LED, 33
    L LED, 33
    Port LED, 33
Loading firmware, 86
Logs
    per port, 28

M

MDI / MDI-X autocrossover, 69
Mounting
    Four-point mounting, 53
    Mounting bracket, 33, 52
    Rack, 33, 52
Mounting bracket, 33, 35, 51, 53
    Use on ships, 96
MTBF, 91

O

Overvoltage protection, 64

P

Permitted ambient conditions, 90
Pin assignment, 68
PLUG, 35
Pluggable transceiver
  Inserting, 73
  Notes on deinstallation, 74
  Removing, 74
  SFP, 35, 36
  SFP active, 36
Pluggable transceiver slot, 73, 74
Plug-in transceiver
  SFP bidirectional, 37
Port LED, 33
Power supply, 89
  24 V AC/DC, 33, 64
Protective grounding, 65

R

Rack mounting, 33, 52
Removable data storage medium, 35

S

Safety extra low voltage, 65
Safety notices
  for installation, 45
  general, 15
  Use in hazardous areas, 15, 45, 57
  when connecting up, 57
Sealing plug, 73, 74
SELECT/SET button, 33, 42, 84
Serial cable, 35
Serial interface, 76
SFP plug-in transceiver, 35
SFP transceiver, 36
SFP/SFP+ transceiver
  Slots, 33
SFP+ transceiver, 37
Ship, 53
Signaling contact, 33, 74
Slot, 73
Spare parts, 34
Spring-loaded terminal, 74
System manual, 49, 102

T

TFTP, 87
Type of installation, 49

U

USB cable, 35
USB console interface, 33

W

Web User Interface (Web UI), 84
Weight, 90
Wiring, 61
Wiring rules, 75